



Central Bank of India

Cent NEO Department

Request for Proposal (Bid) Document

For

**RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and
AI/ Gen AI Platform for “Data Transformation and AI Banking”**

Bid Number: GEM/2026/B/7203650

06th February 2026

Contents

Tender Details	12
1 Eligibility Criteria	15
2 Bid Security (Earnest Money Deposit-EMD).....	19
3 Performance Bank Guarantee (PBG)	19
4 Cost of Bidding.....	20
5 Manufacturer's Authorization Form.....	20
Section-2	21
Scope of Work.....	22
6 Scope of work for the SI	23
6.1 Project planning and management	23
6.2 Project Staffing.....	23
6.3 Design and Architecture of Platform	25
6.3.1 Lakehouse Architecture	26
6.3.2 Accelerators.....	27
6.3.3 AI, GenAI, and Agentic AI Enablement	28
6.3.4 Advanced Analytics Capabilities.....	28
6.3.5 Rapid Onboarding Framework.....	28
6.3.6 Future-Ready Design	29
6.4 Target State Platform Capabilities	29
6.4.1 Sources.....	29
6.4.2 Integration.....	30
6.4.3 Storage and Processing	31
6.4.4 Access.....	35
6.4.5 Consumption	38
6.4.6 Operations	42
6.4.7 Security.....	49
6.4.8 Governance.....	51
6.4.9 Infrastructure.....	52
6.5 Sizing for the Platform Infrastructure	54
6.5.1 Compliance and Documentation.....	55
6.5.2 Leverage Bank's existing resources	55
6.5.3 Licensing and Software Requirements	56
6.5.4 Hardware Specifications	57
6.5.5 Infrastructure Sizing and Design	62
6.5.6 High Availability and Disaster Recovery.....	63

6.5.7	Security and Network Requirements	63
6.5.8	Performance and Scalability	63
6.5.9	Implementation and Support.....	64
6.5.10	Additional Requirements	64
6.6	Platform infrastructure setup.....	64
6.7	Implementation of Platform	67
6.7.1	Sources.....	67
6.7.2	Integration.....	67
6.7.3	Storage and Processing	70
6.7.4	Access.....	74
6.7.5	Consumption	75
6.7.6	Operations	79
6.7.7	Security	83
6.7.8	Governance.....	85
6.7.9	Infrastructure.....	87
6.8	Implementation of use cases	88
6.8.1	Data Preparation and Integration	90
6.8.2	Reporting and Analytics Use Cases.....	90
6.8.3	AI and Machine Learning Use Cases.....	91
6.8.4	Generative AI Use Cases	91
6.8.5	Agentic AI Use Cases	91
6.8.6	Impact Tracking System	91
6.8.7	Support implementation of additional use cases	92
6.9	Testing and quality assurance	93
6.9.1	Perform Unit Testing	93
6.9.2	Conduct System Integration Testing (SIT)	93
6.9.3	Execute Functional Testing	93
6.9.4	Assist the Bank in Acceptance Testing (AT)	93
6.9.5	Perform Regression Testing.....	94
6.9.6	Conduct Performance Testing	94
6.9.7	Perform Security and Compliance Testing	94
6.9.8	Set up the Test Environment	94
6.9.9	Provide Testing Tools	94
6.10	Migration from current Data Infrastructure	95
6.10.1	Assessment and Planning.....	95
6.10.2	Data Migration	96

6.10.3	Migration of Reporting Solution	97
6.10.4	Migration of Business Applications	97
6.10.5	Migration of Business Intelligence Dashboards	99
6.10.6	Migration of Machine Learning Models	99
6.10.7	Testing and Validation.....	99
6.10.8	Composition of the current Technology stack:.....	100
6.11	Operations and Maintenance.....	100
6.11.1	Patch and Configuration Management.....	100
6.11.2	Infrastructure Ownership and Management.....	101
6.11.3	Facility Management and Maintenance	101
6.11.4	Warranty and AMC	102
6.11.5	Service Level Management.....	103
6.11.6	Incident and Change Management	103
6.11.7	Compliance and Security	103
6.11.8	Business Continuity and Disaster Recovery	104
6.11.9	Information Protection.....	104
6.11.10	End of Sales/Support and Roadmap	104
6.11.11	Monitoring and Reporting.....	104
6.11.12	Contract Extension.....	104
6.11.13	Service Desk	104
6.11.14	Enhancements and Upgrades	105
6.11.15	Data Tiering Requirements.....	105
6.11.16	Data Operations	105
6.11.17	Data Backup and Recovery	107
6.12	Change Request	108
6.13	Regulatory Compliance	109
6.13.1	Adherence to Regulatory and Statutory Guidelines.....	109
6.13.2	Audit and Risk Management	110
6.13.3	Warranty and AMC Support.....	110
6.13.4	Backup, Storage, and Restoration.....	110
6.14	Data Protection	110
6.14.1	Compliance with Data Protection Regulations.....	110
6.14.2	Deployment of Data Protection Components	111
6.14.3	Cryptographic Key Management	111
6.14.4	Data Protection Functionalities	111
6.14.5	Historical Data Management.....	111

6.15 Documentation	111
6.15.1 Creation and Maintenance of Documentation	111
6.15.2 Additional Documentation Requirements	112
6.15.3 Documentation Updates and Accessibility	113
6.15.4 Incident Reporting and Root Cause Analysis.....	113
6.16 Training and knowledge transfer.....	113
6.16.1 Training	113
6.16.2 Knowledge Transfer	113
6.17 Disaster Recovery.....	113
6.17.1 Disaster Recovery Strategy and Procedures	114
6.17.2 Infrastructure Resilience and Redundancy	114
6.17.3 Replication and Data Consistency	114
6.17.4 Data Ownership and Retention.....	114
6.17.5 DRC Infrastructure Requirements.....	114
6.17.6 Monitoring and Reporting.....	114
6.17.7 Operational Scenarios	115
6.17.8 Zero Data Loss and SLR Adherence.....	115
6.17.9 Additional Solution Features	115
6.18 Project Execution Location	115
6.19 Hardware and Software Warranty & AMC	115
6.19.1 Warranty and AMC/ATS Support.....	115
6.19.2 Roadmap and End-of-Life Management	116
6.19.3 Problem Resolution and Service Levels.....	116
6.19.4 Licensing and Legal Compliance.....	116
6.19.5 AMC/ATS and Payment Terms	116
6.19.6 Equipment Replacement and Maintenance Standards.....	117
6.19.7 ATS for Software	117
6.20 Certifications.....	117
6.20.1 Attainment of ISO Certifications	117
7 Required Artefacts	118
7.1 Platform Architecture	118
7.2 Infrastructure Sizing	118
7.3 Implementation Approach.....	118
7.4 Commercials	118
7.5 Team and Resources	118
7.6 Case Studies and References	118

8 Project Timelines	119
9 Maintenance Support.....	128
Section-3	129
Terms & Conditions.....	130
10 Liquidated Damage	131
11 Land Border Sharing Clause	132
12 Monitoring & Audit	135
13 Bid Submission	136
14 Integrity Pact	137
15 Technical and Commercial Offers	138
16 Evaluation & Acceptance	140
17 Evaluation Process	141
17.1 Stage 1-Eligibility Criteria.....	141
17.2 Stage 2-Technical Evaluation Criteria.....	141
17.2.1 Technical Bid Submission	143
17.2.2 Scoring of SI Presentation and Solution Evaluation	154
17.2.3 Final Scoring of Technical Bid Evaluation of Technical Bids	157
17.3 Stage 3 – Commercial Evaluation Criteria.....	157
18 General Terms	160
18.1 Important Terms & Conditions:	160
18.2 Applicability of Preference to Make in India, Order 2017 (PPP-MII Order).....	161
19 Payment Terms	161
20 Service Level Agreement	170
21 Reporting of Material Adverse Events and Incident Management	182
22 Insurance	183
23 Order Cancellation	183
24 Indemnity.....	184
24.1 General Indemnity	184
24.2 Patent, Copyright, Trademark, and Intellectual Property Infringement.....	185
25 Confidentiality & Non-Disclosure	186
26 Force Majeure.....	187
27 Resolution of Disputes	187
28 Format of the Letter of undertaking of Authenticity to be submitted by the Bidder.....	188
29 Sub-Contractor/ Independent Contractor	189
30 Assignment	189
31 Execution of Contract, SLA & NDA	190

32 SI / Bidder's Liability	190
33 Change in Location/ Merger/Amalgamation	190
34 Information Ownership	191
35 Inspection, Audit, Review, Monitoring & Visitations.....	191
36 Monitoring	192
37 Visitations	192
38 Information Security	193
39 Intellectual Property Rights	193
40 Enterprise License:	196
41 Termination	197
41.1 Termination for Default	197
41.2 Termination for Insolvency	198
41.3 Termination- Key Terms & Conditions	198
41.4 Right to Transfer IT Outsourcing Arrangements	198
41.5 Exit Option & Contract Re-Negotiation.....	198
42 Privacy & Security Safeguards	199
43 Governing Law and Jurisdiction.....	199
44 Compliance	200
44.1 Adherence to Cyber Security Policy	203
44.2 Compliance with Laws	204
45 Violation of Terms	204
46 Corrupt & Fraudulent Practices	204
47 Publicity	205
48 Entire Agreement; Amendments	205
49 Survival and Severability	205
50 Bidding Document.....	205
50.1 Amendments to Bidding Documents	205
50.2 Period of Validity	206
50.3 Last Date and Time for Submission of Bids	206
50.4 Late Bids	206
50.5 Modifications and/or Withdrawal of Bids.....	206
50.6 Clarification of Bids	206
51 Signing of Contract.....	206
52 Sustainable Sourcing.....	206
53 Remote Access	207
54 Business Continuity and Disaster Recovery	207

54.1 Business Continuity Plan (BCP)	207
54.2 Disaster Recovery Plan (DRP)	207
55 Obligation to Co-operate with relevant authorities in case of Insolvency/Resolution	207
55.1 Insolvency	207
55.2 Cooperation.....	207
55.3 Continued Service During Resolution	208
55.4 Notification.....	208
56 Data Localization	208
57 Authorized Signatory	208
58 Escrow Arrangements	208
59 Digital Personal Data Protection Act/Rules	209
60 Labour Law	209
61 Right to alter/ delete Components and Quantities specified in the RFP	210
62 Conflict of Interest.....	210
Section-4	211
Annexures	212
Checklist for Submission.....	213
Annexure 1: Conformity Letter	215
Annexure 2: Commercial Bill of Material	216
Annexure 3: Bidder's Information	244
Annexure 4: Letter for Conformity of Product as per RFP	246
Annexure 5: GOI Guidelines with Model wise classification (Make in India)	247
Annexure 6: Undertaking of Authenticity for Products Supplied.....	250
Annexure 7: Undertaking for Acceptance of Terms of RFP	251
Annexure 8: Manufacturer's Authorization Form	252
Annexure 9: Integrity Pact.....	253
Annexure 10: Non-Disclosure Agreement.....	259
Annexure 11: Performance Bank Guarantee.....	264
Annexure 12: Minimum Technical Specifications	267
Annexure 13: Bid Security (BG Format- for Earnest Money Deposit)	320
Annexure 14: Bidder's Particulars	322
Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"	323
Annexure 16: NPA UNDERTAKING.....	324
Annexure 17: Land Border Sharing Undertaking Letter	325
Annexure 18: Cover Letter	327

Annexure 19: Escalation Matrix.....	328
Annexure 20: Query Format.....	329
Annexure 21: Guidelines on Banning of Business Dealing.....	330
Annexure 22: Undertaking of Information Security from Bidder	339
Annexure 23: Software Bill of Material (SBOM) Format.....	341
Annexure 24: Template for Third Party Due Diligence Questionnaire	342
Annexure 25: List of Hardware and Software Components:	347
Annexure 26: Letter for Refund of EMD	348
Annexure 27: Format for Submission of Client References by Bidder.....	350
Annexure 28: Undertaking for Data Privacy	352
Annexure 29: Undertaking for 7 Years Roadmap.....	353
Annexure 30: Format for Local Content	354
Annexure 31: Proposed Team Profile.....	355
Annexure 32: Volumetrics	357
Annexure 33: Declaration of Source Code Audit.....	367
Annexure 34: Existing Application Details.....	368
34.1 ADF Application.....	368
34.2 Financial Planning & Budgeting Application.....	370
Annexure 35: Self-Declaration Regarding Non-Suspension by GeM in the Last Six Months ..	375
Annexure 36: Declaration / undertaking from bidder to comply with the Information and cyber security controls.....	376
Annexure 37: Information/Cyber-Security Measures/Controls for selected Service Provider	377

List of Abbreviations

AMC	Annual Maintenance Contract
APM	Application Performance Management
ATS	Annual Technical Support
BOM	Bill of Material
Bank	Central Bank of India
DB	Database
DC	Data Centre
DRC/ DRS	Disaster Recovery Centre/ Site
EMD	Earnest Money Deposit
EMS	Enterprise Management System/Solution
EPP	End Point Protection
FY	Financial year
GSI	Global system integrator
GST	Goods & Service Tax
HLD	High Level Design Document
IT	Information Technology
ITAM	IT Asset Management
LLD	Low Level Design Document
LLP	Limited Liability Partnership
MAF	Manufacturer Authorization Form
MSME	Micro, Small & Medium Enterprise
NEFT	National Electronic Funds Transfer
NS	Near Site
OEM	Original equipment manufacturer
PBG	Performance Bank Guarantee
PO	Purchase order
PSE	Public Sector Enterprise
PSU	Public Sector Undertaking
RBI	Reserve Bank of India
RFP	Request for Proposal
RTGS	Real Time Gross Settlement
SAN	Storage Area Network
SAS	Serial attached SCSI
SDR	Single Data Repository
SI	System Integrator
SPOC	Single Point of Contact
SSD	Solid state drive

Section-1

Tender Details

Invitation for Tender Offers

Central Bank of India, herein after referred to as the "Bank", is a leading Public Sector Bank established in the year 1911. The equity shares of the Bank are listed in both Bombay Stock Exchange/ National Stock Exchange. The Bank is having its Central Office at Chander Mukhi, Nariman Point, Mumbai- 400021. & it's Customer Care Department at 2nd floor, MMO Building, Fort, Mumbai 400001. Bank has completed 114 years of its service to the Nation and its millions of satisfied customers with technology-oriented bouquet of user-friendly services and in the field of IT we are known for providing new innovative and customer friendly services. The Bank has pan India presence through its wide network of more than 4685 plus branches, 13 Zonal Offices, 90 Regional Offices spread across the country as on 31.03.2025. The Bank also has specialized branches for catering to the specific needs of Retail customers, Industrial units, corporate clients, Forex dealers, Exporters and Importers, Small Scale Industries and Agricultural sector.

The Bank plans to build a Data Driven AI Banking which includes comprehensive Data Transformation with AI and Gen AI capabilities and building state-of-art Data stack hosted **on-premises**. This platform will seamlessly integrate Data, Advanced analytics, and cutting-edge AI capabilities, including both Generative AI (GenAI) and Agentic AI. This **integrated approach aims to generate value through at least 20+ specific use cases with a provision to scale up further use cases**.

The Bank through this Request for Proposal (RFP) is interested in identifying a Solution Provider/System Integrator for building a **Data Driven AI Bank**.

Bank invites online tender offers (Technical offer and Commercial offer) from eligible, reputed SIs/Bidders to create a Vision, Roadmap for Data Transformation and AI Banking, Design the Technological Architecture to make the Organisation as **Data Driven AI Bank** which includes Supply, Implement, Configure and Maintain the Data and Gen AI Platform and related System Software at DC and DRC as well as create a Robust AI Infrastructure and Data Stack for Transforming our Bank as a Data Driven AI Bank.

The Contract Period shall be for 5 years from the date of "Production deployment and sign off on implementation of Lakehouse Platform" (refer Section-2, Clause#8).

The Bank has the option for extending the AMC/ATS of the in-scope components for additional 2 years or more after expiry of the contract at reasonable cost which is mutually agreeable both to the Bank and the vendor.

The details are given below:

Tender Reference Number	GEM/2026/B/7203650
Date of RFP Issue	6/2/2026
Bid Security (EMD)	₹5,00,00,000/- (Rupees Five crore Only) in the form of Bank Guarantee issued by a Scheduled Bank other than Central Bank of India for the entire period of Bid validity (180 days) plus 3 months or by means of Banker's Cheque / Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India (IFSC Code - CBIN0283154) with narration Tender ref no GEM/2026/B/7203650 in Favor of "Central Bank Of India" and payable at Mumbai.
e-mail IDs for sending queries and Last Date for submission of queries	cmit1neobida@centralbank.co.in, agmitdigital@centralbank.co.in latest by 11/2/2026 up to 15:00 hrs. Queries to be submitted with Proof of remittance of document/Tender cost (If required).
Date and time for Pre-Bid Meeting,	12/2/2026 at 15:00hrs.
Last Date and Time submission of Bids Mode of bid submission & online portal's URL	06/03/2026 up to 15:00 hrs. Mode-Online Government e Marketplace (GeM)
Time & Date of Opening of technical bids	06/03/2026 at 15:30 hrs.
Response Types	1. Technical Bid + Bid Security 2.Commercial Bid
Address for Communication	Asstt. General Manager-IT Digital Central Bank of India Cent NEO Department, 6 TH Floor, Tower 7, Sector-11, CBD Belapur Station Complex, Navi Mumbai- 400614 <u>Mail address:</u> cmit1neobida@centralbank.bank.in, agmitdigital@centralbank.bank.in smitpurchase@centralbank.bank.in
Contact Telephone Numbers	022- 2758 2458, 67123669,

The pre bid meeting will be held in person with the SI/Bidders. For any clarification with respect to this RFP, the SI/Bidder may send their queries/suggestions, valuable inputs by email to the Bank. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to designated email ID within stipulated time as mentioned in the below format:

S. No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	SI/Bidder's Query/Suggestion/Remarks

Exemption from submission of EMD shall be given to bidders, who are Micro and Small Enterprises (MSE) having valid Udyam Registration Number/ Startup. The bidder who are MSE must submit necessary document issued by NSIC and the bidder who are Startups must be recognized by Department of Industrial Policy & Promotion (DIPP) to avail the exemption. To qualify for EMD exemption, firms should necessarily enclose a valid copy of registration certificate issued by NSIC/DIPP which are valid on last date of submission of the tender documents. MSE firms which are in the process of obtaining NSIC certificate/ DIPP will not be considered for EMD exemption.

Tender offers will normally be opened half an hour after the closing time. Any tender received without Document/Tender Cost (If required), will be disqualified.

Technical Specifications, Terms and Conditions and various format and Performa for submitting the tender offer are described in the tender document and its Annexures.

DISCLAIMER The information contained in this Request for Proposal (RFP) document or information conveyed subsequently to SI/Bidder(s) or applicants whether verbally or in documentary form by or on behalf of Central Bank of India (Bank), is provided to the SI/Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of unconditional bids. The purpose of this RFP is to provide the SI/Bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each SI/Bidder may require. Each SI/Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

1 Eligibility Criteria

The SI/Bidder must fulfil following eligibility criteria:

Sl. No	Eligibility	Documents to be submitted
1	SI should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the SI/Bidder
2	SI should be registered under G.S.T. and/or tax registration in state where SI has a registered office	Proof of registration with GSTIN
3	The SI should have had an annual turnover of at least INR 1,500 crores in each of the last three (3) financial years, i.e., FY 2022-23, FY 2023-24, and FY 2024-25. This must represent the turnover of the individual company and not that of any group of companies.	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding two FYs
4	The SI should have achieved a positive operating profit (as EBITDA, i.e., Earnings Before Interest, Tax, Depreciation, and Amortization) in at least two out of the last three financial years of operations, i.e., FY 2022-23, FY 2023-24, and FY 2024-25. Applicable provisions for start-ups will be applied.	Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FY
5	SI Capability The SI must have successfully implemented either a Data Lakehouse* / Data Lake** / Data Warehouse*** of minimum capacity of 100 TB on-premises , including archival and backup storage. The implementation must encompass Installation and Management of the Data Lakehouse / Data Lake/ Data Warehouse platform. This must have been executed for at least one BFSI sector, RBI, NSE, BSE, Central Government organisation like CBDT, GST, Income Tax etc in India.	Copy of Purchase Order ¹ and Completion certificate from Client OR Email Confirmation ¹ from the Client's executive. OR Any other document which suffices the requirement to the satisfaction of the Bank ¹ The start date of the referenced Project must be no earlier than five (5) years or if it is more than 5 years, then it should be ongoing project.

Sl. No	Eligibility	Documents to be submitted
6	SI capability The SI must have successfully operationalized, in a production environment, at least two (2) Generative AI (GenAI) and/or Agentic AI use cases. For the purpose of this requirement, 'operationalized in a production environment' refers to the deployment and active use of the use cases in a live, real-world setting, delivering measurable outcomes for the Client.	Copy of Purchase Order¹ and Completion certificate from Client OR Email Confirmation¹ from the Client's executive. OR Any other document which suffices the requirement to the satisfaction of the Bank ¹ The start date of the referenced Project must be no earlier than five (5) years
7.a	OEM capability The proposed Data Lakehouse technology (OEM) must have been implemented on client premises in India or Globally, with a minimum used capacity of 1 PB. For the purpose of this requirement, 'used capacity' refers to the actual amount of data stored and actively utilized in the production environment, excluding backup or archival storage The Data Lakehouse technology must support integration (including batch processing, streaming, change data capture (CDC), and messaging), medallion architecture, data access (via APIs etc) data consumption and operations	Certificate from the OEM
7.b	The proposed platform version must either possess in-built capabilities or the ability to integrate seamlessly with other enterprise tools to support the following functionalities: a. Data security, including encryption, access control, and data masking; b. Data governance and data quality, including metadata management, lineage tracking, and data validation; c. Storage security solutions d. Business intelligence, dashboards, and reporting.	Certificate from the OEM

Sl. No	Eligibility	Documents to be submitted
8	The SI must have a minimum of 500 personnel on its payroll in India , with expertise across areas such as Business Analytics (including banking domain specialists), Data Science, Data Lakehouse implementation, and other relevant fields, to provide services to the bank.	Undertaking on Company's letter head
9	The SI must be an authorized partner, service provider (SP), or system integrator (SI) of the Original Equipment Manufacturer (OEM) or Original Software Developer (OSD) in India of the Lakehouse Platform, with the authority to perform implementation, customization and upgrades during the contract period with the Bank.	Certificate from the OEM
10	The SI must be a CMMI Level 5 certified organization at least once in any of the last three years.	Undertaking on Company's letter head
11	SI/Bidder should not have been debarred / black-listed by any Bank or RBI or any other regulatory authority or Financial Institutions in India at the time of Bid submission.	Undertaking / self-declaration on Company's letter head
12	At the time of bidding, there must not have been any pending litigation or legal disputes in the last two (2) years between the SI or the Original Equipment Manufacturer (OEM) and the Bank, before any court of law, pertaining to the supply of goods or services.	Undertaking / self-declaration on Company's letter head
13	SI should not have a) NPA with any Bank /financial institutions in India. b) Any case pending or otherwise, with any organization across the globe which affects the credibility of the SI in the opinion of Central Bank of India to service the needs of the Bank.	Submit self-declaration on Company's letter head.

Sl. No	Eligibility	Documents to be submitted
14	If the SI is from a country that shares a land border with India, the SI must be registered with the Competent Authority, as per applicable regulations. The required approvals / NOCs / Clearances should be in place at the time of Bid submission.	Certified copy of the registration certificate

***Data Lakehouse** is Unified data platform that combines data lake scalability with data warehouse performance, supports ACID transactions, schema enforcement, and BI tools, and enables efficient storage, processing, and analytics of structured, semi-structured, and unstructured data within a single architecture

****Data Lake** is a scalable data platform that prioritizes cost-efficient storage and the ability to ingest data in its native format (structured, semi-structured, and unstructured). It enables flexible processing and analytics but lacks native support for ACID transactions and strong schema enforcement, typically resulting in lower performance for structured BI workloads compared to Data Warehouse.

*****Data Warehouse** is a highly organized data platform that prioritizes high performance for analytical queries over massive, raw data scalability. It mandates ACID transactions and rigorous schema enforcement (schema-on-write), enabling efficient storage, processing, and traditional BI tool integration exclusively for structured and highly modeled data within a purpose-built architecture.

The SI/Bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the SI/Bidder will be bound to provide the same.

Central Bank of India reserves the right to verify references provided by the SI/Bidder independently. Any decision of Bank in this regard shall be final, conclusive, and binding up on the SI/Bidder. Bank may accept or reject an offer without assigning any reason whatsoever.

- 1) SI/Bidders need to ensure compliance to all the eligibility criteria points.
- 2) In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
- 3) In case of business transfer where SI/Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
- 4) SI/Bidder must provide credential letter or installation sign off document.
- 5) Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.
- 6) While submitting the bid, the SI/Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I)

2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:

- i. *In RFP, either the Indian agent on behalf of the SI/Bidder/OEM or SI/Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that SI/Bidders will deliver to the customer.*
- ii. *If an agent submits the bid on behalf of the SI/Bidder /OEM, the same agent shall not submit a bid on behalf of another SI/Bidder /OEM in the same RFP for the same item/product.'*

2 Bid Security (Earnest Money Deposit-EMD)

An amount of **₹5,00,00,000/- (Rupees Five crore Only)** in the form of Bank Guarantee issued by a scheduled Bank other than Central Bank of India for the entire period of Bid validity (180 days) plus 3 months or by means of Account Payee Demand Draft/ Banker's cheque /RTGS/NEFT in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no **GEM/2026/B/7203650** in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai.

The EMD / Bid Security shall be liable to be forfeited:

- 1) If a SI/Bidder withdraws its tender during the period of tender validity (180 days) specified by the SI/Bidder; or
- 2) If the SI/Bidder does not accept the correction of its Tender Price; or-
- 3) If the successful SI/Bidder fails within the specified time to:
 - i. Sign the Contract; or
 - ii. Furnish the required security deposit.
- 4) The EMD / Bid Security of a Joint Venture (JV) must be in the name of the JV that submits the tender. If the JV has not been legally constituted at the time of bidding, the EMD / Bid Security shall be in the name of all future partners as named in the letter of intent.
- 5) The EMD / Bid Security will be refunded to the Successful SI/Bidder; only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG).
- 6) The EMD / Bid Security of unsuccessful SI/Bidders shall be returned as promptly as possible after completion of bidding process.

3 Performance Bank Guarantee (PBG)

- 1) As mentioned above, the Successful SI/Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given by the Bank in for Performance Bank Guarantee, for 5 % of the total project cost valid for 66 months, (5 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of the PO acceptance by the SI/Bidder.

- 2) The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the letter head of the issuing Bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents.
- 3) Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
- 4) In the event of the Successful SI/Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the SI/Bidder is unable to service the contract for whatever reason.
- 5) In the event of delays by Successful SI/Bidder in ATS support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
- 6) Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful SI/Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful SI/Bidder is in default.
- 7) The Bank shall also be entitled to make recoveries from the Successful SI/Bidder's bills or any other amount due to him, the equivalent value of any payment made to him by the Bank due to inadvertence, error, collusion, misconstruction or misstatement.
- 8) The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful SI/Bidder under the contract. However, no interest shall be payable on the PBG.

4 Cost of Bidding

The SI/Bidder shall bear all the costs associated with the preparation and submission of bid and Bank will in no case be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

5 Manufacturer's Authorization Form

SI/Bidders must submit a letter of authority from their manufacturers, as per format given in **Annexure 8**, that they have been authorized to quote OEM Product.

Section-2

Scope of Work

6 Scope of work for the SI

- Responsible for the design, size, supply, commission, implementation, migration (data assets, ETL pipelines, reports, applications etc) and operations of the solution in accordance with the project implementation plan and within the timelines as detailed in Section 8 titled, 'Project Timelines'.
- Support the Bank to enhance its internal expertise in intelligent systems, generative technologies, and autonomous agents.
- Core Principles Governing Engagement should be abiding - Complete Ownership (Design to Run), IP Ownership of the custom built software, scripts or any artefacts with the bank, Preferably vendor neutral technologies to be used, Integration of newer features should be easy, the designed solution should be configurable and extensible by design, As much as possible **Vendor Agnostic/ Open-source with Enterprise Support** first technology choices should be made, Security and Responsible **AI/GenAI/Agentic AI** models Built in to the solution, Knowledge Transfer and Capability Uplift approach with the banks internal teams must be part of the SI scope.

Wherever Open-Source Software is used it should be Enterprise class with back to back support from the OEM.

SI to submit MAF for all the components being supplied as a part of Data Lakehouse and AI Solution.

6.1 Project planning and management

- Develop a detailed project plan that outlines the timeline, milestones, resources, and budget requirements. Comprehensive Project Plan along with detailed sub milestones of implementation should be shared with the Bank during kick-off meeting post issuance of Purchase Order.
- Setup a Project Management Office headed by Project Director onsite to manage the project deliverables, timelines and governance cadence.
- Establish key performance indicators (KPIs) to measure the success of the implementation and create suitable Dashboards both figures as well as graphical to understand the trends.
- Ensure alignment with the bank's strategic objectives and regulatory requirements
- Coordinate with bank stakeholders to ensure project alignment with business objectives
- Manage project resources, including personnel, budget, and timelines
- Identify potential risks and develop mitigation strategies to address them
- Implement a risk management framework to monitor and manage risks throughout the project
- Collaborate closely with the Bank to ensure that the implementation strategy of the Platform remains closely aligned with the use case roadmap, adapting as needed.

6.2 Project Staffing

- Plan for resources to complete the project as per the timelines mentioned in the RFP document considering various dependencies on integrations with internal & external channels.
- The Bank suggests that the team size during peak phases should ideally fall between 40 and 50 members.
- The SI should ensure that **Architects and Subject Matter Experts of the Platform OEM are actively involved in the design phase and are available onsite** during this period. The SI must also ensure that the design is documented and **approved in writing by the Platform OEM Architect** assigned to the project. This entire activity, including the involvement of the OEM Architects and Subject Matter Experts (SME), must be provided at no additional cost to the Bank. The SI to obtain sign off from the **OEM Architect/Solution Designer/ SMEs after implementation and before deploying the Data Lakehouse platform and its related components to Production in DC & DRC.**
- The SI should allocate adequate personnel for the following key roles, based on the specific requirements of each phase of the project. If the SI in its own assessment finds requirement for any other domain experts, SMEs, technical resources, they may deploy to ensure the project is implemented within the timelines delivering intended objectives including Business outcomes.

Role	Description
Project Manager / Scrum Master (SM)	Oversee project delivery, resource allocation, and stakeholder communication. Ensure alignment with program objectives
Data Architect	Design the overall architecture, including data pipelines, storage, and AI, GenAI and Agentic AI model integration. Ensure scalability, security, and performance.
Data Migration Architect	Plan and oversee the migration of data , reports etc from existing DWH to Lakehouse, ensuring data integrity and consistency
BI Lead	Lead the BI team, ensuring alignment with program goals and delivery of required dashboards and reports, including AI-driven insights.
Business Analyst	Gather business requirements and translate them into technical specifications for the implementation team.
Data Engineer	Build and maintain data pipelines for ingestion, transformation, and storage in the Lakehouse
Data and MLOps Engineer	Operationalize machine learning and GenAI models, automating workflows for deployment, monitoring, and retraining.
API Developer	Develop APIs to integrate Lakehouse and AI/GenAI models with external systems, ensuring performance and scalability.

Role	Description
BI Developer	Create dashboards, reports, and visualizations, incorporating AI/GenAI-driven insights to provide actionable intelligence.
Data Scientist	Develop machine learning, Computer Vision, Neural and GenAI models for advanced analytics and business problem-solving, leveraging the Lakehouse data. AI/ML Engineer: Design, implement, and maintain production-grade machine learning services by engineering model pipelines, optimizing performance, and integrating ML models.
GenAI Engineer	Specialize in building, fine-tuning, and deploying GenAI models, such as large language models (SLM / LLMs),), RAG, Prompt engineering and context engineering for specific organizational use cases.
AIOps(LLMOps and AgentOps) Engineer	Operationalize LLM, RAG, and Agentic, Multi Agentic system automating workflows for deployment, monitoring, evaluation and AI observability. Responsible for end to end ops workflow.
AI Agentic Engineer	Specialize in building, maintaining, upgrading, validating AI agent and multi AI agent system for specific gen AI use case.
AI Validation Engineer	Specialize in validation and evaluation for ML, DL, genAI , RAG, Agent and multi agent system. Responsible for to ensure modal are aligned with AI governance with AI testing and validation strategies
QA Lead	Lead the QA team, defining testing strategies and ensuring the quality of the Lakehouse implementation, including AI/GenAI components.
QA Automation Engineers	Develop and execute automated test scripts to ensure the functionality, performance, and reliability of the Platform and models.
Platform Administrator	Manage the infrastructure hosting the Platform and models, ensuring system availability, performance, and security.
Security Lead Engineer	Ensure the overall security of the Platform and models by implementing and monitoring security protocols, policies, and controls.

6.3 Design and Architecture of Platform

Guiding Principles for Bank's target state platform based on open standards and modular architecture

6.3.1 Lakehouse Architecture

The proposed Data Platform shall be based on a Lakehouse architecture that unifies the scalability and cost efficiency of a data lake with the reliability, governance, and performance of a data warehouse. The architecture shall support enterprise-grade analytics, AI/ML, and Generative AI use cases across structured, semi-structured, and unstructured data.

a) Unified Data Storage and Processing

The platform shall provide a single, unified data layer capable of storing and processing diverse data types, including transactional data, logs, documents, images, audio, and video, without requiring multiple isolated systems.

b) Data Consistency and Reliability

The Lakehouse shall support for ACID transactional data operations to ensure data consistency, integrity, and reliability for analytical, reporting, and AI workloads, especially for regulatory and risk-sensitive use cases.

c) Schema Management and Evolution

The platform shall enable controlled schema enforcement with the ability to evolve schemas over time, supporting changing business requirements while ensuring data quality and backward compatibility.

d) Data Versioning and Recovery

The solution shall provide data versioning capabilities, enabling access to historical versions of data for audit, analysis, reconciliation, and recovery purposes, including rollback where required.

e) Support for Multiple Data Modalities

The architecture shall natively support multi-modal data, including structured, semi-structured, and unstructured formats, to enable advanced analytics, AI/ML, and GenAI use cases.

f) Performance Optimization

The platform shall support data partitioning, indexing, and optimization techniques to ensure efficient query performance on large-scale datasets used for reporting, analytics, and AI workloads.

g) Batch and Real-Time Processing

The Lakehouse architecture shall support both batch and near real-time data ingestion and processing, enabling use cases such as operational reporting, fraud monitoring, and event-driven analytics.

h) BI and Analytics Tool Integration

The platform shall be compatible with industry-standard BI and analytics tools, enabling secure and performant access for dashboards, reports, and ad-hoc analysis.

i) Data Lifecycle Management

The solution shall include automated data lifecycle management, covering data retention, archival, and purging policies in line with regulatory, audit, and internal data governance requirements.

j) Open Standards and Interoperability

The Lakehouse shall be built using open standards and interoperable technologies, ensuring seamless integration with existing enterprise systems and future extensibility, while avoiding vendor lock-in.

- **Modular and Scalable Architecture**
 - **Microservices- Based Design:** Architect the platform using microservices to enable modularity, scalability, and independent deployment of components.
 - **Elastic or Dynamic Scaling:** Design the platform for elastic or dynamic scaling of resources (e.g. compute, storage, and processing resources) within the available on-premises infrastructure, enabling efficient resource utilization and workload-based scaling without service disruption based on workload demands.
 - **Event-Driven Architecture:** Incorporate event-driven patterns to support real-time data processing and analytics use cases.
 - **Layered Architecture:** Separate the platform into distinct layers for data ingestion, processing, storage, analytics, and AI workloads.
 - **Distributed Processing Frameworks:** Leverage distributed processing technologies for handling large-scale data and AI workloads.
 - **Containerization and Orchestration:** Enable containerization and orchestration for flexible deployment and scaling.
- SI must submit and maintain complete Target Architecture with HLD, LLD, deployment diagrams, data flow diagrams, component interaction diagrams, Security architecture, DR architecture

6.3.2 **Accelerators**

- **Use Case Accelerators:** Provide reusable accelerators or reference implementations for common analytics and AI use cases, such as fraud detection, customer segmentation, and predictive maintenance.
- **Data Pipeline Accelerators:** Offer re-usable templates or configurable patterns for data ingestion, transformation, and processing pipelines for batch and streaming data.
- **AI/ML Model Archetypes:** Include archetypes for common AI/ML models (e.g., classification, regression, clustering) with pre-configured hyperparameters.
- **Analytics Dashboard Templates:** Deliver pre-designed dashboards for key business metrics, enabling faster insights and decision-making.

- Integration Blueprints: Provide blueprints for integrating with third-party systems (e.g., CRM, ERP, cloud services) and APIs.
- MLOps Accelerators: Provide reusable workflows or templates supporting end-to-end ML lifecycle management, including training, validation, deployment, monitoring, and retraining, without mandating any specific tool or framework.

6.3.3 **AI, GenAI, and Agentic AI Enablement**

- AI/ML Experimentation Framework: Provide tools for rapid experimentation with AI/ML models, including automated hyperparameter tuning and model selection. The framework should also support tracking and comparing experiments, including data versions, parameters, and results to maintain consistency across repeated experiments.
- Pre-Trained Models: Include a library of pre-trained AI/ML models (e.g., NLP models, vision models, generative models) that can be fine-tuned for specific use cases.
- Generative AI Capabilities: Enable multi-lingual text generation, audio generation, image synthesis, video generation, and other GenAI functionalities.
- Agentic AI Framework: Provide a framework for building autonomous agents capable of decision-making and task execution.
- Feature Store: Implement a centralized feature store for storing, sharing, and reusing features across AI/ML models.
- Explainable AI (XAI): Ensure models are explainable and auditable to meet ethical AI standards and regulatory requirements.
- Natural Language Querying: Enable users to query data using natural language for faster insights.

6.3.4 **Advanced Analytics Capabilities**

- Self-Service Analytics: Enable business users to access and analyse data independently through intuitive, drag-and-drop interfaces.
- Real-Time Analytics: Provide capabilities for real-time analytics and event-driven insights to support time-sensitive decision-making
- Advanced Data Visualization: Include support for heatmaps, and interactive dashboards.
- Natural Language Processing: Analyse, understand, and generate human language from text or speech for insights, automation, and intelligent interactions.
- Multi-Dimensional Analysis: Provide OLAP (Online Analytical Processing) capabilities for slicing and dicing data.

6.3.5 **Rapid Onboarding Framework**

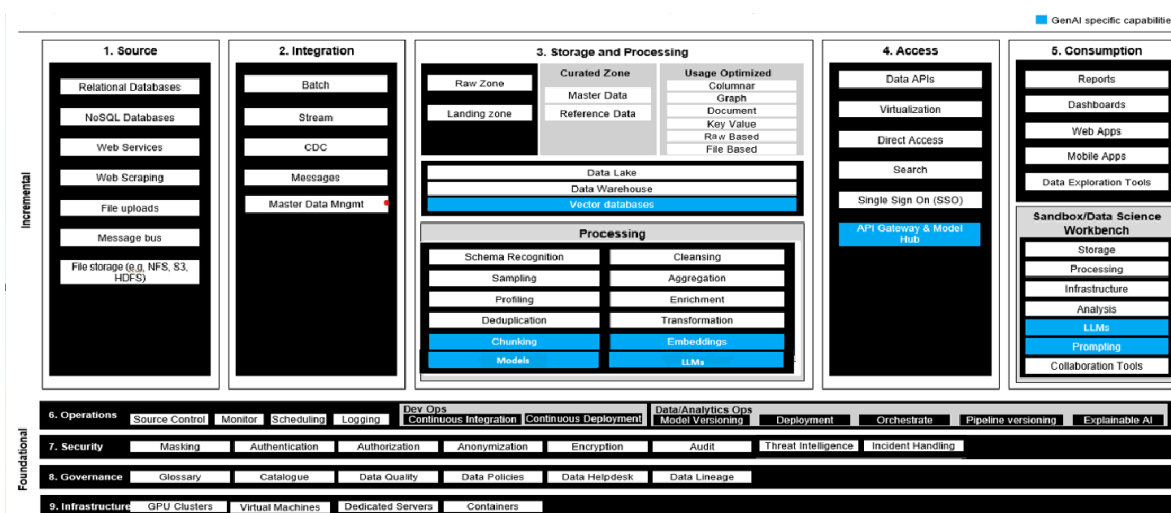
- Onboarding Playbooks: Develop detailed playbooks for onboarding new analytics and AI use cases, including step-by-step guides and best practices.
- Pre-Built Connectors: Offer pre-built connectors for commonly used data sources, analytics tools, and AI frameworks.
- Innovation Sandbox: Provide a sandbox environment for experimenting with new tools, technologies, and methodologies before production deployment.

6.3.6 Future-Ready Design

- Support for Emerging Technologies: Ensure the platform can integrate with emerging technologies like quantum computing, edge AI, and federated learning.
- Interoperability with Open Standards: Build the platform on open standards to ensure compatibility with future tools and frameworks.
- Continuous Improvement Mechanisms: Implement feedback loops and automated upgrades to ensure the platform evolves with business needs.

6.4 Target State Platform Capabilities

The Platform should be developed with a layered approach with a collection of capabilities to enable Insights and Intelligent Automation.



The SI will be responsible for enabling the following capabilities in the Platform.

6.4.1 Sources

- Ingestion pipelines for multi-modal data (text, images, audio, video, QR code, etc.).
- Implement Connectors for diverse data sources with appropriate approval (APIs, databases, IoT devices, etc.).
- Pre-process and normalize data into consistent formats for downstream use.
- Enable metadata extraction and tagging for better organization and retrieval.
- Integrate with storage systems optimized for multi-modal data (e.g., object stores, vector databases).
- Ensure real-time and batch ingestion capabilities for dynamic workloads.
- Monitor data ingestion performance and handle errors gracefully.
- Secured end to end data journey for data pipeline with encryption and access controls.
- Adhere to governance, compliance, and data privacy standards.

6.4.2 Integration

6.4.2.1 Batch

- Facilitate the periodic ingestion of large volumes of data from various sources, such as relational databases, files, or APIs, into the data lakehouse.
- Ensure reliability, scalability, and fault tolerance during ingestion processes.
- Import data from relational databases into Storage layer of the Lakehouse
- Design and automate batch ingestion workflows from diverse data sources.
- Store ingested batch data in a distributed and fault-tolerant manner.
- Manage and monitor batch ingestion pipelines.
- Stage data before batch ingestion, if required.

6.4.2.2 Stream

- Support real-time ingestion of high-velocity data streams from sources like logs, and streaming systems.
- Ensure low-latency processing, scalability, and fault tolerance for continuous data flow into the Lakehouse.
- Real-time data streaming and message queuing.
- Stateful stream processing and real-time analytics.
- Orchestrate and manage streaming data pipelines.
- Scalable and fault-tolerant stream processing.
- End-to-end management and monitoring of streaming data ingestion workflows.

6.4.2.3 Change Data Capture

- Enable real-time or near-real-time ingestion of incremental changes (inserts, updates, deletes) from source systems into the Lakehouse.
- Ensure low-latency processing, data consistency, scalability, fault tolerant irrespective of changes in source and to reduce the need for full/Partial data reloads.
- Integrate CDC connectors and orchestrate CDC pipelines.
- Manage and monitor CDC-based ingestion workflows.
- Capture database changes and stream them to downstream systems.
- Buffer and stream CDC events in real time.
- Process and apply CDC events to the target lake house.
- The platform shall ensure 100% consistency & integrity for all data. Any inconsistency or integrity issue reported must be remediated immediately. Any loss incurred to the Bank on account of this will be recovered from the SI.

6.4.2.4 Messages

- Facilitate ingestion of data from message-based systems (e.g., message queues or pub/sub systems) into the lake house.
- Ensure low-latency, reliable, and scalable processing of messages for real-time or near-real-time analytics.
- Ingest and stream messages from distributed systems.

- Design and manage message ingestion pipelines.
- Orchestrate and monitor message-based ingestion workflows.
- Process and transform message streams in real time.
- Scalable and fault-tolerant processing of message streams.

6.4.2.5 Master Data Management

- Facilitate the ingestion of clean, consistent, and de-duplicated master data from source systems into the lake house.
- Ensure data integrity, standardization, and integration of master data for downstream analytics and operations.
- Batch ingestion of master data from relational source systems.
- Store ingested master data in a scalable and fault-tolerant manner.
- Metadata management and governance of master data.
- The platform shall ensure 100% consistency & integrity for all data. Any inconsistency or integrity issue reported must be remediated immediately. Any loss incurred to the Bank on account of this will be recovered from the SI.

6.4.3 Storage and Processing

6.4.3.1 Landing Zone

- Serve as a transient storage area where raw data from various sources is initially ingested before further processing.
 - Ensures data is captured in its original format, supports multiple ingestion methods (batch, streaming, CDC), and provides a staging area for validation and transformation.
 - Store raw ingested data temporarily in a distributed and scalable manner.
 - Manage and monitoring ingestion pipelines.
- Secure access and enforcement of data governance policies in the Landing Zone.

6.4.3.2 Raw Zone

- Store data in its original, unprocessed format as ingested from source systems.
- Ensure immutability, scalability, and fault tolerance, serving as a single source of truth for downstream processing and analytics
- Distributed, scalable, and fault-tolerant storage of raw data.
- Manage and monitor data pipelines feeding into the Raw Zone.
- Secure access and enforce data governance policies in the Raw Zone.

6.4.3.3 Curated Zone

6.4.3.3.1 Master

- Store cleansed, enriched, and standardized master data that is ready for consumption by downstream analytics, reporting, and applications.
- Ensure data consistency, deduplication, and alignment with business rules and governance policies.
- Scalable and fault-tolerant storage of curated master data.
- Create structured, query able datasets for master data.

- Data transformation, deduplication, and enrichment processes.
- Automatic Metadata management and lineage tracking of master data.
- Secure access and enforcing governance policies on curated datasets.

6.4.3.3.2 Reference Data

- Provide a centralized, consistent, and version-controlled repository for reference data.
- Ensure high availability, scalability, and efficient querying for downstream applications.
- Distributed storage for scalability and fault tolerance.
- SQL-based querying and metadata management.
- Low-latency access for key-value lookups.
- Metadata governance and lineage tracking.
- Security and access control for data governance.

6.4.3.4 Usage Optimized

6.4.3.4.1 Columnar

- Layered storage for data in-line with Access and store to optimize performance and capacity.
- Optimized for analytical workloads with columnar storage formats, enabling faster query performance.
- Support efficient compression, predicate pushdown, and parallel processing for large-scale data analysis
- Columnar storage format for efficient analytics and compression.
- Optimized Row Columnar format for high-performance queries.
- SQL-based querying and analytics over columnar formats.
- Distributed processing engine for transforming and querying columnar data.
- Underlying storage layer for scalability and fault tolerance.

6.4.3.4.2 Graph

- Enable the storage, processing, and querying of graph-structured data for use cases like network analysis, relationship modelling, and recommendation systems.
- Support efficient traversal, pathfinding, and graph algorithms for large-scale datasets.
- Key-value store to manage graph data with adjacency lists.
- Metadata management and lineage tracking for graph data.
- Distributed graph processing and analytics.
- Graph database for scalable and transactional graph queries.
- Underlying storage for scalability and fault tolerance of graph data.

6.4.3.4.3 Document

- Facilitate the storage, indexing, and querying of semi-structured or unstructured document data (e.g., JSON, XML).
- Support schema-on-read, enabling flexible data exploration and analytics on document-based data.
- Full-text search and indexing for document data.
- Storage for semi-structured document data with low-latency access.
- SQL-based querying of document data using JSON or XML SerDes.
- Distributed processing for transforming and analysing document data.
- Underlying storage for scalability and fault tolerance of document data.

6.4.3.4.4 Key Value

- Provide low-latency storage and retrieval for key-value pairs, enabling fast lookups and updates.
- Support use cases such as session management, caching, and real-time applications requiring high throughput.
- Distributed, scalable key-value store for low-latency access.
- SQL layer on top of key-value store for querying key-value data.
- Underlying storage for durability and scalability.
- Process and transform key-value data at scale.
- Security and access control for key-value data.

6.4.3.4.5 Raw Based

- Provide a storage layer for raw, unprocessed data in its native format (e.g., JSON, CSV, Avro, Parquet).
- Enable schema-on-read capabilities for flexible data exploration and supports downstream transformations and processing.
- Scalable and fault-tolerant storage for raw data.
- Schema-on-read querying of raw data.
- Distributed processing for transforming raw data into curated formats.
- Data ingestion and flow management for raw data pipelines.
- Security and access control for raw data storage.

6.4.3.4.6 File based

- Enable the storage and processing of file-based data (e.g., CSV, JSON, XML, Avro, Parquet) in a distributed and scalable manner.
- Support schema-on-read, compression, and efficient querying for file-based datasets.
- Distributed storage for file-based data with scalability and fault tolerance.
- Schema-on-read querying for file-based data.
- High-performance SQL queries on file-based datasets.
- Distributed processing and transformation of file-based data.
- Security and access control for file-based data.

6.4.3.5 Data Lakehouse Capabilities

A Data Lakehouse is a modern data architecture that features a fully decoupled storage-compute model using scalable storage, open file formats (e.g., Parquet, ORC), and open table formats to deliver ACID transactions, with query engines and processing clusters scaling independently. It supports structured, semi-structured, and unstructured data along with governance for metadata, access control, lineage, and compliance.

The Data Lakehouse platform must have the below capabilities:

1. Data Lake

- Act as a centralized repository for storing structured, semi-structured, and unstructured data at scale.
- Support schema-on-read, enabling flexibility for data exploration and downstream processing. Provides scalability, fault tolerance, and integration with various processing and analytics tools.
- Core distributed storage layer for scalability and fault tolerance.
- Metadata management and SQL querying over data stored in the lake.
- Distributed processing for data transformations and analytics.
- Data ingestion and flow management into the data lake.
- Security and access control for data governance.

2. Data Warehouse

- Provide a structured and optimized environment for analytical queries and reporting on curated data.
- Support ACID transactions, indexing, and performance optimizations like partitioning and bucketing for large-scale analytics.
- Integrate seamlessly with BI tools for enterprise reporting and dashboards.
- Data warehouse infrastructure with SQL-based querying and metadata management.
- High-performance, low-latency SQL engine for interactive analytics.
- Support OLAP-style queries on structured data.
- Distributed query engine for processing structured data.
- Security and governance for data access in the warehouse.

6.4.3.6 Vector Database

- Support the storage, indexing, and querying of high-dimensional vector data for multiple use cases, including analytics and AI.
- Enable efficient nearest-neighbour, hybrid, time-weighted, metadata-aware, and vector-based analytics on large datasets.
- Scalable storage for vector data with custom indexing.
- Index and search vector representations.
- Generate and processing vector embeddings.
- Build and deploy machine learning models that generate vector data.
- Secure role-based access with integration to Bank's Active Directory for AuthN and multifactor authentication to vector data.

6.4.3.7 Agentic Orchestration & Reasoning Layer

- Design agent lifecycle management (creation, activation, scheduling, termination).
- Workflows for multi-agent coordination and task execution.
- Integration with real-time and batch data pipelines.
- Reasoning logic using AI/ML or rule-based systems.
- Event-driven triggers for agent activation.
- Optimize agent performance and resource utilization.
- Error handling, recovery, and context awareness.
- Connection to knowledge graphs for semantic understanding.
- Ensure scalability, interoperability, and security (e.g., RBAC).
- Monitoring tools and feedback loops for continuous improvement.
- Solution to provide adherence to governance and compliance policies.

6.4.3.8 Agentic Long-Term Memory

- Configured embedding generation from agent interactions and contextual data.
- Efficient similarity search for memory retrieval based on relevance.
- Memory schemas to organize and manage long-term knowledge.
- Memory updates for adding, modifying, or forgetting information.
- Memory retrieval with agent workflows for context-aware decision-making.
- Optimized storage and retrieval performance for scalability.
- Secure memory data with encryption and access controls.
- Monitoring of memory usage and refine retrieval strategies for accuracy.
- Compliance with governance and data privacy regulations.
- Provide Centralized Vector Memory & Retrieval System to store embeddings for documents, chat history, KYC data, operational knowledge, and customer cases, enabling all AI systems (GenAI agents, chatbots etc.) to perform accurate and context-aware information retrieval from a unified vector repository.

6.4.4 Access

6.4.4.1 Data APIs

- Provide programmatic access to data in the lakehouse through RESTful APIs, enabling integration with external applications and services.
- Support secure and scalable data access with fine-grained controls for different user roles and use cases.
- Gateway for secure API access to Platform services.
- Metadata and lineage APIs for data discovery and governance.
- APIs for orchestrating and accessing data pipelines.
- SQL-based programmatic access to structured data.
- API-level access control and security enforcement.

6.4.4.2 Agentic API and Agentic API Catalogue

- Implement an Agentic API Framework for interoperability and governance.
- Provide Agentic Category and Agentic catalogue APIs for use cases such as research, compliance, analytics, and automation.

- Ensure context-aware execution, safe multi-agent communication, and access control.
- Include observability hooks and metadata for every API call.
- Maintain API version control and integration documentation
- Maintain API version control, integration, and documentation using state of the art, tool based API management practices to ensure consistency, traceability, and controlled updates.

6.4.4.3 Prompt Management & RAG Pipeline

- Design and version prompts for AI workflows.
- Optimize RAG pipelines with vector databases and embeddings.
- Standardized prompts and retrieval strategies for relevance and accuracy.
- Integration with AI models and external knowledge sources.
- Ability to monitor and improve pipeline performance through feedback loops.
- Secure data and compliance with governance policies.
- Design and version prompts for AI workflows by implementing a centralized prompt management system that enables the bank to securely create, store, version, test, and govern all AI/LLM system prompts used across departments and users.

6.4.4.4 Direct Access

- Enable users and applications to directly access data stored in the lakehouse using SQL, APIs, or file-based protocols.
- Support high-performance, low-latency access to structured, semi-structured, and unstructured data for analytics, machine learning, and reporting.
- High-performance SQL engine for direct querying of structured data.
- SQL-based access to data with schema-on-read capabilities.
- Direct file-based access to raw and processed data.
- Programmatic access to data for distributed processing and analytics.
- Security and governance for direct data access.

6.4.4.5 Data Virtualization and Data Federation Capabilities

- Queries must be executed across multiple sources like Lakehouse Storage, Database, Streaming Platform, File Based Storage, REST/API-based data sources in a single logical query
- Creation of virtual views across one or more source systems
- Logical data modelling independent of physical storage
- Reusable and shareable virtual datasets
- Versioning of virtual views
- Performance optimization through Result catching, partial or full materialization, adaptive, query execution, Intelligent query pushdown
- Unified schema representation across sources
- Enforce security at virtualization layer using RBAC, Row level and column level security, Integration with AD/SSO. Secure credentials management for source systems
- Isolate workloads to avoid impacting source systems

- Scale independently of storage, support high concurrency
- Monitoring of virtual query performance, resource utilization tracking, administrative controls for virtual datasets

6.4.4.6 Search

- Provide the ability to index, search, and retrieve data stored in the lakehouse using keyword-based or full-text search capabilities.
- Support fast and scalable search across structured, semi-structured, and unstructured data for data discovery and analytics.
- Distributed search engine for indexing and querying data.
- Metadata search and discovery for data governance.
- Integration with distributed search engine for indexing file-based data.
- Manage data pipelines that prepare data for search indexing.
- Secure and access control for search operations.

6.4.4.7 Single Sign On

- Enable seamless and secure access to the data lakehouse by integrating with Bank's enterprise identity management systems/SSO.

6.4.4.8 API Gateway and Model Hub

- Allow secure and scalable access to data and machine learning models through APIs, enabling integration with external systems and applications.
- Provide a centralized hub for managing, deploying, and monitoring machine learning models, ensuring version control and governance.
- API gateway for secure access to Platform services and data.
- Manage and deploy machine learning models.
- Build and operationalize models with API endpoints.
- Secure API access to data and models.
- Metadata and lineage tracking for APIs and deployed models.

6.4.4.9 Tool Interface & Agent API Registry

- APIs for seamless interaction between tools and agents.
- A centralized registry for managing agent APIs and tool integrations.
- API versioning and backward compatibility for smooth updates.
- Dynamic discovery of APIs and tools for agents.
- Authentication and authorization for secure API access.
- Standardized API communication protocols.
- Integration with external tools, platforms, and third-party services.
- Monitoring of API usage and performance with observability tools.
- Automated API documentation generation for ease of use.

6.4.5 Consumption

6.4.5.1 Reports

- Enable the generation of interactive and static reports from data stored in the lakehouse, supporting business intelligence and decision-making.
- Provide integration with reporting tools for visualizing structured and semi-structured data, with support for real-time and batch reporting.
- SQL-based querying and reporting on structured data.
- High-performance SQL engine for real-time reporting.
- Batch reporting and querying large datasets.
- Integration with BI Tools for report generation and visualization.
- Secure access to reporting data and ensuring compliance.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle.

6.4.5.2 Dashboard

- Provide real-time and interactive visualizations of data stored in the lake house, enabling monitoring, trend analysis, and decision-making.
- Integrate with BI and analytics tools to create dashboards that aggregate data from structured, semi-structured, and unstructured sources.
- SQL-based querying and reporting on structured data.
- High-performance SQL engine for real-time reporting.
- Batch reporting and querying large datasets.
- Integration with BI Tools for report generation and visualization.
- Secure access to reporting data and ensuring compliance.
- Metadata management and lineage tracking of dashboard data.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle

6.4.5.3 Web App

- Enable custom web applications to consume and visualize data from the lake house via APIs or direct queries.
- Support integration with real-time and batch data pipelines, providing tailored interfaces for specific business use cases.
- Secure gateway for API-based access to lake house data for web applications.
- Query structured data to feed web applications.
- High-performance SQL engine for real-time data access by web applications.
- Process and deliver data to web applications via APIs.
- Secure and govern access to data consumed by web applications.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle

6.4.5.4 Mobile App

- Enable mobile applications to securely access and consume data from the lake house through APIs or direct integrations.

- Support real-time and batch data delivery to mobile apps, enabling interactive visualizations, notifications, and decision-making on the go.
- Secure API gateway for mobile app access to lake house data.
- Query structured data to serve mobile app needs.
- High-performance SQL engine for real-time data access by mobile apps.
- Process and deliver data to mobile apps via APIs.
- Secure and govern access to data consumed by mobile apps.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle

6.4.5.5 Multi Modal Outputs

- Output pipelines for delivering multi-modal content (text, images, audio, video, etc.).
- APIs and interfaces for seamless access to multi-modal outputs.
- Outputs for compatibility with various platforms and devices.
- Personalization and contextual adaptation of outputs for end-users.
- Integration with visualization tools for presenting complex data (e.g., dashboards, charts).
- Optimized delivery for real-time and batch use cases.
- Monitoring of output performance and user interactions for continuous improvement.
- Secured output channels with encryption and access controls.
- Compliance with accessibility, governance, and data privacy standards.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle

6.4.5.6 Data Exploration Tools

- Provide tools for interactive exploration of structured, semi-structured, and unstructured data stored in the lake house.
- Support SQL-based querying, data profiling, and visualization to enable analysts and data scientists to derive insights quickly.
- SQL-based exploration of structured data.
- Web-based interface for querying and exploring data using SQL and other tools.
- High-performance SQL engine for interactive queries.
- Advanced exploration of large datasets using Python, R, or Scala.
- Metadata-driven exploration and lineage tracking.
- In case of any backend manual changes in data, time should be consistent throughout the Data life cycle

6.4.5.7 Sandbox / Data Science Workbench

- Provide a secure, isolated environment for data scientists to experiment, build, and test machine learning models and analytics workflows.
- Support integration with the lake house for accessing data, running distributed computations, and deploying models seamlessly.

- Build, train, and deploy machine learning models in a collaborative environment.
- Distributed data processing and advanced analytics.
- Interactive data exploration and model development.
- Secure access to data and resources within the workbench.
- Track metadata and lineage of experiments and models.

6.4.5.7.1 Storage

- Provide scalable, high-performance storage for data scientists to store intermediate datasets, experiment outputs, and model artifacts.
- Support integration with the lake house storage layer to enable seamless access to raw and processed data for analytics and experimentation.
- Store large datasets and intermediate files.
- Scalable object storage to manage unstructured and semi-structured data.
- Store experiment-specific artifacts and outputs.
- Structured storage and querying of datasets.
- Secure and governing access to storage resources.

6.4.5.7.2 Processing

- Provide a scalable and distributed processing environment for data scientists to perform advanced analytics, machine learning, and data transformations.
- Support multiple programming languages (e.g., Python, R, Scala) and frameworks for experimentation and model development.
- Distributed data processing and machine learning workflows.
- Run interactive sessions and batch jobs in isolated environments.
- SQL-based data processing and querying.
- Deep learning and advanced machine learning model training.
- Secure and govern processing activities.

6.4.5.7.3 Infrastructure

- Provide a robust and scalable infrastructure to support isolated, resource-intensive data science workloads.
- Ensure resource allocation, monitoring, and management for sandbox environments to optimize performance and cost efficiency.
- Provision, monitor, and manage infrastructure resources.
- Container orchestration and resource isolation within the sandbox.
- Resource management and scheduling of distributed workloads.
- Manage compute resources for data science experiments.
- Monitor infrastructure performance and resource utilization.

6.4.5.7.4 Analysis

- Facilitate advanced data analysis, statistical modelling, and machine learning experimentation in an isolated, secure environment.

- Support integration with the lake house for seamless access to datasets and provides tools for interactive and batch analysis workflows.
- Collaborative data analysis and model development.
- Distributed data analysis and machine learning.
- Interactive exploratory data analysis using Python, R, or Scala.
- Statistical computing and visualization within the sandbox.
- Query and analyse structured datasets.

6.4.5.7.5 SLM / LLM

- Enable data scientists to experiment with, fine-tune, and deploy large language models (SLM / LLMs) for NLP tasks such as text generation, summarization, and sentiment analysis.
- Provide infrastructure and tools for handling the computational and storage demands of SLM / LLMs, with seamless access to lake house datasets for training and inference.
- Manage SLM / LLM experimentation, fine-tuning, and deployment.
- Distributed processing of large datasets used in SLM / LLM training and inference.
- Handle high computational demands of SLM / LLM training and inference.
- Secure access to sensitive datasets used in SLM / LLM workflows.

6.4.5.7.6 Prompting

- Provide an environment for experimenting with and optimizing prompts for Large Language Models (SLM / LLMs) to improve accuracy and relevance in NLP tasks.
- Support iterative testing of prompts with real-time feedback and integration with SLM / LLM APIs or fine-tuned models hosted within the lake house infrastructure.
- Interactive experimentation with prompts and SLM / LLMs.
- Test and iterate on prompt designs using Python-based SLM / LLM libraries
- Develop prompt evaluation system to systematically measure and monitor the reliability, hallucination rate, relevance, bias, and overall performance of prompts used across pre-trained and custom-trained SLM/LLM systems.
- Distributed processing of prompt datasets and evaluation results.
- Secure access to sensitive data used in prompt engineering workflows.

6.4.5.7.7 Collaboration Tools

- Facilitate seamless collaboration among data scientists, analysts, and engineers by providing shared environments for code, notebooks, and experiment tracking.
- Support version control, real-time collaboration, and sharing of insights, models, and results within the sandbox environment.

- Collaborative development, experiment tracking, and sharing of notebooks and results.
- Version control and collaborative code development.
- Shared, interactive analysis and visualization.
- Metadata management and lineage tracking of shared datasets and models.
- Real-time communication and updates.

6.4.6 Operations

6.4.6.1 Source Control

- Enables version control for code, configuration files, and scripts used in the data lake house environment, ensuring traceability and rollback capabilities.
- Facilitates collaborative development and deployment workflows, including integration with CI/CD pipelines for automated testing and deployment.
- Version control of code, scripts, and configuration files.
- Host repositories and enabling collaborative workflows.
- Integrate source control with CI/CD pipelines.
- Build and dependency management.
- Secure access to source control repositories and enforce policies.

6.4.6.2 Monitor

- Provide real-time monitoring and alerting for the health, performance, and availability of the data lake house infrastructure and workloads.
- Enable proactive identification and resolution of issues through centralized dashboards, log analysis, and automated alerts.
- Monitor and manage the Platform ecosystem components.
- Real-time metrics collection, visualization, and alerting.
- Centralized log aggregation and analysis.
- Monitor and manage the Platform clusters (if applicable).
- Infrastructure-level monitoring and alerting.

6.4.6.3 Scheduling

- Automate the execution of data pipelines, workflows, and recurring tasks to ensure timely data processing and availability.
- Support dependency management, retries, and notifications to handle complex workflows and ensure reliability.
- Workflow orchestration and scheduling in the Platform ecosystem.
- Advanced workflow orchestration, scheduling, and monitoring.
- Schedule and manage operational tasks within the Platform ecosystem.

- Lightweight scheduling of simple, recurring tasks.
- Resource-aware scheduling of Platform jobs.

6.4.6.4 Logging

- Provide centralized logging for capturing, storing, and analysing logs generated by various components of the data lake house.
- Enable efficient troubleshooting, auditability, and monitoring of system activities and data workflows.
- Collect and manage logs from Platform components.
- Logs must be tamper-proof, time-stamped, and digitally signed.
- Support traceability, rollback, and lineage visualization.
- Logs should be exportable for audit and governance reviews.
- Centralized log aggregation, indexing, and visualization.
- Ingest log data into storage or analysis systems.
- Stream log data in real-time for analysis and storage.
- Audit and secure access to log data.
- Retention periods for logs and metrics shall be defined in compliance with audit and regulatory requirements.

6.4.6.5 Observability

- Monitoring & alerting across all layers — infrastructure, network, storage, and computing resources.
- Data Observability for Movement of data between various layers including AI models.
- Collect and visualize real-time data including GPU usage, memory throughput, network performance with configurable alerts and dashboard for anomaly detection and failure tracking
- Collect and visualize real-time data for Data pipeline latency, data quality, response consistency, model latency, streaming jobs and job execution details, with configurable alerts and dashboard for anomaly detection and failure tracking.
- Tracing capabilities to follow data across services and components, supporting easy troubleshooting and performance tuning. Also, Track inference-level telemetry (confidence, hallucination, and drift metrics).
- Scalable with workload growth (supporting more than 100 use cases) and provide sufficient long-term storage for logs and metrics to support audit and compliance requirements.

SI/Bidder to bring in the required observability tools and integrate with the platform.

6.4.6.6 DevOps

6.4.6.6.1 Continuous Integration

- Enable automated continuous integration of code changes into a shared repository, with automated build and testing workflows to validate changes early, detect integration issues, improve code quality, and accelerate the overall development lifecycle.
- Integrated version control and continuous integration pipelines.
- Build and dependency management.
- Static code analysis and quality checks.
- Integrating DevSecOps into Continuous Integration ensures that code and artefacts are automatically scanned for security vulnerabilities and compliance issues before they progress further in the delivery pipeline.
- Implement audit logging and role-based access control (RBAC) within Continuous Integration pipelines to provide end-to-end traceability, accountability, and compliance for code changes, build executions, approvals, and user activities.

6.4.6.6.2 Continuous Deployment

- Automate the deployment of tested and validated code, configurations, and artefacts into production or staging environments.
- Ensure consistent, repeatable, and error-free deployments while supporting rollback mechanisms for stability.
- Manage and deploy Platform components.
- Management of Configuration, Containerized deployments and orchestration
- Implement approval gates and environment segregation (DEV, UAT, PROD) in Continuous Deployment to ensure controlled, validated, and authorized production releases.
- Enable automated rollback mechanisms and disaster recovery-ready deployment strategies, including versioned artefacts and configurations, to quickly restore services in case of deployment failures.

6.4.6.7 Data / Analytics Ops

6.4.6.7.1 Model Versioning

- Enable tracking, managing, and versioning of machine learning (ML) models and associated metadata throughout their lifecycle.
- Facilitate reproducibility, rollback, and deployment of specific model versions for consistency and operational reliability.
- Metadata management and lineage tracking of models.
- Version control of model code and configuration files.
- Containerize and deploy specific model versions.

- Implement approval-based promotion of machine learning models across environments with documented governance, version control, and rollback capabilities.

6.4.6.7.2 Deployment

- Facilitate the deployment of machine learning (ML) models into production environments for real-time or batch inference.
- Ensure scalability, monitoring, and governance of deployed models to support business-critical analytics operations.
- Manage model deployment workflows and serving models.
- Containerize and orchestrate model deployments.
- Real-time data streaming with High Throughput and Low Latency and inference integration.
- Scalable Stream Processing
- Integration with Data Lakehouse to manage both raw streaming data and processed outputs, supporting batch and micro-batch analytics
- Enable continuous monitoring of deployed ML models for performance, accuracy, data drift, and resource utilization, with alerting mechanisms for anomalies.
- Ensure secure and compliant model deployment by implementing strong access controls, encryption, audit logging, and controlled deployment mechanisms to prevent unauthorized changes or misuse of deployed AI/ML models.

6.4.6.7.3 Orchestration

- Manage and automate complex workflows and dependencies across data pipelines, analytics processes, and machine learning operations.
- Ensure efficient execution, error handling, and monitoring of tasks in a unified and scalable manner.
- Workflow orchestration and scheduling of data and analytics pipelines.
- Data flow orchestration and real-time streaming workflows.
- Orchestrate containerized analytics and ML workloads.
- Provide centralized monitoring, retry mechanisms, timeout handling, and alerting for orchestrated data and analytics workflows.

6.4.6.7.4 Pipeline Versioning

- Enable tracking, managing, and versioning of data and analytics pipelines to ensure reproducibility, traceability, and rollback capabilities.
- Support collaboration and governance by maintaining a history of pipeline changes and associated metadata.
- Version control of pipeline code, configurations, and scripts.
- Metadata management and lineage tracking of pipeline versions.
- Version and manage data flow pipelines.
- Track and version ML pipelines and related artefacts.
- Fault Tolerance and Exactly-Once Processing

- Maintain complete version history, change tracking, and approval workflows for data and ML pipelines, along with lineage and metadata management.

6.4.6.7.5 MLOps

- MLOps workflows must be integrated to ensure continuous, automated AI lifecycle management.
- Support CI/CD pipelines for retraining, deployment, and rollback.
- Automate model retraining triggers and anomaly diagnostics.
- Maintain configuration-as-code for version consistency and traceability

6.4.6.7.6 Open Source Regulations in AI/ML Domain

Guardrails:

- License & Legal Compliance: Open-source components shall be used only under permissive licenses, with no legal, IP, or disclosure obligations imposed on the Bank.
- Transparency & Disclosure: The Bidder shall provide complete transparency of all open-source models, tools, versions, and dependencies used in the solution.
- Ensure continuous security governance of open-source component
- Model Governance: Open-source models shall be subject to strict version control
- Explainability, Ethics & Risk Controls: Open-source models shall incorporate explainability, bias mitigation, and human-in-loop controls suitable for regulated banking environments.

6.4.6.7.7 AgentOps (Agentic AI Management)

- Provide AgentOps capabilities for managing multiple autonomous or semi-autonomous AI agents.
- Each agent must have defined roles, goals, API permissions, and safety constraints.
- Enable sandboxed execution, runtime supervision, and complete decision traceability.
- Support collaboration between agents (e.g., analysis agent, summarizer agent).
- Maintain logs for all agentic actions, prompts, and outcomes for governance review.

6.4.6.7.8 LLMOps – Generative AI Operations

- The solution must support LLMOps for managing large language models and generative systems.
- Manage model fine-tuning, context optimization, and retrieval-augmented generation (RAG).
- Language & Context Requirements for AI / GenAI / Agentic Models:

- AI, GenAI, and Agentic AI models shall support context-aware conversational interactions suitable for Indian banking environments.
- The models shall support multilingual capabilities, including multiple Indian languages.
- The system shall be capable of accurately understanding and responding to customer inputs across supported languages.
- Provide monitoring for hallucination detection, prompt performance metrics, and drift detection to ensure consistent, reliable, and accurate AI/LLM outputs over time.
- Integrate Model Context Protocol (MCP) for context-grounded inference
- Language & Context:
 1. AI, GenAI, and Agentic AI models shall support context-aware conversational interactions suitable for Indian banking environments.
 2. The models shall support multilingual capabilities, including multiple Indian languages.
 3. The system shall be capable of accurately understanding and responding to customer inputs across supported languages.
 4. Multilingual and context-aware capabilities shall be available for customer-facing workflows, including: KYC and customer onboarding Account and service-related inquiries Customer support and grievance handling
 5. The models shall maintain conversation context across interactions, even when language switching occurs.
 6. All multilingual interactions shall ensure consistency, accuracy, and compliance with applicable banking regulations and policies.

6.4.6.7.9 Explainable AI

- Provide insights into machine learning model behaviour, predictions, and decision-making processes to ensure transparency and trust.
- Support compliance with regulatory requirements and fosters stakeholder understanding of AI-driven outcomes.
- Interpret model predictions and feature importance.
- Explain individual predictions in a model-agnostic manner.
- Track and manage explainability artefacts alongside models.
- Integrate explainability tools into the data science workflow.
- Visualize explainability results and insights.
- Every model decision should include rationale and confidence scoring
- Provide explain ability dashboards for reviewers and auditors.
- LLM outputs must store grounding references and contextual justification logs.

6.4.6.7.10 No-code Agentic AI Platform

- A No-Code Agentic AI Platform shall be provided to design and deploy agentic workflows without coding.
- The platform must include a drag-and-drop visual builder to connect LLMs, APIs, databases, and tools.

- Support creation of multi-agent workflows, reusable templates, and role-based execution.
- Enable prompt and RAG (retrieval-augmented generation) design visually

Even though this capability is required in the Data /Gen AI Platform, the SI / Bidder has to develop each of the related Use cases independently using Best Practices.

6.4.6.7.11 AI Data Lifecycle Management

- A comprehensive AI Data Lifecycle Management Framework must be implemented.
- Ingestion: Validate and authorize data sources.
- Pre-processing: Clean, label, and de-bias datasets.
- Storage: Secure, versioned repositories with audit trails.
- Usage: Track data used for training, validation, and inference.
- Retention: Time-bound retention and automatic archival.
- Disposal: Irreversible, compliant data deletion post-lifecycle.
- Ensure continuous monitoring of data quality, drift, and lineage integrity.
- Synthetic data using AI and LLM should be provided by SI/Bidder

6.4.6.7.12 AI Lifecycle Manifest

- Each deployed AI system must generate and maintain an AI Lifecycle Manifest.
- Include model name, version, datasets used, performance metrics, validation status, and risk classification.
- Update manifests automatically upon retraining or redeployment.
- Maintain in JSON/YAML for interoperability.
- Integrate with audit and governance systems.

6.4.6.7.13 AI Repository Management

- A dedicated AI Repository must be created to serve as the single source of truth for all AI artefacts.
- Model Repository: Store and version all trained, tuned, and deployed models.
- Dataset Repository: Maintain lineage-tracked datasets used in training and evaluation.
- Prompt Repository: Manage prompt templates, grounding contexts, and prompt chains.
- Agent Repository: Track configurations, roles, and API mappings for all deployed agents.
- Evaluation Repository: Store validation reports and model performance metrics.
- Must support Git-based versioning or enterprise equivalents (e.g., MLflow, DVC, Hugging Face Hub).
- Include fine-grained access control, approval workflows, and immutable audit logs

6.4.6.7.14 Simulation & Guardrail Layer

- Simulation environments to test agent behaviours and workflows.

- Implemented guardrails to enforce safety, compliance, and operational boundaries.
- Mechanisms to detect and mitigate errors or anomalies in real-time.
- Ability to enable scenario-based testing for edge cases and failure conditions.
- Monitor agent actions and enforce policies for ethical AI usage.
- Integrate feedback loops to refine guardrails and improve system reliability.
- Ensure scalability, security, and adherence to governance standards.

6.4.7 Security

6.4.7.1 Masking

- Ensure sensitive data is protected by obscuring or redacting data fields to prevent unauthorized access while maintaining usability for analytics.
- Support compliance with data privacy regulations by applying dynamic or static data masking techniques.
- Define and enforce data masking policies.
- Audit and manage sensitive data access.
- Implement consistent masking policies across the data lake house.
- Apply masking policies at the query level.
- Implement data masking during data ingestion and transformation.

6.4.7.2 Authentication

- Support integration with the Bank's IDP and enable single sign-on (SSO) for seamless and secure authentication.

6.4.7.3 Authorization

- Provide fine-grained access control to ensure that users and applications can only access data and resources they are authorized to use.
- Support role-based access control (RBAC) and attribute-based access control (ABAC) to enforce security policies across the data lake house.
- Centralize policy management and enforcement of access control.
- Consistent access control policies across the data lake house.
- Manage user roles and group memberships.
- Implement fine-grained access control at the data and file level.
- Monitor and audit access control configurations.

6.4.7.4 Anonymization

- Protect sensitive data by transforming it into an irreversible form, ensuring privacy while retaining data usability for analytics.
- Support compliance with data privacy regulations by anonymizing personally identifiable information (PII) and other sensitive data.
- Apply anonymization techniques during data ingestion and transformation.
- Enforce anonymization policies on sensitive data fields.

- Consistent anonymization policies across the data lake house.
- Open-source or custom libraries for implementing anonymization algorithms (e.g., tokenization, hashing).
- Apply anonymization at the query level during data access.

6.4.7.5 Encryption

- Ensure data security by encrypting data at rest and in transit to protect it from unauthorized access and breaches.
- Support compliance with regulatory requirements by implementing robust encryption standards and key management practices.
- Encrypt data at rest in the Platform Distributed storage
- Encrypt data in transit between services and clients.
- Leverage existing KMS solution to manage encryption keys and policies.
- Consistent encryption policies across the data lake house.
- Must enforce the use of Strong Cipher Suites to ensure secure communication over the network

6.4.7.6 Audit

- Provide comprehensive tracking and logging of user activities, data access, and system events to ensure accountability and detect potential security breaches.
- Support compliance with regulatory requirements by maintaining detailed audit trails for data and resource usage.
- Centralized auditing of access control policies and user activities.
- Detailed auditing and lineage tracking of data access and transformations.
- Storage level audit Logs for tracking file-level access and operations.
- Audit data flow and transformations.
- Monitor and audit cluster-level activities and configurations.
- Implement mechanisms for internal and third-party audits of AI models and workflows
- Support continuous validation to ensure performance integrity and regulatory alignment
- All audit reports and validation results must be archived in the central AI repository

6.4.7.7 Perimeter Protection

- VLANs, ACLs, and fine-grained traffic control at and below the Top of Rack (ToR) level to isolate workloads, sensitive data, and critical services. All communication between components below the ToR level is encrypted using TLS/SSL to protect data in transit. Strict authentication, authorization, and role-based access control (RBAC) to ensure least privilege access for all systems and services .
- Internal traffic below the ToR is monitored for anomalies and secure infrastructure with hardware-level protections.

6.4.7.8 Host Protection

- Secure individual hosts in the data lake house cluster by implementing measures such as intrusion detection, malware protection, and system hardening.
- Ensure that all nodes in the cluster are protected against unauthorized access, vulnerabilities, and potential security threats.
- Monitor and manage host-level security configurations.
- Enforce mandatory access control on hosts.
- Restrict inbound and outbound traffic on individual nodes.
- Detect and mitigate malware threats on hosts.
- Secure the operating system by disabling unnecessary services and applying security patches.

6.4.7.9 Hardware Security

- Standard hardware security features such as secure boot and firmware integrity checks shall be supported and enabled.

6.4.8 Governance

6.4.8.1 Glossary

- Enable the creation and management of a centralized business glossary for the data elements in the Lakehouse, to standardize terminology and definitions across the organization.
- Link business terms with technical metadata, ensuring alignment between business and technical stakeholders and enhancing data governance practices.
- Define and manage business terms and their relationships.
- Metadata management, lineage tracking, and associating business terms with technical assets.
- Enforce consistent governance policies across the data lake house.
- Enable users to easily search and understand glossary terms.
- Integrate Glossary with external governance and analytics tools.

6.4.8.2 Catalogue

- Provide a centralized repository for managing metadata, enabling data discovery, classification, and lineage tracking.
- Facilitate collaboration by allowing users to search, understand, and govern data assets effectively within the data lake house.
- Metadata management, data discovery, and governance.
- Metadata classification, lineage tracking, and integration with other governance tools.
- Consistent governance and metadata management across the lake house.
- Enable users to search, tag, and classify data assets.
- Integrate the catalogue with external tools and workflows.
- Provide Agentic Category and Agentic catalogue APIs for use cases such as research, compliance, analytics, and automation

6.4.8.3 Data Quality

- Ensure data accuracy, completeness, consistency, and reliability across the data lake house.
- Provide tools for profiling, validating, and monitoring data quality to support governance and decision-making processes.
- Profile, validate, and monitor data quality.
- Define and enforce data quality rules and metrics.
- Consistent enforcement of data quality policies across the lake house.
- Analyse and understand data patterns and anomalies.
- Notify stakeholders of data quality issues.
- The platform shall ensure 100% consistency & integrity for all data. Any inconsistency or integrity issue reported must be remediated immediately. Any loss incurred to the Bank on account of this will be recovered from the SI.

6.4.8.4 Data Policies

- Enable the definition, enforcement, and management of data access, usage, and compliance policies across the data lake house.
- Ensure data security, privacy, and regulatory compliance by applying consistent governance rules.
- Centralized policy management and enforcement.
- Fine-grained access control and policy enforcement.
- Metadata-driven policy creation and governance.
- Track policy compliance and user activity.
- Integrate with the existing AD, for role-based access control (RBAC) and user authentication.

6.4.8.5 Data Lineage

- Tracks the flow of data across the data lake house, providing visibility into its origin, transformations, and usage.
- Enables organizations to ensure data integrity, support compliance, and troubleshoot data issues by understanding dependencies and transformations.
- Capture and visualize end-to-end data lineage.
- Integrate metadata and lineage information for data discovery.
- Consistent governance and lineage tracking across the lake house.
- Capture lineage during data ingestion and transformation.
- Present lineage information in an intuitive, user-friendly format.

6.4.9 Infrastructure

6.4.9.1 GPU Clusters

- Provides high-performance computing capabilities for workloads like machine learning (ML), and data-intensive analytics, as required.
- Accelerates data processing and model training by leveraging GPU hardware for parallel computation.
- Manage GPU-enabled clusters within the Platform ecosystem.
- Develop GPU-accelerated applications.
- Distribute data processing with GPU acceleration.
- Schedule and manage GPU resources.
- The bidder/SI shall submit OEM-certified reference architecture & compatibility details and shall be responsible for procuring, delivering, installing, and commissioning the GPU cluster infrastructure at DC and DRC.
- Wherever possible adopt open-source GPU framework for GPU abstraction

6.4.9.2 Dedicated Servers

- Provide high-performance, scalable, and reliable compute and storage resources tailored to the specific needs of the data lake house, as applicable.
- Ensure optimal performance for resource-intensive workloads, such as ETL, analytics, and machine learning, by isolating resources from shared environments.
- High-performance servers optimized for Platform workloads.
- Provision, monitor, and manage dedicated server clusters.
- Distributed storage on dedicated servers.
- Resource allocation and workload management.
- RAID Configurations for enhanced data redundancy and performance on dedicated storage.
- The bidder/SI plan for servers like ETL, analytics, and machine learning and submit infrastructure sizing details based on expected workloads, covering compute, memory, storage, and network requirements.
- Servers should have Mandatory Features like
 - More than one CPU sockets
 - A baseboard management controller that supports out-of-band management operations
 - One or more network connections
 - Error-correcting memory
 - Ability to run server operating systems and applications
- Sold and marketed by the vendor as a server Common Features like
 - Redundant power supplies
 - Redundant cooling
 - Expansion slots for input/output (I/O) devices.

6.4.9.3 Containers

- Enable OCI-Compliant lightweight, portable, and scalable deployment of applications and services within the data lake house, as applicable.
- Facilitate efficient resource utilization, rapid provisioning, and consistent environments for development, testing, and production.

- Containerize applications and services in the lake house. Wherever possible adopt open-source GPU framework for GPU abstraction
- Orchestrate and manage containerized workloads.
- Integrate containerized applications with the Platform ecosystem.
- Manage the configurations and deployments on the container orchestration platform.
- Monitor containerized workloads and infrastructure.

6.4.9.4 Virtual Machines

- Provide flexible, scalable, and isolated environments for running workloads in the data lake house, as applicable.
- Support multi-tenancy, resource allocation, and workload isolation, enabling efficient use of physical hardware.
- Create and managing virtualized environments.
- Integrate with virtualized environments to manage Platform workloads.
- Monitoring Tools for tracking VM performance and resource utilization.
- Virtualization should support Mandatory Features like:
 - Hypervisor-based virtualization
 - Live migration between VMs
 - Third-party integration: Functionality to enable administration of third-party tools using GUI, API and/or CLI.
 - Support for confidential computing; encryption of virtualized compute, storage and network resources; and security of bare metal infrastructure (firmware, lights out management).
 - Technical support.
- Common Features like
 - OS-level virtualization
 - Software-defined infrastructure
 - Container-VM convergence
 - GPU support
 - Additional processor architectures like non-x86 processors, such as ARM.

6.5 Sizing for the Platform Infrastructure

Expected Data Growth over the 5 years contract period

	Y1	Y2	Y3	Y4	Y5	Total Size	Total Size in PB
Incremental daily in GB	350	525	788	1181	1772		
Structured Data	126000	189000	283500	425250	637875	1661625	1.66
Incremental daily in GB	105	158	236	354	532		

Un-structured Data	37800	56700	85050	127575	191363	498488	0.50
Existing Data size Day zero onwards							1.70
<u>Total Structured + Un-structured + Existing Data</u>							~ 4.00

6.5.1 Compliance and Documentation

- Ensure full compliance with the functional and technical specifications set forth herein.
- Submit datasheets for all proposed components as part of its bid response.
- Propose higher specifications wherever deemed necessary to meet sizing requirements and the proposed solution.
- Warrant that all hardware, software, and associated components proposed shall be of the latest version and free from end-of-life (EOL) or end-of-support (EOS) status at the time of submission of the bid, throughout the contract period and 2 years post completion of contract period.

6.5.2 Leverage Bank's existing resources

The Bank's available resources, as outlined in the table below, may be utilized by SI to meet the functional and non-functional requirements of the Platform. To fulfill the requirements detailed in **Annexure 12**, the SI must also include any additional tools in the BoM.

When incorporating the Bank's existing & emerging resources, SI must ensure full validation & interoperability with the proposed solution. If this cannot be guaranteed, the SI will be responsible for including alternative tools in the BoM, implementing the necessary infrastructure, and ensuring that these tools operate effectively within the Bank's environment.

Category	Technology	Additional Comments
Oracle Suite of Products	Oracle Database Enterprise Edition Oracle Real Application Clusters Oracle Partitioning Oracle Diagnostics Pack Oracle Tuning Pack Oracle Web Logic Suite Oracle Advanced Security	Oracle Golden Gate license is not available with the bank.

Category	Technology	Additional Comments
	Oracle Data Masking and Sub setting Pack Oracle Advance Data Guard	
ITSM Tool	Motadata Serviceops	-
Anti-Virus	Trend Micro Deep security-Enterprise	-
LDAP / AD	Microsoft Active Directory	'On-premises' version
HSM	IBM HSM Crypto Express 8S - CEX8 with z16)	-
KMS	IBM Encryption Platform	-
PIM	Privileged Identity Management-SECTONA	
SIEM	Net Witness Platform for SIEM	-
API Gateway	IBM API Connect (part of CP41)	-
Data center (space, power, cooling)	Not Applicable	Power: 12KVA
DC- DRC connectivity	Not Applicable	Two links of 5gbps each (Both active)
TOR Switch	Cisco N9K-C93180YC-FX3 With 10G/25G multimode fiber SFP and 1G Copper SFP	
WAF	F5 12900	WAF is also used as LB for DMZ segment which is exposed to internet.
Firewall (Perimeter, Internal and DMZ Firewalls)	Not Applicable	-

6.5.3 Licensing and Software Requirements

- Provide enterprise-wide licenses for all software modules proposed, without any constraints on the number of users, transactions, APIs, screens, channels, devices, branches, or any other parameters.
- Should account for all environments, including but not limited to Development, UAT, Dev, Sandbox, the Data Center (DC), and the Disaster Recovery Center (DRC).

- All proposed software should include 24x7x365 support from the Original Equipment Manufacturer (OEM). Any open-source components proposed as part of the solution shall be back-to-back supported from the OEM with Enterprise class support model or subscription, including defined support SLAs, security updates, and maintenance. Community-only or unsupported editions shall not be considered acceptable for deployment.
- Provide requisite licenses for system software, including but not limited to operating systems, compilers, multipathing software, file systems, volume managers, server hardening tools, failover agents, and clustering software, with no restrictions on usage or instances.
- The bidder/SI shall ensure that all system software licenses are compatible with the proposed hardware, virtualization, and container platforms. All licenses shall remain valid and supported for the entire contract period, including extensions, without additional cost to the Bank.

6.5.4 Hardware Specifications

- SI shall provision either Blade Server/Rack server to meet the requirements mentioned in RFP.
- SI shall ensure proposed form factor (Blade or Rack) shall be consistent across DC and DRC for operational uniformity
- SI shall propose GPU/on-chip AI accelerator in Rack/Blade server-based platform meeting the requirement stated in RFP.
- Server should have latest Generation processors.
- The servers must be rack-mounted and equipped with minimum dual 32-core Intel Xeon Platinum CPUs (2.7 GHz or better) or equivalent CPU that support the latest computational and graphics accelerators.
- High density servers with in-built cooling should be available to support current and future demands.

• GPU specifications:

Each GPU card should have a memory capacity of 141 GB or more to handle large and complex AI models.

Any model of the GPU from the OEM should be in use in any Bank in India.

The memory type must be HBM3e with a memory bandwidth of up to 4.8 TB/s or higher to support demanding tasks. GPU slicing with minimal performance overhead should be available.

SI/Bidder must ensure that all GPUs are supplied with the appropriate interface and power connections required for their type and form factor.

It should offer seamless interconnectivity options to enable the formation of powerful GPU clusters and support high-speed interconnect technologies (NVLink, NVSwitch) with a bi-directional bandwidth of approximately 900 GB/s. Additionally, it must be compatible with PCIe Gen5 X 16 (128 GB/s) interconnects and deliver performance metrics of FP64 equivalent to or exceeding 30-34 TeraFLOPs and FP32 equivalent to or exceeding 60-67 TeraFLOPs.

SI to ensure GPUs are supplied with all the required specific proprietary software stack including but not limited to LLMs, Tool kit, drivers, control panel, etc.

- Each server must include a minimum of 512 GB DDR5 5600 MHz RAM (using minimum 64GB DIMMs), scalable to minimum 4 TB in a fully populated

configuration. The servers must be capable of identifying and reporting whether genuine OEM memory is installed to ensure system reliability.

- The servers must support minimum 32 DDR5 DIMM slots (RDIMMs/LRDIMMs) with speeds of 5600 MT/s or higher and provide advanced memory protection features, including ECC with multi-bit error protection, online spare, mirrored memory, and fast fault tolerance.
- Server shall be Controller Embedded / PCIe based or connected over the Fiber Channel via FCP to support RAID controller supporting RAID, 1, 5, 6, 10, 50, 60.
- Server should support Operating Systems and Virtualization Software proposed as part of solution. All kind of software licenses should be provided by the bidders.
- The servers must support a minimum of 12 x 2.5" SSD/NVMe drives and include a RAID controller with 12GB NV Cache, supporting RAID levels 1, 5, 6, 10, 50, 60. The storage controller must support secure encryption/data-at-rest encryption and hardware RAID for NVMe disks.
- NVMe drives intended for hot-tier workloads shall be directly connected and not bottlenecked by shared controllers.
- NVMe drives (with min. IOPS-5000) should be provided for Hot Tier & Production workloads, which should be directly connected and not bottlenecked by shared controllers. However, to meet SLA SI/Bidder to provide NVMe drives in Warm/Cold Tier as well as UAT, Dev, Sandbox wherever required.
- Storage performance testing aligned to expected workloads shall be included as part of acceptance testing
- Storage performance figures shall be validated during acceptance testing under representative workloads.
- Throughput to be assessed by the Storage size, data transformation window etc

NVLink Switch Specification

- High Bandwidth Interconnect: The NVLink switch should provide a minimum bandwidth of 900 GB/s per GPU pair, ensuring fast communication between GPUs to handle heavy AI and analytics workloads effectively.
- Scalability: It must support scaling up to at least 16 GPUs per cluster, delivering low latency and high throughput to enable efficient parallel processing across multiple GPUs.
- Compatibility: The switch should be compatible with common enterprise-grade GPUs (such as NVIDIA H200) widely used in AI and analytics solutions.
- Reliability and Redundancy: Features like failover support and error correction are necessary to maintain uninterrupted data flow and high availability.
- The bidder/SI shall submit indicative rack-level and cluster-level GPU interconnect layouts.

6.5.4.1 Connectivity and Expansion

- User and application traffic:
 - at least 2 dual-port 25 Gb Base-SFP+ network interface cards (NICs) and transceivers.
- Management:
 - Dedicated management port with 1× 1GbE for BMC and 10 GbE for OS Management
- Storage Network:
 - 2× 200 Gb Ethernet
 - Support for RoCE v2, Jumbo Frames, NVMe-oF (wherever applicable)
- GPU/ AI Network:
 - 2× 200 Gb or higher NICs per GPU server
 - GPUDirect RDMA
 - InfiniBand or RoCE Ethernet
- Intra-Node GPU Connectivity:
 - NVlink Switch 900 Gb/s per GPU pair
- Minimum of 12 PCIe Gen5 slots or more for upgrades (SmartNIC, additional GPU, DPU, or accelerator card). SI to ensure CPU and GPU clusters connectivity to meet the SLA.
- The servers must include a minimum of 1 VGA/video port, 2 x USB 2.0/USB 3.0 ports, dedicated management ports, and support for serial, MicroSD, and USB 3.0 interfaces.
- The servers should support and be certified for the operating system proposed to be installed and must integrate with leading server management software.

6.5.4.2 Power and Monitoring:

- The servers must include platinum-rated dual redundant power supplies and provide system ID and status information to reflect the health and error conditions of the system.
- The servers must support real-time power monitoring, graphing, threshold settings, and alerts, as well as temperature monitoring and graphing. Predictive failure monitoring and proactive alerts must be provided for critical components, including fans, power supplies, memory, CPUs, RAID controllers, NICs, and HDDs.
- Intelligent power distribution units with real-time usage telemetry shall be deployed. Remote monitoring capabilities should comply with Indian IT monitoring standards for operational transparency.
- Proposed Infrastructure must be compatible with data centre UPS; SI/Bidder to include runtime estimates for full-load conditions
- Power Per Rack: Design for an average rack power density of maximum 12 kVA. This accommodates modern high-density analytics and storage servers commonly deployed in large-scale Lakehouse implementations.

- Power Redundancy: Dual independent electrical feeds (A and B power sources) to each rack are mandated. Power feeds should be supported with stable UPS systems ensuring continuity despite grid fluctuations common in Indian infrastructure.
- Inclusion of surge protectors and voltage regulators to handle grid voltage spikes and dips.
- Scalability: Infrastructure should be modular for easy capacity expansion in alignment with evolving use-case demands and power availability improvements by Indian utilities.

6.5.4.3 Cooling:

- The platform needs cooling infrastructure that can reliably handle the heat generated by high-density compute and storage racks used by AI and advanced analytics workloads. Cooling systems should be scalable, energy-efficient and support current and future demands based on RFP use cases.
- Cooling design should follow recognized industry standards for temperature, humidity and airflow to ensure hardware operates safely and efficiently.
- The solution must include detailed thermal output (BTU/hr) and power draw (Wattage) characteristics per unit.
- Hardware should come with inbuilt direct to chip Liquid cooling capability. Liquid cooling system must be vendor-certified, include all necessary pumps, connectors, and leak protection
- Utilize chilled water systems if water availability is ensured, with environmental sustainability and water conservation measures in line with regulations.
- Cooling systems must maintain room temperatures around 22-26°C with relative humidity between 45-60%
- N+1 redundancy in cooling equipment is mandatory to ensure uninterrupted operation despite potential failures or maintenance
- Provision for backup cooling (e.g., additional CRAH units or chilled water redundancy) to manage extreme heat days.
- MIG/Virtual GPU Partitioning Must not interfere with thermal thresholds
- All equipment must have CE, RoHS, and BIS certification.
- GPU thermal components must be rated for 24x7x365 enterprise operation.
- Temperature sensors and automated fan speed control
- Smart PSU monitoring and alerts
- Liquid-cooling support with leak detection (for high-density deployments)
- Equipment must operate reliably at ambient temperature range of 10°C to 35°C
- Humidity Tolerance 20%–80% RH (non-condensing)
- Front-to-back airflow preferred for rack deployments
- SI/Bidder must specify delta impact on CRAC/air conditioning load in tons or kW
- Deploy environmental sensors for temperature, humidity, airflow, and integrate with centralized control systems for dynamic cooling adjustments
- Monitoring Support Systems must provide real time data on temperature, airflow, fan speed, water flow, leak detection. They should support common protocols like SNMP, Modbus TCP, Redfish for integration with Data Center management.

- Safety Features – Leak detection, drip trays, condensation controls (e.g dew point management) are critical for protecting sensitive equipment.
- Maintenance – Fans, controllers, power supplies should be hot-swappable, allowing servicing without downtime
- Cooling equipment should be compatible with existing building management and data centre infrastructure management systems
- Cooling infrastructure must be designed with modularity to accommodate expansion in rack density and power without major overhauls.
- The solution should fit within the planned power and cooling infrastructure, ensuring smooth integration into the data centre environment.

6.5.4.4 Hardware Performance and Management:

- The servers must support real-time hardware performance monitoring and alerting, agent-free monitoring, driver updates, and configuration.
- The solution must include features for power monitoring and capping, RAID management, external storage management, and monitoring of Fiber Channel, Host Bus Adapters (HBAs), I/O ports, and overall system health.

6.5.4.5 Industry Standards and Compliance:

- The servers must comply with industry standards such as ACPI 6.1, PCIe 5.0, Energy Star, and UEFI.

6.5.4.6 Security Features:

- The servers must include the following security features:
 - Secure default passwords
 - Persistent event logging, including user activity
 - Secure alerting mechanisms
 - Automatic BIOS recovery
 - Rapid OS recovery
 - System erase functionality
 - Cryptographically signed firmware
 - System lockdown capabilities
 - Secure boot, firmware integrity checks, and system recovery features

6.5.4.7 Workload Optimization:

- The servers must support workload profiles for simplified performance optimization.

6.5.4.8 Storage and Redundancy:

- SAN-based storage facilities must be provisioned for all environments.
- The proposed solution should ensure high-speed and low-latency storage networking.
- The SAN fabric shall be dual-fabric with multipathing, lossless, NVMe-oF capable, and fully redundant, providing line-rate performance, zero packet loss, and microsecond end-to-end latency to meet enterprise Lakehouse and GenAI SLAs, which will be validated during acceptance testing.

- There should not be any oversubscription for storage paths. Automatic path failover without I/O interruption.
- The SAN and network switches must be designed to accommodate port-level redundancy, path level redundancy, etc ensuring high availability and fault tolerance for critical operations.
- All critical hardware components, including but not limited to Switch, Link, Optics, Power Supply, Control Plane, Hard disks, PCI cards, fans, etc. shall not possess any single point of failure and must be hot-swappable to ensure zero downtime.
- Software & Control Plane capabilities like Non-disruptive upgrades (ISSU), stateful failover, Fast convergence (< 1s) shall be available.

6.5.4.9 Server Racks

- The server racks must conform to industry standards (e.g., 42U racks) and include redundant Power Distribution Units (PDUs), cable management arms, perforated doors, mounted wheels, exhaust fans, and lock-and-key mechanisms.

6.5.4.10 Futureproofing and Scalability:

- The SI must ensure that all hardware provisioned is sufficient to support the Bank's current and future requirements, including any additional infrastructure necessary for migration, testing, and operational continuity.

6.5.5 Infrastructure Sizing and Design

- Determine the optimal sizing of all infrastructure components, including but not limited to:
 - Hardware: High-Performance Servers, Processors (CPUs, GPUs, TPUs as applicable), Memory, Storage Controllers, Cooling Systems, Power Redundancy etc)
 - Software: Operating systems, Middleware, Platform Applications, Development Tools, Monitoring and Management
 - Network Components: High-Speed Networking, Load Balancers, Network Segmentation.
 - Storage Solutions: Primary Storage (SSD, HDD), Data Lakehouse Storage, Backup and Recovery, Archival Storage, Data Tiering
 - Virtualization and Containerization: Virtualization Platforms, Containerization, Bare Metal Management
 - Data Management and Governance: Data Integration Tools, Data Catalogues, Data Governance, Data Quality
 - AI/ML-Specific Infrastructure: AI Accelerators, Model Training and Deployment, Experimentation and Tracking, Inference Optimization, Vector Databases
 - Performance Optimization: Caching Solutions, Data Compression, Parallel Processing
 - Foundational SLM / LLMs (available on premises of the Bank)
- The infrastructure design shall align with the Bank's business objectives, scalability requirements, and Service Level Requirements (SLRs). The SI shall ensure that the solution meets performance, reliability, security, compliance, and cost-effectiveness criteria.

- Ensure that the infrastructure is future-proof and scalable. Should the infrastructure fail to meet SLRs during the contract period, the SI shall deploy additional hardware, software, or other components at its own cost to meet the required performance levels and storage requirements.
- Provide all necessary components, tools, and utilities required for the seamless setup, operation, and migration of the platform, ensuring that the solution is fully functional and compliant with the Bank's requirements.
- Required to prepare and submit, as part of their technical proposal, a detailed description of the methodologies and computations used for determining the sizing and capacity requirements for all Infrastructure components.
- The SI shall quote for dedicated infrastructure for each component listed in the Bill of Materials (BoM), ensuring that all dependencies and contingencies for the successful implementation of the platform are addressed.
- Environment-wise sizing guidance:
 - **Data Centre (DC): 100% of production capacity**
 - **Disaster Recovery Centre (DRC): 100% of production capacity**
 - **User Acceptance Testing (UAT): minimum 30% of production capacity**
 - **Development (Dev): minimum 10% of production capacity**
 - **Sandbox: minimum 10% of production capacity**

6.5.6 High Availability and Disaster Recovery

- Design and implement the DC and DRC in an active-passive mode.
- Ensure synchronous/asynchronous data replication with zero data loss and conduct quarterly DR drills to validate readiness and effectiveness.
- Encrypt all backup files and leverage the encryption key management services of the Bank.
- Ensure real-time monitoring of DR parameters, including RPO, RTO, and replication status, and provide centralized dashboards for reporting and alerts.
- The solution must comply with all applicable guidelines issued by the Reserve Bank of India (RBI), PCI-DSS standards, and other statutory requirements.

6.5.7 Security and Network Requirements

- Integrate with security components of the Bank, including firewalls, intrusion prevention systems, and secure access mechanisms, to protect all data at the DC and DRC.
- Provision and implement network components starting from Load Balancer, Reverse Proxy and below.
- Install, maintain, and manage antivirus software for servers at the DC and DRC.
- Ensure redundant network links between the DC, DRC, and remote locations to meet Service Level Requirements.
- The solution (Entire Data Lakehouse, AI & GenAI Platform) must support secure communication over both IPv4 and IPv6 networks
- Solution should adhere to the zero trust architecture like Zero-trust network segmentation, ZT between platform components, etc.

6.5.8 Performance and Scalability

- Ensure that servers are load-balanced to prevent performance degradation in the event of server failure.

- Hardware must be vertically scalable to accommodate future requirements.
- The overall solution should be horizontally scalable to accommodate future requirements.
- The solution must eliminate single points of failure across all components, including servers and storage devices.
- Deploy future-ready tools, such as Patch Management Tools, Monitoring Tools, and DR Automation Tools, as specified by the Bank.

6.5.9 Implementation and Support

- Provide 24x7x365 onsite support for the proposed solution.
- Ensure back-to-back OEM support for all hardware and software throughout the contract period.
- Provide training, knowledge transfer, and detailed documentation to Bank officials and obtain sign-off upon completion of the contract period.
- The Bank reserves the right to audit the solution and ensure compliance with IT, Information Security, and Cyber Security policies.

6.5.10 Additional Requirements

- Ensure that all goods supplied under the contract are fully insured against loss or damage during transportation, storage and assembly.
- Maintain spare hardware at the DC and DRC to ensure timely repair or replacement.
- Provide a Manufacturer Authorization Form (MAF) in the prescribed format.
- Ensure that all hardware, software, utilities, and tools provisioned as part of the solution are compatible, interoperable, and sufficient to meet the Bank's operational and migration requirements.
- Ensure that all hardware and software components comply with current standards and guidelines issued by statutory authorities, including Government agencies, RBI, IBA, CERT-in and IDRBT.

6.6 Platform infrastructure setup

- The SI shall design the technology and infrastructure architecture in accordance with the requirements specified in the RFP document.
- The SI shall be responsible for the design, supply, commissioning, installation, and maintenance of all required hardware, including development, user acceptance testing (UAT), and setup at the Data Centre (DC) and Disaster Recovery Centre (DRC) sites for the entire solution stack. This includes, but is not limited to, server hardware, storage, archival systems, backup systems, and tape library systems, with 24x7x365 OEM support.
- The SI shall deliver, install, implement, integrate, commission, and maintain all system software, including but not limited to the operating system and database (Oracle database licenses will be provided by the Bank), along with enterprise licenses, ensuring 24x7x365 OEM support.
- The SI shall design and implement the required setup, including infrastructure, platform, tooling, data replication, and other necessary components, across the DC and DRC.
- During the installation, SI shall check physical availability of items as per the bill of material. If any of the items are not delivered / not as per the specification

/ are damaged etc., SI's representative/s at the site shall take immediate steps and ensure all the items are delivered so that the installation is not hampered. SI shall have to arrange for all testing equipment and tools required for installation, maintenance, and arrange the vehicle for transport at no additional cost to the Bank.

- SI will perform Racking and Stacking of the supplied Hardware Infrastructure and Asset Tagging.
- SI will provide SAN & LAN cables for connectivity of the supplied Hardware in redundant mode with SAN LIUs/SAN Switches and Top of Rack Switches of Bank.
- SI shall carry out structured SAN and LAN cabling for supplied hardware and required tagging for successful deployment of the Hardware Infrastructure.
- SI shall provide Structured Cabling Diagram, Rack Diagram for DC & DRC
- SI shall perform High Availability testing to ensure that there is no single point of failure in the supplied Hardware components & platform.
- The SI shall perform server hardening for all servers as part of the scope of work, adhering to industry best practices and the Bank's policies.
- The SI shall provide the Bank with all necessary prerequisites at least two (2) weeks prior to the delivery of hardware to ensure smooth installation of the hardware infrastructure.
- The delivery of licenses for the operating system, database, and other system and application software, including the generation of software license keys, shall only be undertaken after receiving written confirmation from the Bank following the delivery of the hardware infrastructure.
- The SI shall activate all licenses for the supplied hardware and software.
- The SI shall engage the services of the OEM for the installation of the hardware.
- The SI shall configure the supplied hardware with load balancers to ensure optimal performance.
- The SI shall appoint a dedicated Project Manager to be stationed at the Bank's DC location for the duration of the implementation project until the successful implementation of the complete solution. The Project Manager shall act as the single point of contact, coordinating with all stakeholders to ensure smooth implementation and timely completion of all activities outlined in the RFP document. The Project Manager shall provide weekly progress reports to the Bank's designated official.
- The SI shall hand over complete infrastructure details, including but not limited to operating system configurations, low-level architecture details, license details, and associated documentation, to the Bank.
- The SI shall provide an escalation matrix, including contact persons, phone numbers, and email addresses, for support purposes. Any changes to the escalation matrix must be promptly updated and communicated to the Bank.
- The SI shall visit the DC and DRC locations and include transportation and installation costs up to the server room within the Bill of Material (BoM). Any damages caused during delivery, installation, or commissioning of the hardware shall be rectified by the SI at no additional cost to the Bank.
- The SI shall ensure that all hardware delivered to the DC and DRC locations is covered under comprehensive insurance until successful installation and acceptance by the Bank, without incurring any additional cost to the Bank.

- The SI shall bring all necessary tools, software, firmware, utilities, and databases required for the successful installation and commissioning of the project.
- The SI shall install current and future tools, including but not limited to Patch Management Tools, Monitoring Tools, Application Whitelisting Tools, Enterprise Management Tools, Host Intrusion Prevention Systems, and Disaster Recovery Automation Tools, as provided by the Bank, on the proposed onsite systems.
- The SI shall configure the supplied systems to ensure successful integration with the Bank's Privileged Identity Management Solution and Cyber Security Operation Centre.
- The SI shall configure the supplied solution to enable backup and restoration of applications, file systems, and databases.
- The SI shall coordinate with the Bank's network team to perform the necessary configurations for network connectivity in the supplied solution.
- The SI shall conduct high availability testing to ensure there is no single point of failure in the supplied hardware components and platform.
- The SI shall carry out hardening of the operating system, database, and supplied software and tools in accordance with industry best practices and the Bank's policies.
- The SI shall ensure compatibility of all software components with the supplied hardware infrastructure.
- The SI shall perform power and network cabling, including structured rack cabling and uplink cabling from the Bank's top-of-rack (TOR) switches to the supplied hardware.
- The SI shall provide LAN cables for redundant connectivity of the supplied hardware to the Bank's top-of-rack (TOR) switches.
- The Bidder shall supply all necessary Ethernet and fiber optic cables required for interconnecting the proposed hardware. All cables must be factory-terminated, of high quality, and fully compliant with applicable industry standards—such as Cat6A or higher for Ethernet and OM4/OS2 for fiber, as applicable. Cables from the brands like Corning/Panduit/Siemens shall be used. The use of low-grade, locally assembled, or substandard cables is strictly prohibited. The Bidder shall also provide cables in at least four distinct colours to segregate cabling for Management, Software Defined Storage, HCI and Backup & Replication traffic. The Bank reserves the right to inspect all supplied cable and reject any items that do not meet the required standards. The Bidder shall replace any such non-compliant items at no additional cost to the Bank.
- In the event of any changes to the architecture, the SI shall perform the required reinstallation and reconfiguration at no additional cost to the Bank.
- The SI shall perform firmware upgrades, rollbacks, patching, and bug fixes for the servers during the contract period without incurring additional costs to the Bank.
- The SI shall configure and adhere to OEM best practices, setting all system parameters required to optimize server performance.
- During installation, the SI shall verify the physical availability of all items as per the Bill of Material (BoM). Any missing, non-compliant, or damaged items shall be immediately rectified by the SI to ensure that the installation process is not

delayed. The SI shall arrange all necessary testing equipment, tools, and transportation at no additional cost to the Bank.

- In the event of damage to property owned or leased by the Bank during the delivery or installation of servers, which is attributable to the SI, the SI shall repair or replace the damaged property at no cost to the Bank.
- The SI shall ensure that the hardware and operating systems are installed in accordance with the scope of work. The Bank shall provide hardware installation sign-off only after all activities related to hardware and operating system installation have been completed as per the RFP document.
- **The SI shall ensure that no remote connections from outside the Bank's network are allowed at any time.**
- The SI shall ensure that open internet access to or from the supplied servers is not permitted. However, restricted internet access for specified servers may be allowed in accordance with the Bank's policies.

6.7 Implementation of Platform

For the Implementation of the Platform, the responsibilities of the SI will include, but will not be limited to the following:

6.7.1 Sources

- Design ingestion pipelines for multi-modal data (text, images, audio, video, QR code, etc.).
- Implement connectors for diverse data sources with appropriate approvals (APIs, databases, IoT devices, etc.).
- Preprocess and normalize data into consistent formats for downstream use.
- Enable metadata extraction and tagging for better organization and retrieval.
- Integrate with storage systems optimized for multi-modal data (e.g., object stores, vector databases).
- Ensure real-time and batch ingestion capabilities for dynamic workloads.
- Monitor data ingestion performance and handle errors gracefully.
- Secure data pipelines with encryption and access controls.
- Adhere to governance, compliance, and data privacy standards.

6.7.2 Integration

6.7.2.1 Batch

- Design and implement ETL/ELT pipelines to handle large-scale batch data ingestion and processing.
- Configure workflows to automate scheduled data processing tasks.
- Optimize batch processing for performance, scalability, and fault tolerance.
- Ensure compatibility with diverse data sources (e.g., databases, flat files, APIs).
- Implement data validation and transformation logic to ensure data quality.
- Ensure that all data acquisition methods and systems generate audit and diagnostic logs for each data load.

- Design the platform to ingest encrypted data from the source system. Ensure that it is compatible with the encryption and decryption mechanisms implemented at the source system.
- Implement the proposed tool with the capability to perform data masking as stipulated by the bank during data transformation.
- Develop the ingestion framework to support joining multiple sources, tables, or inputs.
- Include an alerting report and monitoring utility as part of the proposed solution. Configure email notifications and mobile SMS alerts to be sent to all relevant stakeholders in the event of a failure.
- Incorporate automated business-defined sanity checks, validations, and data reconciliations into the proposed data acquisition solution to ensure data integrity
- Incorporate re-runability checkpoints into data pipelines to enable scheduled executions and reruns in case of failures.
- Design data pipelines to enable parallel reading and writing of data into the platform.
- Log job metadata information, including job duration, start time, end time, user details, job status (success or failure), error messages, and other relevant details for every instance of the job. Implement authentication and authorization mechanisms on the metadata repository to ensure secure access.

6.7.2.2 Stream

- Set up and configure streaming platforms.
- Develop real-time data pipelines to process and analyse streaming data.
- Implement mechanisms for low-latency data ingestion and processing.
- Ensure fault tolerance and high availability in streaming workflows.
- Integrate streaming data with the Data Lakehouse for real-time insights.
- Monitor and fine-tune streaming pipelines for optimal performance.
- Design the platform to ingest encrypted data from the source system. Ensure that it is compatible with the encryption and decryption mechanisms implemented at the source system.
- Implement the proposed tool with the capability to perform data masking as stipulated by the bank during data transformation.
- Develop the ingestion framework to support joining multiple sources, tables, or inputs.
- Include an alerting report and monitoring utility as part of the proposed solution. Configure email notifications and mobile SMS alerts to be sent to all relevant stakeholders in the event of a failure.
- Incorporate automated business-defined sanity checks, validations, and data reconciliations into the proposed data acquisition solution to ensure data integrity
- Incorporate re-runability checkpoints into data pipelines to enable scheduled executions and reruns in case of failures.
- Design data pipelines to enable parallel reading and writing of data into the platform.
- Log job metadata information, including job duration, start time, end time, user details, job status (success or failure), error messages, and other relevant details

for every instance of the job. Implement authentication and authorization mechanisms on the metadata repository to ensure secure access.

6.7.2.3 Change Data Capture

- Configure CDC tools to capture real-time database changes.
- Implement a change data capture solution capable of loading data into the target store(s), whether single or multiple, with minimal to no latency
- Implement CDC pipelines to replicate transactional data into the Data Lakehouse.
- Ensure data consistency and integrity during replication.
- Optimize CDC processes for minimal impact on source systems.
- Set up mechanisms to handle schema evolution and data versioning.
- Monitor CDC pipelines for performance and troubleshoot issues as needed.
- The platform shall ensure 100% consistency & integrity for all data. Any inconsistency or integrity issue reported must be remediated immediately. Any loss incurred to the Bank on account of this will be recovered from the SI.

6.7.2.4 Messages

- Develop pipelines to process and store message-based data in the Data Lakehouse.
- Implement message serialization and deserialization
- Ensure reliable message delivery using acknowledgment and retry mechanisms.
- Integrate message queues with other data sources and systems.
- Monitor message queues and pipelines to ensure smooth operations.
- Design the platform to ingest encrypted data from the source system. Ensure that it is compatible with the encryption and decryption mechanisms implemented at the source system.
- Implement the proposed tool with the capability to perform data masking as stipulated by the bank during data transformation.
- Develop the ingestion framework to support joining multiple sources, tables, or inputs.
- Include an alerting report and monitoring utility as part of the proposed solution. Configure email notifications and mobile SMS alerts to be sent to all relevant stakeholders in the event of a failure.
- Incorporate automated business-defined sanity checks, validations, and data reconciliations into the proposed data acquisition solution to ensure data integrity
- Incorporate re-runability checkpoints into data pipelines to enable scheduled executions and reruns in case of failures.
- Design data pipelines to enable parallel reading and writing of data into the platform.
- Log job metadata information, including job duration, start time, end time, user details, job status (success or failure), error messages, and other relevant details for every instance of the job. Implement authentication and authorization mechanisms on the metadata repository to ensure secure access.

6.7.2.5 Master Data Management

- Integrate master data from multiple source systems, storing master data
- Handle schema mapping and transformations to standardize data formats.
- Monitor and troubleshoot data integration workflows for reliability.
- Design the platform to ingest encrypted data from the source system. Ensure that it is compatible with the encryption and decryption mechanisms implemented at the source system.
- Implement the proposed tool with the capability to perform data masking as stipulated by the bank during data transformation.
- Develop the ingestion framework to support joining multiple sources, tables, or inputs.
- Include an alerting report and monitoring utility as part of the proposed solution. Configure email notifications and mobile SMS alerts to be sent to all relevant stakeholders in the event of a failure.
- Incorporate automated business-defined sanity checks, validations, and data reconciliations into the proposed data acquisition solution to ensure data integrity
- Incorporate re-runability checkpoints into data pipelines to enable scheduled executions and reruns in case of failures.
- Design data pipelines to enable parallel reading and writing of data into the platform.
- Log job metadata information, including job duration, start time, end time, user details, job status (success or failure), error messages, and other relevant details for every instance of the job. Implement authentication and authorization mechanisms on the metadata repository to ensure secure access.

6.7.3 Storage and Processing

6.7.3.1 Landing Zone

- Define the architecture and directory structure of the Landing Zone to accommodate various data sources and formats.
- Implement ingestion pipelines to populate the Landing Zone.
- Install and implement tool for data validation and quality check.
- Define and implement systemic data validation and quality checks to ensure data integrity before moving it to the Landing Zone.
- Set up monitoring and logging mechanisms to track data ingestion and identify potential issues.

6.7.3.2 Raw Zone

- Analyse the data sources and define ingestion strategies for batch, streaming, or CDC-based data.
- Design the directory structure for the Raw Zone to align requirements.
- Implement ingestion pipelines.
- Define and enforce data governance policies for access control and compliance.

- Validate data integrity and ensure proper logging and monitoring of ingestion processes.

6.7.3.3 Curated Zone

6.7.3.3.1 Master

- Define the schema and structure for curated master data based on business requirements and governance standards.
- Implement ETL/ELT pipelines to cleanse, transform, and enrich raw master data.
- Configure tables to enable queryable and structured access to curated master data.
- Set up metadata management and lineage tracking to ensure traceability.
- Apply security and access controls to protect sensitive master data.

6.7.3.3.2 Reference Data

- Design the schema and data model for reference data, ensuring normalization and version control.
- Implement ETL pipelines to ingest, validate, and transform reference data into the curated zone.
- Configure metadata management and governance tools for lineage and compliance.
- Set up access control policies to secure sensitive reference data.
- Conduct performance tuning for storage and query optimization.

6.7.3.4 Usage Optimized

6.7.3.4.1 Columnar

- Design and implement data models optimized for columnar storage formats (e.g., Parquet, ORC).
- Build ETL pipelines to transform raw data into columnar formats for analytical use cases.
- Configure tools for efficient querying of columnar datasets.
- Optimize storage and query performance through partitioning, bucketing, and indexing.
- Conduct testing and validation to ensure data integrity, performance benchmarks and regulatory alignment

6.7.3.4.2 Graph

- Design the graph data model (e.g., nodes, edges, properties) based on business requirements.
- Implement ETL pipelines to ingest and transform data into graph structures.
- Configure graph processing tools for analytics and querying.

- Optimize storage and query performance through indexing and partitioning of graph data.
- Validate graph algorithms and ensure data integrity during traversal and processing.

6.7.3.4.3 Document

- Design the data model for document storage, ensuring compatibility with formats like JSON or XML.
- Build ETL pipelines to ingest, parse, and transform document data into the lake house.
- Configure indexing and search capabilities for efficient retrieval.
- Optimize storage and query performance through partitioning and caching strategies.
- Validate the integrity and accessibility of document data through testing and performance benchmarking.

6.7.3.4.4 Key Value

- Design the schema for key-value data, ensuring optimal structure for access patterns.
- Implement ETL pipelines to ingest and transform data into key-value format.
- Configure tools for efficient storage and querying of key-value data.
- Optimize performance through tuning of HBase regions, caching, and compaction settings.
- Validate data integrity, access control, and query performance through testing and benchmarking.

6.7.3.4.5 Raw Based

- Design the raw data storage strategy, including folder structure and naming conventions.
- Implement data ingestion pipelines to load raw data into storage layer using tools.
- Configure tools for querying raw data with schema-on-read capabilities.
- Optimize storage performance through compression and partitioning of raw data.
- Validate data ingestion workflows and ensure data integrity in the raw zone.

6.7.3.4.6 File based

- Define the folder structure and naming conventions for organizing file-based data in Storage Layer.
- Implement ETL pipelines to ingest, validate, and transform file-based data into the lake house.
- Configure tools for querying file-based datasets using schema-on-read.
- Optimize storage through file compression and partitioning.

- Validate data ingestion, query performance, and ensure access control policies are enforced.

6.7.3.5 Data Lakehouse Capabilities:

6.7.3.5.1 Data Lake Capabilities

- Design the logical and physical architecture of the data lake, including folder structures and naming conventions.
- Implement data ingestion pipelines using tools to load raw data into the lake.
- Configure tools for metadata management and schema-on-read querying.
- Optimize storage with compression, partitioning, and replication strategies.
- Validate data ingestion workflows, ensure data quality, and enforce access control policies.
- Design the solution to support data compression, enabling both fast compression and severe compression based on data processing requirements.

Data Warehouse

- Design the data warehouse schema (e.g., star or snowflake schema) based on business requirements.
- Implement ETL pipelines to transform raw data into curated datasets for the warehouse.
- Configure tools for efficient querying, indexing, and partitioning.
- Optimize query performance through bucketing, caching, and tuning execution engines.
- Validate data quality, ensure governance policies, and integrate with BI tools for reporting.

6.7.3.6 Vector Database

- Design the schema and indexing strategy for storing vector data in storage layers.
- Implement ETL pipelines to generate, store, and index vector embeddings from raw data.
- Configure tools for similarity search and nearest neighbour queries.
- Optimize storage and query performance by tuning indexing and partitioning strategies.
- Validate vector search accuracy and integrate with downstream machine learning or analytics workflows.

6.7.3.7 Agentic Orchestration & Reasoning Layer

- Design agent lifecycle management (creation, activation, scheduling, termination).
- Build workflows for multi-agent coordination and task execution.
- Integrate with real-time and batch data pipelines.

- Develop reasoning logic using AI/ML or rule-based systems.
- Enable event-driven triggers for agent activation.
- Optimize agent performance and resource utilization.
- Implement error handling, recovery, and context awareness.
- Connect to knowledge graphs for semantic understanding.
- Ensure scalability, interoperability, and security (e.g., RBAC).
- Deploy monitoring tools and feedback loops for continuous improvement.
- Test workflows and adhere to governance and compliance policies.

6.7.3.8 Agentic Long-Term Memory

- Configure embeddings generation from agent interactions and contextual data.
- Implement efficient similarity search for memory retrieval based on relevance.
- Design memory schemas to organize and manage long-term knowledge.
- Enable memory updates for adding, modifying, or forgetting information.
- Integrate memory retrieval with agent workflows for context-aware decision-making.
- Optimize storage and retrieval performance for scalability.
- Secure memory data with encryption and access controls.
- Monitor memory usage and refine retrieval strategies for accuracy.
- Implement solution to provide adherence to governance and compliance policies.

6.7.3.9 Prompt Management & RAG Pipeline

- Design and version prompts for AI workflows.
- Build and optimize RAG pipelines with vector databases and embeddings.
- Standardize prompts and retrieval strategies for relevance and accuracy.
- Integrate with AI models and external knowledge sources.
- Monitor and improve pipeline performance through feedback loops.
- Secure data and ensure compliance with governance policies.

6.7.4 Access

6.7.4.1 Data APIs

- Design and implement RESTful APIs for accessing data stored in the lakehouse.
- Configure tools for secure API gateway access to Platform services.
- Integrate APIs with metadata and lineage tools for enhanced data discovery.
- Implement role-based access controls using tools to secure API endpoints.
- Test API performance, scalability, and security to ensure reliable integration with external systems.

6.7.4.2 Direct Access

- Configure tools for direct SQL-based access to data stored in the lake house.
- Set up file-based access protocols for applications requiring direct file access.
- Implement role-based access controls and security policies.
- Optimize query performance through indexing, partitioning, and caching.
- Validate direct access workflows for performance, security, and compatibility with analytics and reporting tools.

6.7.4.3 Search

- Configure tools for indexing and searching data stored in the lake house.
- Design and implement data pipelines to preprocess and index data for search.
- Integrate tools to enable metadata-driven search and discovery.
- Define and enforce access control policies for search operations.
- Test and optimize search performance, ensuring scalability and relevance of search results.

6.7.4.4 Single Sign On

- Integrate the lake house with Bank's enterprise identity providers (e.g., LDAP/Active Directory of the Bank) for SSO.

6.7.4.5 Tool Interface & Agent API Registry

- Design and implement APIs for seamless interaction between tools and agents.
- Develop a centralized registry for managing agent APIs and tool integrations.
- Ensure API versioning and backward compatibility for smooth updates.
- Enable dynamic discovery of APIs and tools for agents.
- Implement authentication and authorization for secure API access.
- Standardize API communication protocols.
- Integrate with external tools, platforms, and third-party services.
- Monitor API usage and performance with observability tools.
- Automate API documentation generation for ease of use.
- Test APIs for reliability, scalability, and fault tolerance.
- Ensure compliance with governance, security, and data privacy policies.

6.7.5 Consumption

6.7.5.1 API Gateway and Model Hub

- Leverage the Bank's existing API gateway to provide secure access to data and models.
- Set up tools to deploy models as APIs.
- Integrate with tools to enforce access control policies for APIs and model endpoints.
- Implement version control and monitoring for deployed models in the Model Hub.
- Test API performance, scalability, and security for seamless integration with external applications.

6.7.5.2 Reports

- Configure tools for reporting and analytics use cases.
- Set up integrations with BI tools for report generation and visualization.
- Define and enforce access control policies for reporting data.
- Optimize query performance for real-time and batch reporting workflows.
- Validate report accuracy, scalability, and usability to meet business requirements.

6.7.5.3 Dashboard

- Configure tools to support dashboard queries.
- Integrate BI tools with the lake house for dashboard creation.
- Define and implement access control policies for dashboard data.
- Optimize data pipelines and queries for real-time dashboard performance.
- Validate dashboard functionality, usability, and scalability to meet business requirements.

6.7.5.4 Web App

- Design and implement APIs using tools to provide data access for web applications.
- Configure tools for structured data queries consumed by web applications.
- Define and enforce access control policies for web application data.
- Optimize data pipelines and queries to ensure low-latency responses for web applications.
- Test web application integration, ensuring secure, scalable, and reliable data consumption.

6.7.5.5 Mobile App

- Design and implement APIs using tools to provide secure data access for mobile apps.
- Configure tools for structured data queries consumed by mobile apps.
- Define and enforce role-based access control policies for mobile app data.
- Optimize data pipelines and queries to ensure low-latency responses for mobile app interactions.
- Test mobile app integration, ensuring secure, scalable, and reliable data consumption on mobile devices.

6.7.5.6 Multi Modal Outputs

- Design output pipelines for delivering multi-modal content (text, images, audio, video, etc.).
- Implement APIs and interfaces for seamless access to multi-modal outputs.
- Format outputs for compatibility with various platforms and devices.
- Enable personalization and contextual adaptation of outputs for end-users.

- Integrate with visualization tools for presenting complex data (e.g., dashboards, charts).
- Optimize delivery for real-time and batch use cases.
- Monitor output performance and user interactions for continuous improvement.
- Secure output channels with encryption and access controls.
- Ensure compliance with accessibility, governance, and data privacy standards.

6.7.5.7 Data Exploration Tools

- Configure tools to support interactive data exploration.
- Set up tools for users to query and visualize data through a web-based interface.
- Integrate with tools for advanced data exploration and analysis workflows.
- Implement metadata tagging and lineage tracking to enhance data discovery.
- Validate the performance and usability of data exploration tools for various user personas (e.g., analysts, data scientists).

6.7.5.8 Banking Models

- Design, build, and deliver Pre-configured banking domain data models natively within the Data Lakehouse
- Models shall cover customer, account, product, transaction, risk, finance, and regulatory domains, aligned to banking standards
- All models shall support time-variant data, historical versioning, and full auditability, enabling regulatory traceability and restatement.
- SI shall deliver logical and physical models, ER diagrams, data dictionaries, and regulatory mappings as part of the solution
- Solution shall provide conformed, extensible, and time-variant models supporting historical analysis and auditability
- Models shall be delivered across raw, curated, and analytics layers, with documented business definitions and data lineage
- capability shall enable rapid regulatory reporting, risk analytics, and MIS consumption without requiring custom model design
- All models shall be configurable to bank-specific products, chart of accounts, and local regulatory requirements

6.7.5.9 Sandbox / Data Science Workbench

- Deploy and configure tools for data science and experimentation.
- Integrate tools with the lake house for seamless access to data and distributed computing resources.
- Set up tools for scalable data processing and analytics within the sandbox.
- Define role-based access controls and security policies.
- Validate the functionality, scalability, and security of the sandbox environment for data science workflows.

6.7.5.9.1 Storage

- Configure the primary storage layer for sandbox environments.
- Set up storage integration within tools for experiment outputs and artifacts.
- Define and enforce access control policies for storage.
- Optimize storage configurations for performance and scalability to handle large datasets.
- Validate storage accessibility, security, and integration with data science workflows.

6.7.5.9.2 Processing

- Configure tools for distributed processing within the sandbox environment.
- Set up tools to support interactive and batch processing workflows.
- Integrate machine learning frameworks for model training and experimentation.
- Define and enforce access control policies for processing resources
- Validate processing workflows for performance, scalability, and integration with the data lake house.

6.7.5.9.3 Infrastructure

- Set up and configure tools to provision and monitor sandbox infrastructure.
- Deploy tools for resource isolation and workload orchestration.
- Integrate data science workbench with the infrastructure for managing compute and storage resources.
- Implement monitoring tools for real-time performance tracking.
- Validate infrastructure scalability, reliability, and resource allocation for sandbox workloads.

6.7.5.9.4 Analysis

- Configure tools to support interactive and batch analysis workflows.
- Integrate tools for distributed data analysis and machine learning tasks.
- Set up Jupyter Notebooks for interactive analysis and visualization.
- Enable seamless access to lake house datasets for analysis.
- Validate analysis workflows for performance, scalability, and integration with the data lake house.

6.7.5.9.5 SLM / LLM

- Configure tools to support SLM / LLM experimentation and fine-tuning.
- Set up GPU-enabled nodes within the infrastructure for efficient SLM / LLM training and inference.
- Integrate ML and DL frameworks for developing and fine-tuning SLM / LLMs.
- Enable distributed data processing for SLM / LLM workflows
- Validate SLM / LLM workflows for performance, scalability, and security, ensuring compliance with data governance policies.

6.7.5.9.6 Prompting

- Set up Tools for interactive prompt engineering workflows.
- Integrate fine-tuned models hosted on-premise for prompt testing.
- Configure Jupyter Notebooks for iterative prompt experimentation and result visualization.
- Implement distributed processing of prompt evaluation datasets.
- Validate prompt engineering workflows for performance, scalability, and compliance with data governance policies.

6.7.5.9.7 Collaboration Tools

- Configure Tools to enable shared workspaces and collaboration features.
- Integrate with tools for version control and collaborative code management.
- Set up shared, interactive data exploration and analysis tools like Jupyter Notebooks.
- Implement Tools for metadata tracking and lineage management of shared assets.
- Validate collaboration workflows to ensure seamless sharing, versioning, and communication among team members.

6.7.6 Operations

6.7.6.1 Source Control

- Set up and configure repositories for version control of all scripts, code, and configurations.
- Integrate source control repositories with CI/CD tools for automated testing and deployment.
- Define branching strategies to manage collaborative development workflows.
- Implement access control policies for source control repositories.
- Validate version control and CI/CD workflows to ensure traceability, security, and automation.

6.7.6.2 Monitor

- Configure Tools to monitor Platform components and cluster health.
- Set up Tools for collecting and visualizing key performance metrics.
- Integrate with centralized log aggregation and analysis system of the Bank
- Define and configure alerting thresholds for critical metrics and events.
- Validate monitoring workflows to ensure comprehensive coverage, real-time alerts, and actionable insights.
- Develop the Platform to provide a dashboard for monitoring all types of nodes hosted across multiple locations through a single console. Ensure the system can

generate system-level alarms (e.g., insufficient number of instances) and node-level alarms (e.g., node-specific issues).

6.7.6.3 Scheduling

- Configure tools for orchestrating and scheduling data pipelines and workflows.
- Define task dependencies, retries, and notifications within the scheduling framework.
- Integrate with scheduling tools for centralized management and monitoring.
- Set up resource-aware job scheduling resource management tools.
- Validate scheduling workflows to ensure reliability, scalability, and adherence to SLAs.

6.7.6.4 Logging

- Configure tools to collect and manage logs from Platform components and services.
- Integrate with centralized log aggregation, search, and visualization.
- Integrate with tools for real-time log ingestion and streaming.
- Define log retention, archiving, and access policies to comply with governance and audit requirements.
- Validate logging workflows to ensure comprehensive coverage, search-ability, and actionable insights for troubleshooting and monitoring.

6.7.6.5 Observability

- The platform should provide:
 - Thorough monitoring & alerting across all layers — infrastructure, network, storage, and computing resources.
 - Data Observability for Movement of data between various layers including AI models.
- Collect and visualize real-time data including GPU usage, memory throughput, network performance with configurable alerts and dashboard for anomaly detection and failure tracking
- Collect and visualize real-time data for Data pipeline latency, data quality, response consistency, model latency, streaming jobs and job execution details, with configurable alerts and dashboard for anomaly detection and failure tracking.
- The system must offer tracing capabilities to follow data across services and components, supporting easy troubleshooting and performance tuning.
- Observability tools should integrate smoothly with standard monitoring platforms used in enterprises,
- Implement continuous AI observability, drift detection, hallucination monitoring, and real-time alerts. Enable rollback mechanisms and retraining triggers for non-compliant models
- The observability system should scale with workload growth (supporting more approximately 150 use cases) and provide sufficient long-term storage for logs and metrics to support audit and compliance requirements

- SI/Bidder to bring in the required observability tools and integrate with the platform.

6.7.6.6 DevOps

6.7.6.6.1 Continuous Integration

- Set up CI/CD pipelines to automate code integration, testing, and builds.
- Configure build tools for dependency management and artifact generation.
- Integrate with tools for static code analysis and quality assurance in the CI pipeline.
- Implement artefact repositories to store and manage build outputs.
- Validate CI workflows to ensure seamless integration, automated testing, and compliance with development standards.

6.7.6.6.2 Continuous Deployment

- Design and implement deployment pipelines to automate the release process.
- Configure playbooks for managing configurations and deploying artifacts to target environments.
- Integrate with tools for containerized application deployment and orchestration.
- Use tools for deploying and managing components in the data lake house.
- Validate deployment workflows to ensure reliability, rollback capabilities, and adherence to operational standards

6.7.6.7 Data / Analytics Ops

6.7.6.7.1 Model Versioning

- Set up tools for tracking and versioning models, including associated parameters, metrics, and artifacts.
- Integrate with tools for capturing metadata and lineage of models within the data lake house.
- Use version control tools/software for model training scripts and configurations.
- Deploy models using tools or containerized environments
- Validate model versioning workflows to ensure reproducibility, traceability, and compatibility with analytics operations

6.7.6.7.2 Deployment

- Configure tools for deploying and managing ML models in the data lake house.
- Use tools to serve models and manage deployment workflows.
- Containerize models and orchestrate deployments with orchestration platform for scalability.

- Integrate with tools for real-time data streaming and inference workflows.
- Set up monitoring tools to track model performance and resource utilization in production.
- The streaming analytics platform must process thousands of events per second, with end-to-end latency kept sub one second for real-time insights
- It should support complex event processing and windowing, capable of handling 10 or more simultaneous use cases efficiently
- Support for analytics types: benchmarking, predictive, web, social, geo, trend, profit, etc.

The platform must be tightly integrated with the underlying data lakehouse storage to manage both raw streaming data and processed outputs, supporting batch and micro-batch analytics

6.7.6.7.3 Orchestration

- Design and implement orchestration workflows using tools for data and analytics pipelines.
-
- Configure tools for orchestrating ETL and data processing tasks.
- Set up tools for real-time data flow orchestration and integration.
- Use tools and platform to orchestrate containerized workflows for analytics and machine learning operations.
- Validate orchestration workflows to ensure error handling, scalability, and seamless execution of interdependent tasks.

6.7.6.7.4 Pipeline Versioning

- Set up code repositories to version control pipeline code, configurations, and scripts.
- Integrate with tools to capture metadata and lineage for pipeline versions.
- Configure registries for versioning and managing data flow pipelines.
- Use tools to manage and version ETL pipelines.
- Validate pipeline versioning workflows to ensure traceability, reproducibility, and governance compliance.
- Streaming pipelines should guarantee data consistency and reliability through checkpointing, replay mechanisms, and exactly-once delivery semantics

6.7.6.7.5 Explainable AI

- Integrate Model Explainability tools (justification if proposing open-source tools) into machine learning workflows to provide model interpretability.

- Configure tools to track explainability artefacts and link them to specific model versions.
- Use tools to develop and deploy explainability workflows.
- Create dashboards to visualize explainability metrics and insights.
- Validate explainability workflows to ensure they meet regulatory and business transparency requirements.

6.7.6.7.6 Simulation & Guardrail Layer

- Develop simulation environments to test agent behaviours and workflows.
- Ensure data used for model development is accurate, unbiased, and representative.
- Implement guardrails to enforce safety, compliance, and operational boundaries.
- Design mechanisms to detect and mitigate errors or anomalies in real-time.
- Validate AI outputs for bias, discrimination, and explain ability. Conduct ethical risk assessments before production deployment
- Enable scenario-based testing for edge cases and failure conditions.
- Monitor agent actions and enforce policies for ethical AI usage.
- Leverage tools like DeepEval, Flowwise, or equivalent frameworks to perform both offline and online evaluation of model quality, safety, and accuracy
- Integrate feedback loops to refine guardrails and improve system reliability.
- Ensure scalability, security, and adherence to governance standards.
- All guardrail activities—including violations, corrections, and validations—must be logged, reviewed, and reported periodically to the designated AI oversight body.

6.7.7 Security

6.7.7.1 Masking

- Define and configure masking policies for sensitive data fields.
- Implement dynamic masking at the query level
- Leverage tools to ensure consistent masking policies across the data lake house.
- Use tools to apply masking during data ingestion and transformation processes.
- Validate masking workflows to ensure compliance with regulatory requirements and data privacy standards.

6.7.7.2 Authentication

- Configure mechanisms for secure authentication across the platform ecosystem.
- Integrate with Bank's enterprise Active Directory for user and group management.
- Validate authentication mechanisms to ensure secure and seamless access to the data lake house.

6.7.7.3 Authorization

- Define and implement role-based access control (RBAC) policies
- Integrate with Active Directory to synchronize user roles and groups.
- Configure fine-grained access control at the data level using tools.
- Leverage tools to enforce consistent authorization policies across the data lake house.
- Validate and audit access control policies to ensure compliance with organizational security requirements.
- Restrict access to AI/ML pipelines and artifacts to authorized users only
- Protect AI/ML models from adversarial attacks and unauthorized access
- Ensure the integrity of training data to prevent model poisoning or bias
- Monitor AI/ML models for fairness, transparency, and compliance with ethical AI principles

6.7.7.4 Anonymization

- Design and implement anonymization workflows for data ingestion and processing.
- Configure tools to enforce anonymization policies on sensitive data fields.
- Use tools to ensure consistent anonymization policies across the data lake house.
- Apply anonymization techniques using custom or open-source libraries.
- Validate anonymization workflows to ensure compliance with data privacy regulations and organizational security standards.

6.7.7.5 Encryption

- Configure Transparent Encryption to secure data at rest.
- Enable TLS 1.2+ version with Forward Secrecy encryption for securing data in transit between Platform services and clients. SSL 2.0, 3.0, TLS1.0, TLS1.1 to be disabled to avoid latest Vulnerabilities
- Integrate tools to enforce consistent encryption policies across the data lake house.
- Leverage Bank's KMS for key rotation and lifecycle management.
- Validate encryption configurations to ensure compliance with organizational and regulatory security standards.

6.7.7.6 Audit

- Configure tools to log and audit access control activities across the data lake house.
- Set up tools to track data lineage and maintain detailed audit trails for data access and transformations.
- Enable and analyse Platform audit logs to monitor file-level access and operations.
- Use tools to audit and trace data flow and transformations during ingestion and processing.

- Validate audit configurations to ensure they meet organizational and regulatory compliance requirements.

6.7.7.7 Perimeter Protection

- Implement VLANs, ACLs, and fine-grained traffic control at and below the Top of the Rack (ToR) level to isolate workloads, sensitive data, and critical services.
- Encrypt all communication between components using TLS/SSL to protect data in transit.
- Enforce strict authentication, authorization, and role-based access control (RBAC) to ensure least privilege access for all systems and services operating at and below the ToR level
- Isolate management traffic from data traffic at the ToR level using dedicated VLANs or interfaces to secure administrative access.
- The bidder/SI shall implement logical or physical network segregation for management, storage, application, and replication traffic.

6.7.7.8 Host Protection

- Configure tools to monitor host-level security and detect potential vulnerabilities.
- Implement Linux Security Modules to enforce access control policies on hosts.
- Set up host-based firewalls (e.g., iptables, firewalls) to restrict and monitor network traffic on individual nodes.
- Deploy antivirus/antimalware tools to protect hosts from malicious software.
- Perform OS hardening by disabling unnecessary services, applying security patches, and configuring secure system settings.

6.7.8 Governance

6.7.8.1 Glossary

- Deploy and configure tools to define and maintain the business glossary.
- Integrate metadata management tool to establish relationships between business glossary terms and technical metadata.
- Leverage platform tools to ensure consistent application of governance policies across the lake house.
- Develop workflows or APIs to integrate the glossary with other governance, reporting, or analytics tools.
- Validate the glossary implementation to ensure it meets organizational governance requirements and supports easy access and discovery by stakeholders.

6.7.8.2 Catalog

- Deploy and configure Data Catalogue to manage metadata and enable data discovery.
- Integrate governance tools to track data lineage and classify metadata.
- Ensure systemic enforcement of consistent governance policies and metadata management across the lake house.
- Develop workflows or APIs to integrate the data catalogue with analytics, reporting, and governance tools.
- Validate the data catalogue implementation to ensure it meets organizational governance requirements and supports user-friendly search and discovery.

6.7.8.3 Data Quality

- Deploy and configure data quality tools to define and enforce data quality rules.
- Integrate with relevant tools to ensure consistent application of data quality policies across the lake house.
- Perform data profiling to identify patterns, anomalies, and potential quality issues.
- Set up automated monitoring, alerting, and reporting mechanisms for data quality issues.
- Validate the data quality framework to ensure it meets organizational governance and compliance requirements.
- The platform shall ensure 100% consistency & integrity for all data. Any inconsistency or integrity issue reported must be remediated immediately. Any loss incurred to the Bank on account of this will be recovered from the SI.

6.7.8.4 Data Policies

- Define and implement data access, usage, and compliance policies.
- Configure tools to link metadata with data policies for consistent governance.
- Integrate with Bank's Active Directory for role-based access control and user authentication.
- Set up auditing and logging mechanisms to monitor compliance with data policies.
- Validate the implementation to ensure policies are correctly enforced and meet organizational and regulatory requirements.

6.7.8.5 Data Lineage

- Deploy and configure Data governance tool to capture and visualize data lineage across the lake house.
- Integrate Data Catalogue to link lineage information with metadata for enhanced data discovery.
- Configure ETL tool to capture lineage during data ingestion and transformation processes.
- Implement visualization tools to provide an intuitive interface for exploring lineage information.

- Validate lineage tracking to ensure accuracy, completeness, and alignment with governance and compliance requirements.

6.7.8.6 AI Governance Framework

- A formal AI Governance Framework must be defined and implemented.
- Assign clear ownership roles: AI Owner, Model Validator, Data Steward, and Compliance Reviewer.
- Maintain a central Model Registry containing model versions, validation results, and metadata.
- Conduct periodic governance reviews, risk classification, and explainability audits.
- Enforce model approval and decommissioning workflows

6.7.9 Infrastructure

6.7.9.1 GPU Clusters

- Design and deploy GPU-enabled clusters within the Platform ecosystem to support ML/DL workloads, as applicable.
- Configure resource management tools to allocate and manage GPU resources effectively.
- Integrate analytics engine with GPU libraries for accelerated data processing.
- Optimize GPU utilization by profiling workloads and fine-tuning configurations.
- Validate GPU cluster performance and ensure compatibility with existing data lake house infrastructure.

6.7.9.2 Dedicated Servers

- Design and procure dedicated servers, considering CPU, memory, storage, and network requirements, as applicable.
- Install and configure tools to manage and monitor the dedicated server infrastructure.
- Set up distributed storage and configure RAID for data redundancy and performance.
- Configure tools for efficient resource allocation and workload management on dedicated servers.
- Validate server performance and ensure alignment with the Data Lakehouse's scalability and reliability requirements.

6.7.9.3 Containers

- Design and implement a containerization strategy for applications and services in the data lake house, as applicable.
- Deploy and configure tools for orchestrating and managing containerized workloads.
- Integrate the Platform with containerized services to ensure seamless operation within the Platform ecosystem.

- Use tools to simplify container deployment and configuration management.
- Set up monitoring tools to track container performance and resource utilization.

6.7.9.4 Virtual Machines

- Design and provision virtual machines based on workload requirements, including CPU, memory, and storage specifications, as applicable.
- Configure virtualization platforms to host Platform services, if required
- Integrate the Platform with the virtualized environment to manage the workloads effectively.
- Implement monitoring tools to track VM performance and optimize resource allocation.
- Validate the virtualized infrastructure to ensure it meets performance, scalability, and reliability requirements.

6.8 Implementation of use cases

SI will size, design and implement the platform for approx. 150 use cases. However, SI will deliver 20–25 use cases under this contract. SI may refer to the list of **indicative use cases** below, for estimation and planning purposes. The detailed scope for the Use Cases will be finalized with the successful bidder. Bidder to ensure the system performance and SLA are met throughout the contract period.

The Bank reserves the right to change/modify the indicative use-case list and adjust implementation priorities based on prevailing business or regulatory requirements at the time of implementation, without incurring any additional cost to the Bank.

Each quarter, the Bank will share a list of use cases that are to be implemented as part of this initiative. These use cases will include a combination of Reporting, Business Intelligence (BI), Analytics, and GenAI applications across various business domains.

Key Performance Indicators (KPIs) will be defined for all use cases; however, adherence to the KPIs for 11 of these use cases will be linked to payment milestones.

Domain	Theme	Use case Group /Components
Growth of CASA	NTB acquisition	Driving CA acquisitions through digital marketing campaigns
		Driving SA acquisitions through digital marketing campaigns
	ETB Deepen engagement through cross sell	Cross-sell for CA customers to drive additional transaction products (e.g., salary, POS, QR, tax , bill payments) including leveraging marketing campaigns for cross-sell

		Cross-sell for SA customers to drive additional payments products (e.g., UPI, bill and tax payments, subscriptions and transfers) including leveraging marketing campaigns for cross-sell
	Churn	Identify customers likely to churn and launch interventions to reduce attrition for CA base
		Identify customers likely to churn and launch interventions to reduce attrition for SA base
	Reactivation	Reactivate dormant /inoperative CA accounts
		Reactivate dormant /inoperative SA accounts
Growth of fee income	Increase cross-sell	Cross-sell products to CA base to drive corporate fee income growth through LC (letter of credit), BG
		Cross-sell products to CA base to drive corporate/SME fee income growth through POS, Digi FMS, CMS, Insurances, virtual accounts, locker facility, CIB platform, etc.
		Cross-sell products to SA base to drive retail fee income growth through mutual funds, insurance, fastags, bill payment (BBPS), Debit cards
Growth of RAM advances	RAM NTB acquisition	Drive new acquisitions for Retail advances (incl. DLP, lead conversions and underwriting)
		Drive new acquisitions for MSME advances (incl. new acquisitions and underwriting)
		Drive new acquisitions for Agri advances (incl. DLP, lead conversions and underwriting)
	RAM ETB cross-sell	Cross-Sell Products to Retail advances customers
		Cross-Sell Products to MSME advances customers
		Cross-Sell Products to Agri advances customers
Improving collections	Collections efficiency	Driving recoveries for Agri through targeted campaigns leveraging risk segmentation, settlements (late-stage delinquencies) etc.
Reduction in fraud	Early warning systems and mule hunting	Develop anomaly detection models to flag irregularities in customer transaction behaviour using AI-driven models
		Develop AI-driven mule hunting models to detect and flag suspicious accounts
Driving operations efficiency	GenAI led productivity	Enhancing productivity of call-centers using GenAI based call summarization
		GenAI led virtual assistant for internal employees
		Enable self-service data exploration and analysis through 'Ask your data' based insight generation

Customer analytics	Customer 360 & Lifetime value	Develop 360-degree view of the customer (e.g. portfolio of products, account history) to enable RM interventions
		Develop customer lifetime value scorecards for relationship management
Additional potential use Cases	Gen AI	GenAI-led copy and creative creation for marketing campaigns (i.e., for outbound channels generate end to end copies for SMS, Email, Whatsapp)
		Personalize landing pages for products
		Personalized humanoid bot calling for droppers
		GenAI led alert generation (e.g., tracking of key metrics for Retail app Centeez)
		Profile and tag NTB Centeez customers leveraging lookalike models
		Design interventions to improve adoption of Centeez App for Retail customers

6.8.1 Data Preparation and Integration

- Implement data pipelines for ingestion, transformation, and enrichment to support the use cases.
- Ensure data quality, consistency, and governance, including the implementation of data validation and cleansing processes.
- Implement mechanisms for data versioning and lineage tracking to ensure traceability and compliance.

6.8.2 Reporting and Analytics Use Cases

1. Implement reporting dashboards and visualizations to provide actionable insights for the identified use cases.
2. Ensure that the reporting solutions support self-service capabilities for business users, enabling ad hoc analysis and exploration.
3. Configure the reporting tools to deliver real-time or near-real-time insights, as required by the use cases.
4. Implement role-based access controls to ensure secure and compliant access to reports and analytics.

6.8.3 AI and Machine Learning Use Cases

1. Design and implement machine learning models to address the identified AI use cases, including model development, training, and validation.
2. Integrate the models into the Bank's operational workflows, ensuring seamless deployment and execution.
3. Implement mechanisms for monitoring model performance, including accuracy, latency, and resource utilization.
4. Implement retraining workflows with automated drift detection and human in the loop approval to ensure safe and compliant model updates.

Triggers for retraining-

Time-based (monthly/quarterly),

Performance based, or

Event-based (new products, regulation changes).

6.8.4 Generative AI Use Cases

1. Implement Generative AI models to address specific use cases, such as content generation or summarization
2. Configure the Generative AI models to operate within the Bank's compliance and ethical guidelines, ensuring responsible AI usage.
3. Integrate Generative AI capabilities into existing systems and workflows, enabling seamless user interaction and output generation.
4. Implement safeguards to prevent misuse of Generative AI systems and to ensure outputs are accurate, safe, unbiased, and authorized, avoiding any negative impact on customers or bank operations.

6.8.5 Agentic AI Use Cases

1. Implement Agentic AI solutions capable of autonomous decision-making and action execution for the identified use cases.
2. Ensure that Agentic AI systems are configured with clear decision boundaries, escalation protocols, and human oversight mechanisms.
3. Integrate Agentic AI systems with the Bank's existing operational and decision-making frameworks.
4. Implement monitoring and feedback loops to evaluate the performance and reliability of Agentic AI systems.

6.8.6 Impact Tracking System

- Design an automated system for tracking the impact of each use case.
- Include components for:
 - Data collection and metric calculation.
 - Visualization of metrics through dashboards and reports.
 - Alerts and notifications for deviations from expected thresholds.
- Ensure that the design enables seamless onboarding of future use cases without requiring significant changes.
- Implement an automated system for tracking the impact of each use case.
- Include components for:
 - Data collection and metric calculation.
 - Visualization of metrics through dashboards and reports.
 - Alerts and notifications for deviations from expected thresholds.

6.8.7 Support implementation of additional use cases

6.8.7.1 Requirement Analysis and Validation Support

- Assist the Bank's Data team in analyzing and validating business and technical requirements for additional use cases.
- Provide inputs to ensure alignment with the existing system architecture

6.8.7.2 Solution Design Support

- Support the Bank's Data team in designing solutions for the use cases by providing technical guidance and recommendations.
- Review and validate the proposed designs to ensure compatibility with the existing system and scalability for future enhancements.

6.8.7.3 Data Integration and Preparation Support

- Provide guidance on data pipeline design, data quality checks, and governance best practices.
- Implement data pipelines to onboard the required data sources with the required quality, correctness and comprehensiveness.

6.8.7.4 Development and Configuration Support

- Provide advisory and technical support to the Bank's Data team during the development and configuration of workflows, models, and processes for the use cases.
- Assist in troubleshooting issues and optimizing configurations to ensure performance and reliability.
- Enable required technical capabilities of the platform for implementation of the use cases.

6.8.7.5 Integration Support

- Guide the Bank's Data team in integrating the use cases with existing systems, tools, and workflows.

6.8.7.6 Compliance and Security Support

- Implement access controls, encryption mechanisms, and audit trails to maintain data confidentiality and integrity.

6.8.7.7 Automation and Optimization Support

- Support the Bank's Data team in identifying opportunities for automation within workflows associated with use cases.
- Provide recommendations for optimizing resource utilization, including choice of processor units, compute, storage, and memory, to enhance operational efficiency.

6.8.7.8 Support During Deployment and Post-Implementation

- Technical support to the Bank's Data team during the deployment of use cases into production.
- Assist in resolving issues, fine-tuning configurations, and ensuring a smooth transition to production.

6.8.7.9 Reporting and Metrics Support

- Assist the Bank's Data team in configuring dashboards and reporting tools to monitor the performance of additional use cases.

6.9 Testing and quality assurance

6.9.1 Perform Unit Testing

- Develop and document unit test cases.
- Prepare test data and execute unit test cases to validate individual components, including AI models, algorithms, and analytics modules.

6.9.2 Conduct System Integration Testing (SIT)

- Design the SIT strategy, test scenarios, and test cases for all integrated systems, including AI and analytics components.
- Prepare test data, execute test cases, log and resolve defects, and provide root cause analysis.
- Ensure that AI models, cognitive systems, and analytics workflows are fully functional and tested during SIT.
- Provide SIT sign-off upon successful completion.

6.9.3 Execute Functional Testing

- Validate that each application feature, including AI-driven functionalities, works as per the defined requirements.
- Ensure that AI models produce accurate, reliable, and explainable results aligned with business objectives.

6.9.4 Assist the Bank in Acceptance Testing (AT)

- Support the Bank in preparing and executing acceptance testing, including defect logging, resolution, and root cause analysis.
- Assign dedicated resources to support UAT at the Bank's specified premises, including for AI and analytics use cases.
- Provide daily updates on UAT status to the Bank's IT Head or a designated representative, including progress on AI and analytics components.

- Assist the Bank in obtaining acceptance testing sign-off for AI, analytics, and reporting modules.
- Ensure acceptance testing includes validation of AI models' performance, accuracy, and compliance with ethical AI guidelines.

6.9.5 Perform Regression Testing

- Re-run functional and non-functional tests to ensure modifications or updates to AI models, analytics workflows, or reporting systems do not impact overall functionality.

6.9.6 Conduct Performance Testing

- Perform performance testing for AI models, analytics pipelines, and reporting systems before go-live and annually post-go-live.
- Log and resolve performance issues and provide root cause analysis. Share performance and stress test reports with the Bank, ensuring they meet agreed performance criteria (e.g., model latency, scalability, and throughput).

6.9.7 Perform Security and Compliance Testing

- Implement a quality assurance framework to monitor and maintain data quality for AI and analytics use cases.
- Conduct regular audits and reviews to ensure compliance with data governance policies, ethical AI standards, and regulatory requirements.
- Ensure all AI models, analytics workflows, and reporting systems are rigorously tested for security, privacy, and compliance.

6.9.8 Set up the Test Environment

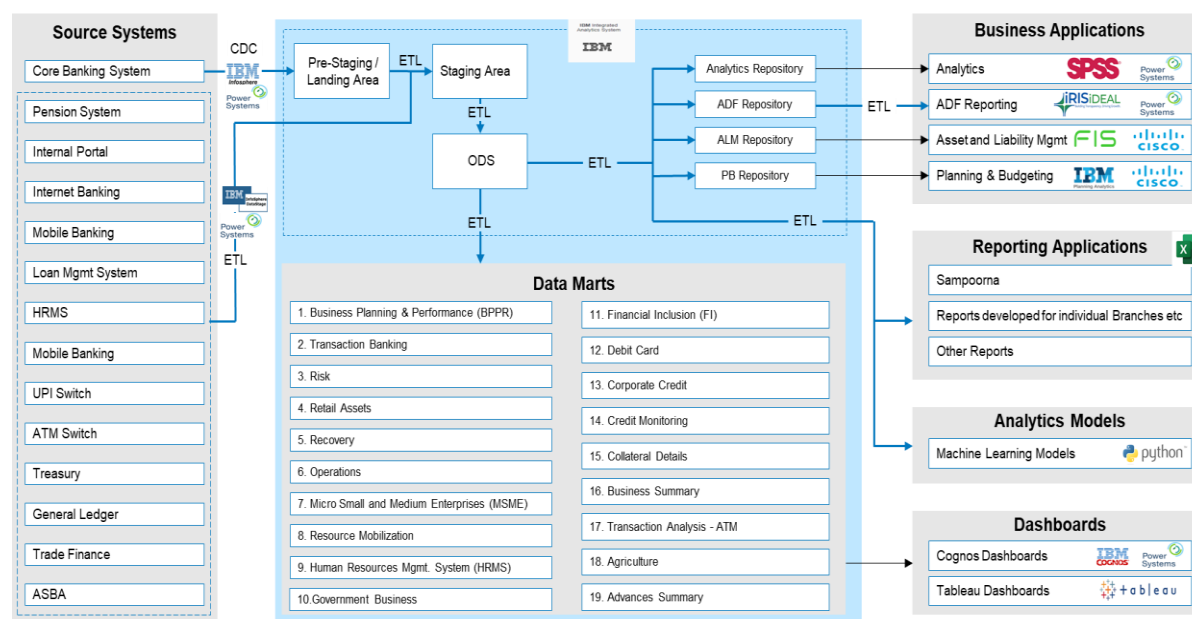
- Configure a test environment that reflects real-world scenarios, including AI and analytics use cases.
- Generate anonymized test data for all attributes as required, ensuring data is suitable for AI model training and testing.

6.9.9 Provide Testing Tools

- Provide and configure tools for user interface testing, functional testing, API testing, and AI-specific testing (e.g., model validation, bias detection, explainability testing).
- Ensure automated unit testing, functional testing, and non-functional testing (e.g., performance, security) are integrated into the CI/CD pipeline.
- Include execution reports as part of release artifacts, with specific focus on AI and analytics components.

6.10 Migration from current Data Infrastructure

High Level Architecture of the current DWH system



The SI should work closely with the existing Technology Partner / Vendors, of the current DWH, source systems and consumer systems for the overall Migration planning and execution.

6.10.1 Assessment and Planning

- Perform a detailed assessment of the existing data infrastructure, including the Data Warehouse, Operational Data Store (ODS), reporting solution, other data assets and Machine Learning (ML) models.
- The current volumetrics for the existing Data Infrastructure have been provided separately in **Annexure 32**.
- Analyse the data architecture, data flows, and dependencies across the existing Data Warehouse, ODS, reporting systems and tools integrated with the DWH solution for business functions.
- Identify and document functional and technical requirements of the Consumer systems [Business Applications, Reporting Applications, Analytica Analytics, Dashboards] that need to be migrated to and / or developed on the new platform, ensuring alignment with the Bank's objectives, operational and regulatory requirements.
- Prepare a detailed migration strategy and roadmap, which must include:
 - Timelines for each phase of the migration process
 - Approach – "Big-bang" or "Phased" migration approach, provided along with rationale for selected approach, execution timelines, component wise details and dependencies (internal and external)
 - Resource requirements, including personnel, tools, and infrastructure
 - Risk mitigation plans to address potential challenges during migration

- Rollback strategy to ensure business continuity in case of migration failure
 - Downtime of the existing applications which are to be migrated, shall be planned during non-peak hours, holidays wherever required. Further, it should not extend till the Business hours.
 - SI/Bidder should plan and provide the temporary requirement of bubble hardware, software, tool if any required to support the migration which should be compatible with the existing hardware and software to achieve the migration timelines
 - If required, The SI shall restore the existing tape data as an initial step and subsequently back it up to the new solution proposed by the SI, ensuring data integrity and availability of the existing Data Warehouse throughout the process
 - Successful SI/Bidder to assess the existing Data, jobs, tables, dashboards, etc and optimize wherever feasible before migrating to the new Data platform.
- Identify and document all data sources (tables and columns), data pipelines, and integrations that need to be migrated to the new platform. This includes ensuring compatibility with the proposed Platform and addressing any dependencies
 - Identify and document all existing applications / systems/ reports built on top of the DWH solution and clearly categorize them into one of the following categories
 - migration from existing data infrastructure to the proposed solution
 - develop them on the proposed solution (with full coverage of existing functional and non-functional requirements
 - sunset / merge
 - SI must ensure that Consuming Applications being migrated, whether through re-pointing or other methods, are abstracted from changes to the data model, integration protocol, authentication mechanism, or other related aspects, as enabled by the proposed data platform.
 - Conduct stakeholder workshops to finalize the migration plan and obtain sign-off from the Bank.
 - Prepare a comprehensive inventory to track each component to be migrated
 - The migration plan must prioritize minimizing manual intervention, ensuring data reconciliation between the existing and proposed systems, and reducing the duration of parallel runs of the legacy and new solutions.

6.10.2 Data Migration

- **Design and Implement ETL/ELT Processes**
Design and implement data extraction, transformation, and loading (ETL/ELT) processes to facilitate the migration of both historical and incremental data from the source tables in the existing DWH infrastructure.

- **Ensure Alignment with the New Platform**
Ensure that all data transformations and mappings are aligned with the new platform's data model and architecture.
- **Encrypted Data Migration**
Either Encrypted data with decryption key or, Decrypted data will be available for migration to the new platform.
- **Perform Data Quality Checks and remediation of issues**
Conduct data quality checks for:
 - **Stock Data:** Data already present in the existing system, ensuring it is cleaned and prepared before migration to the target platform.
 - **Flow Data:** Data being processed as part of the target platform implementation.
 Implement remediation for any identified data quality issues, prioritizing critical data domains and elements.
- **Migrate Data Assets**
Migrate the data assets from the existing DWH ecosystem (including ODS, Data Repositories, and Cubes) to the new platform.
Ensure that the migrated data continues to serve consumers, such as business applications, reporting applications, analytical models, and dashboards, as referenced in the diagram.
Maintain data accuracy, completeness, and consistency throughout the migration process.
- **Validate the Migrated Data**
Validate the migrated data to ensure it matches or improves upon the source data in terms of structure, quality, and integrity.
- **Perform Data Reconciliation**
Perform data reconciliation to verify that all data has been successfully migrated.
Generate detailed reconciliation reports to confirm the accuracy and completeness of the migration process.

6.10.3 Migration of Reporting Solution

- **Maintain Existing Reporting Channels**
Ensure that the existing reporting channels (e.g., Sampoorana) continue to function as-is without any interruptions.
- **Abstract Reporting Channels from Data Model Changes**
The SI must ensure that the existing reporting channels are abstracted from any changes to the underlying data model of the new platform.
- **Preserve Integration Contracts**
Ensure that the reporting channels continue to receive data extracts (e.g., .xls-based or data dump-based) from the target state data platform.
Maintain the existing integration contract, including the format of the data dumps, to avoid any changes or disruptions to the reporting processes.

6.10.4 Migration of Business Applications

- **Planning and Budgeting Application (PB Application):**

Used for Target setting and Performance tracking of Branches. **(Refer Annexure-34)**

Developed using IBM Planning Analytics (TM1)

The SI to evaluate if the application needs to be migrated, re-pointed (Retained) to the target data platform; updated (Refactored); or needs to be designed and developed afresh (Re-developed).

The SI shall be accountable for end-to-end delivery including design, development, testing, operationalization activities for the application, UAT support, performance tuning, production deployment, and post-go-live stabilization, with no exclusions, regardless of the selected option (Retain, Refactor, Re-developed)

In the case of "Re-develop" option, the SI shall also be solely responsible for the sizing, procurement, setup, and commissioning of the requisite Infrastructure (both hardware and software). All associated costs and specifications for this infrastructure must be comprehensively documented and included in the Bill of Materials and the Bill of Quantities.

All the current functional and non-functional capabilities and features of the application need to be matched or improved upon, in the target state platform.

The historical data, specific to this application of the past 7 years, must be migrated to the target state solution.

- **Automated Data Flow (ADF) application:**

Used for automated submission of Regulatory reports to RBI via Integration with CIMS Server – also support Element Based Reporting.

(Refer Annexure-34)

Developed using iRISiDeal

The SI to evaluate if the application needs to be migrated, re-pointed (Retained) to the target data platform; updated (Refactored); or needs to be designed and developed afresh (Re-developed).

The SI will be responsible for all activities around design, development, testing and operationalization activities for the application, regardless of the selected option (Retain, Refactor, Re-developed).

In the case of "Re-develop" option, the SI shall also be solely responsible for the sizing, procurement, setup, and commissioning of the requisite Infrastructure (both hardware and software). All associated costs and specifications for this infrastructure must be comprehensively documented and included in the Bill of Materials and the Bill of Quantities.

All the current functional and non-functional capabilities and features of the application need to be matched or improved upon, in the target state solution.

- **Asset and Liability Manager (ALM) Application:**

Used for regulatory reporting

Developed using Ambit Focus (FIS Balance Sheet Manager)

The SI must ensure that the existing ALM application is abstracted from any changes to the underlying data model, integration contract, integration

protocols and authentication mechanism etc., to avoid any changes or disruptions to the application and continues to function as-is. The historical data, specific to this application of the past 7 years, must be migrated to the target state solution.

- **SPSS Application**

Used to perform statistical analyses and build models without extensive coding

Developed using IBM SPSS.

SI to conduct a situation assessment to determine whether the application needs to be migrated or sunset in the target end state.

Regardless, all Operational Analytics models must be re-developed or migrated to the target-state analytics platform and operationalized with equal or improved performance.

6.10.5 Migration of Business Intelligence Dashboards

Developed using IBM Cognos and Tableau for Operational and Reporting requirements.

The SI to evaluate if the Dashboards need to be migrated / re-pointed to the target data platform without a change to the underlying tool or needs to be designed and developed afresh using a different tool. The SI will be responsible for all design, development, testing and operationalization activities for the dashboards, regardless of the selected option.

The target-state solution must match or exceed all current functional and non-functional capabilities, features, and performance levels of the dashboards.

6.10.6 Migration of Machine Learning Models

- Migrate the existing ML models developed on the ODS to the new platform, ensuring compatibility and performance.
- Support reconfiguring the ML models to leverage the new platform's data architecture and processing capabilities.
- Support validation of the performance and accuracy of the migrated ML models by conducting test runs and comparing results with the existing environment.
- Document the migration process for the ML models, including details of any changes made during the migration.
- Design and implement rollback and fallback mechanisms to safely revert to the existing environment in the event of issues during or after machine learning model migration, ensuring continuity of business operations.

6.10.7 Testing and Validation

- Conduct end-to-end testing of the migrated data capabilities, including functional, performance, and security testing.
- Validate the new platform's ability to support operational requirements, reporting, analytics, and ML model execution.

- Support user acceptance testing (UAT) to ensure the migrated data capabilities meet the Bank's requirements.
- Resolve any defects or issues identified during testing before the final deployment.

6.10.8 Composition of the current Technology stack:

Function	Product Details
Appliance (Data Warehouse)	IIAS M4004-006S
Servers	Cisco UCS (x86 Servers)
Servers	IBM Power Series (S922)
Servers	IBM Power Series (S924)
Servers	IBM Power Series (E950)
Data Pipelines	IBM Infosphere (11.7)
Analytics Model Dev Tools	SPSS (8.2.1)
Asset Liability Management	FIS - 10
Visualization / Dashboard	IBM Cognos Analytics 11.1
Budgeting and Planning	IBM Cognos 2.0.7
Automated Data Flow reporting	IRIS (iDeal)
Change Data Capture	IBM Infosphere - 11.4
Database technology	IBM DB2 - 11.2
Data Warehouse Modelling	BFMDW- 8.9.1
Tape Library	IBM TS4500
Archive Log Backup	IBM V5010E

6.11 Operations and Maintenance

6.11.1 Patch and Configuration Management

- Apply firmware updates, bug fixes, and critical patches for hardware, operating systems, databases, and applications as per Bank policy.
- Ensure all supplied infrastructure and solutions are updated with the latest configurations and consistent setups across the DC and DRC.
- Use ITSM tools to track patching schedules, approvals, and compliance reporting.
- Implement configuration management tools to enforce patching policies and ensure consistency across environments.
- Automate compliance checks to ensure patches meet regulatory requirements
- Use vulnerability scanners to identify missing patches and security vulnerabilities.
- Automate patch notifications and updates from vendors (e.g., OS, hardware, AI frameworks, BI tools)
- Use CI/CD pipelines to automate patch testing workflows in staging environments.

- Implement automated regression testing for Reporting, BI, and Analytics workflows.
- Performance testing tools to validate system performance post-patch.
- Automated rollback mechanisms to revert to previous states if patches fail.
- Automate patch deployment using tools
- Schedule automated patch rollouts during low-usage periods using job schedulers
- Patch and upgrade activities shall follow defined change windows with documented rollback procedures.
- Implement zero-downtime deployment strategies using blue-green or canary deployments.
- Automate AI model performance monitoring to detect degradation in GenAI and Agentic AI capabilities.
- Implement data privacy and security tools to ensure patches do not compromise sensitive data.
- Test and approve all patches and upgrades before deployment on live systems.
- Bear the responsibility for any downtime caused by patching or upgrades not agreed upon with the Bank
- The bidder should inform to the bank if any new version/update/service pack/upgrade of the proposed solution is released by OEM, within seven (7) days of such release and provide the upgraded solution within one month of such release without any cost to the bank covering all parts, labour and accessories at the respective locations (DC and DR) of the Bank during the period of the contract.

6.11.2 Infrastructure Ownership and Management

- Manage the Bank's infrastructure during the contract period, while the ownership of the infrastructure shall remain with the Bank.
- Provide training, knowledge transfer, and detailed documentation to Bank officials and obtain sign-off upon the completion of the contract period.

6.11.3 Facility Management and Maintenance

- Provide onsite facility management services, Level 2 (L2) and Level 3 (L3) support with a 24x7 coverage window, with trained and experienced personnel for the maintenance and management of the supplied hardware infrastructure and system software throughout the contract period.
- Ensure 24x7x365 uninterrupted system availability and resolve issues within the timelines prescribed in the Service Level Agreement (SLA).
- Perform preventive and reactive maintenance, including necessary repairs and replacement of parts, without impacting system performance or uptime during working hours unless approved by the Bank.
- Manage system administration tasks, including:
 - Access control management.
 - User creation and management.
 - Backup and restoration of data and configurations.
 - Production monitoring and troubleshooting.

- The SI/Bidder to provide the Facility Management services (Post Go-Live) support as per below schedule:

Skillset	Coverage Window (Hours X Days)	Minimum Count of Resources
Data Lakehouse	16 x 7	4
Scripting Language	8 x 5.5	2
PL/SQL	8 x 5.5	
Reporting Tools	16 x 5.5	2
Analytical Tools	16 x 5.5	
Ingestion Tool	24 x 7	6
CDC Tool	24 x 7	
Infrastructure and Tools Management	24 x 7	6
Backup and restore	16 x 5.5	
OS Support	24 x 7	
Network Management	24 x 7	5
Security Management	24 x 7	
DBA	24 x 7	5
Total		30

- Minimum Qualification should be BE/B. Tech.
- Minimum post qualification relevant experience should be 5 years
- Any L3 support if required to resolve any issue faced by these L2 resources should be provided onsite/ offsite by the SI/Bidder without any additional cost to the Bank.
- The Roles and numbers may be rationalised (increased or decreased) by the Bank based on the Project Requirement.

6.11.4 **Warranty and AMC**

- Provide a three-year warranty for hardware, starting from the date of successful installation and sign-off by the Bank.
- Comprehensive Annual Maintenance Contract (AMC) for hardware for two years, commencing after the warranty period.
- Provide onsite warranty support for all components, including hardware and software, for the entire contract period
- The warranty shall include:
 - Labor, preventive and unscheduled maintenance, spares, and transport costs.
 - Bug fixes, fault resolution, and elimination of any functional deficits.
 - Replacement or repair of defective parts or systems as per the scope of this RFP.
- Ensure that all goods supplied are brand new, unused, and free from defects in design, materials, or workmanship.
- The warranty shall remain valid even if the Bank integrates supplementary hardware/software from certified third-party vendors.

- Replace or repair defective parts or systems at no additional cost to the Bank during the warranty and AMC periods

6.11.5 Service Level Management

- Maintain service levels as per the RFP and provide periodic reports assessing device performance against SLAs, including availability, uptime, and utilization metrics.
- Implement proactive performance tuning and monitoring to ensure compliance with SLA requirements.
- Establish an escalation mechanism for AMC, ATS, and subscription services to ensure smooth operations

6.11.6 Incident and Change Management

- Establish a robust incident management process, including quick support, automated fault detection, escalation, and resolution.
- Ensure all changes to infrastructure and solutions are recorded, version-controlled, and consistently applied across both DC and DRC.
- Categorize and prioritize incidents by severity
- Provide 36 hours' notice to the Bank for preventive maintenance, including details of changes, testing results, fallback processes, and user impact.
- Maintain an auditable incident register accessible to compliance teams

6.11.7 Compliance and Security

- Assist the Bank in ensuring compliance with regulatory, statutory, and data security requirements, including RBI, NCIIPC, and Bank ISMS & BCMS policies.
- Address vulnerabilities identified by auditors or statutory bodies without additional cost to the Bank.
- Replace hardware or software if vulnerabilities cannot be resolved through updates or fixes, at no extra cost to the Bank.
- The SI shall close audit observations, including secure code reviews, AppSec audits, configuration audits, and VA/PT audits, within stipulated timelines.
- Align AI solutions with organizational risk management, ethics, and internal control frameworks.
- Periodic compliance reports must cover model lineage, data traceability, guardrail activation logs, and exception handling.
- All documentation should be auditable and retained for internal and external review

6.11.8 Business Continuity and Disaster Recovery

- Implement and maintain Business Continuity and Disaster Recovery (BC/DR) readiness, ensuring compliance with the Bank's RTO and RPO objectives.
- Perform real-time data replication between the DC and DR sites and conduct quarterly switch-over and switch-back drills.
- Ensure data operations, such as replication, archiving, cleansing, and purging, are carried out as per agreed frequencies and service levels.
- The proposed Lakehouse solution must ensure that, in the event of a disaster, any data generated within the defined 10-minute RPO window is automatically recoverable from the source, ensuring zero data loss and full data consistency upon recovery.

6.11.9 Information Protection

- Ensure secure backup, storage, and restoration of data, configurations, and mission-critical information required for regulatory compliance.
- Maintain system audit logs for the agreed retention period and archive them offsite as per the Bank's policies.

6.11.10 End of Sales/Support and Roadmap

- Ensure that all supplied solutions and equipment have a minimum support lifecycle of seven years from the date of supply.
- Replace equipment reaching end-of-support within this period with equivalent or upgraded specifications at no additional cost to the Bank.
- Provide a Seven-year roadmap for all solutions, including applications and hardware, from the project sign-off date.

6.11.11 Monitoring and Reporting

- Provide 24x7x365 monitoring and management of the overall solution, including availability and performance of hardware, software, and infrastructure.
- Provide regular performance reports with metrics such as utilization, throughput, and uptime.
- Implement proactive measures based on performance trends to ensure system reliability

6.11.12 Contract Extension

- Support the Bank's right to extend the contract for two additional years (6th and 7th years) on the same terms and conditions, including subscription, AMC, ATS, and onsite services at mutually agreed commercials.

6.11.13 Service Desk

- Provide technical assistance for troubleshooting and managing service requests. (Note: Helpdesk tool, L1 level support will be provided by the Bank)

- Monitor and resolve incidents related to hardware, software, application (including but not limited to implemented functional and non-functional features of the platform) and infrastructure health.

6.11.14 Enhancements and Upgrades

- Provide version upgrades for hardware and software during the contract period, ensuring customizations are carried forward seamlessly.
- Implement enhancements required by statutory, regulatory, or industry standards, as well as additional changes requested by the Bank.

6.11.15 Data Tiering Requirements

- Automated Tiering: Support for policy-driven, automated movement of data across multiple storage tiers (e.g., hot, warm, and cold) based on access frequency, data age, and business requirements to ensure efficient storage management, without manual intervention.
- Performance Optimization: High-performance storage for frequently accessed (hot) data and cost-effective storage options for infrequently accessed (cold) data.
- Transparent Access: Ensure transparent data access across tiers without requiring application-level changes or impacting query performance.
- Scalability: Ability to scale storage tiers independently to meet growing data volume and workload demands.
- Data Lifecycle Management: Support for data retention policies, archival, and deletion workflows to comply with regulatory and business requirements.
- Monitoring and Reporting: Provide tools for monitoring data usage, tiering activity, and storage costs across all tiers.

6.11.16 Data Operations

- Data Archiving and Retention Management:
 - Implement and manage a robust data archiving strategy that aligns with the Bank's data retention policies and regulatory requirements.
 - Ensure that archived data is securely stored in a cost-effective manner, with appropriate indexing and metadata tagging for easy retrieval when required.
 - Periodically review archived data to ensure compliance with retention timelines and regulatory mandates.
 - Provide mechanisms to retrieve archived data efficiently without impacting the performance of the live platform.
- Data Deletion and Purging:
 - Implement automated processes for data deletion and purging based on the Bank's data lifecycle policies and retention schedules.
 - Ensure that data marked for deletion is securely and permanently removed, with no possibility of unauthorized recovery, in compliance with data privacy regulations.
 - Maintain detailed logs and audit trails of all data deletion activities for compliance and reporting purposes.

- Provide mechanisms to handle exceptions, such as data subject requests for deletion under applicable privacy laws.
- **Data Lifecycle Management:**
 - Define and manage the lifecycle of data within the platform, from ingestion to archival or deletion, ensuring alignment with business and regulatory requirements.
 - Classify data based on its criticality, usage, and retention requirements, implementing policies for each classification.
 - Ensure that inactive or infrequently accessed data is moved to lower-cost storage tiers without compromising accessibility when needed.
- **Data Backup and Recovery Operations:**
 - Ensure that archived and live data are included in the backup and recovery strategy, with appropriate recovery point objectives (RPO) and recovery time objectives (RTO).
 - Periodically test the recovery of archived data to validate the effectiveness of the backup and archiving processes.
 - Provide mechanisms to restore deleted or archived data in case of accidental deletion or business requirements.
- **Data Governance and Compliance:**
 - Ensure that all data archiving, deletion, and retention activities comply with the Bank's data governance policies and applicable regulatory requirements.
 - Implement mechanisms to enforce data retention and deletion policies across all data sources and systems within the platform.
 - Provide regular compliance reports and support audits related to data retention, archiving, and deletion.
- **Data Storage Optimization:**
 - Optimize storage utilization by identifying and managing redundant, obsolete, or trivial (ROT) data.
 - Monitor storage usage and provide recommendations for capacity planning and optimization.
- **Data Access and Retrieval:**
 - Ensure that archived data remains accessible to authorized users and applications, with appropriate access controls and permissions.
 - Implement search and retrieval mechanisms for archived data, enabling efficient access to historical information for reporting, analytics, or compliance purposes.
 - Provide tools and processes for retrieving archived data in formats compatible with the Bank's reporting and analytics systems.
- **Data Privacy and Security:**
 - Implement encryption and other security measures to protect archived and deleted data from unauthorized access or breaches.
 - Ensure that data deletion processes comply with privacy laws, including secure erasure of data from all storage media.
 - Provide mechanisms for handling data subject requests, such as the right to be forgotten, in compliance with privacy regulations.
- **Monitoring and Reporting:**
 - Monitor data archiving and deletion processes to ensure they are executed as per defined schedules and policies.

- Generate regular reports on archived and deleted data, including metrics such as data volumes, storage utilization, and compliance with retention policies.
- Provide dashboards and alerts for tracking the status of archiving and deletion activities.
- Data Archiving for AI/ML Models:
 - Archive datasets used for training, testing, and validating AI/ML models, ensuring they are available for future reference or re-training.
 - Maintain version control and metadata for archived datasets to support reproducibility and compliance with AI governance policies.
- Data Archiving for Regulatory and Historical Purposes:
 - Ensure that data required for regulatory reporting, audits, or historical analysis is archived in compliance with applicable laws and standards.
 - Implement processes to retain data for the duration mandated by regulatory authorities, ensuring its integrity and accessibility.
- Automation of Data Operations:
 - Implement automation tools and workflows for data archiving, deletion, and lifecycle management to reduce manual intervention and improve efficiency.
 - Use AI/ML-based tools to identify patterns in data usage and recommend archiving or deletion actions.
- Data Archiving for Analytics and Reporting:
 - Ensure that archived data remains available for historical reporting and analytics use cases, with minimal impact on the performance of the live platform.
 - Provide mechanisms to integrate archived data with analytics tools for trend analysis, forecasting, and other advanced analytics.

6.11.17 Data Backup and Recovery

- Backup Solution Design: The SI must propose a comprehensive and cost-effective solution to store backups of the solution on infrastructure that ensures fast recovery and aligns with the Bank's operational requirements.
- The SI must implement a dual-backup solution, comprising both disk-to-disk (D2D) and disk-to-tape (D2T) backup mechanisms, to ensure comprehensive data redundancy and recovery flexibility for the solution. The specific data elements, tiers, or zones requiring backup, the corresponding backup solution (D2D) or (D2T) to be utilized for each, and the required backup frequency, shall be finalized and agreed upon with the Bank during the detailed design phase of the project.
- Uninterrupted Database Operations: The proposed backup solution must allow users and systems to continue using the database while the backup process is in progress. The background backup process must not degrade the performance of user queries or impact system responsiveness.
- SLA Compliance: The data backup and recovery solutions must support backup and recovery operations in strict adherence to the Service Level Agreements (SLAs) stipulated by the Bank.
- Disk-to-Disk Backup Support: The proposed solution must include robust disk-to-disk backup capabilities to ensure efficient and reliable data storage and recovery.

- Alignment with Bank Policies: The proposed backup and recovery solution must be fully aligned with the Bank's data backup and recovery policy, ensuring compliance with all relevant guidelines and standards.
- The bidder/SI shall document backup architecture and validate restore procedures during implementation.

6.12 **Change Request**

The SI/Bidder shall make available a dedicated Change Request ("CR") Bucket as part of the engagement. The CR Bucket is designed to accommodate business-driven enhancements, new requirements, and unforeseen scope expansions that may arise following Go-Live and throughout the five-year Facility Management Support period. This provision encompasses, but is not limited to:

- Enhancements or extensions to the implemented in Data Lakehouse platform and associated analytics, artificial intelligence features, etc.
- Integration of business applications or data sources beyond those included in the initial scope of work.
- Development and implementation of new use cases, analytical models, data pipelines, dashboards, or modifications to business reporting, etc.

Change Management and Approvals:

- For each change or enhancement proposed under the CR Bucket, the SI/Bidder shall prepare and submit a written effort estimate detailing the scope of work and the anticipated utilization of person-days.
- The proposed estimate and scope shall be subject to the Bank's review and written approval.
- No activity that draws upon the CR Bucket shall commence until the Bank has issued an explicit written authorization for the specific change request.
- All changes must comply with the Bank's change management and approval procedures. Comprehensive documentation shall be maintained for each CR Bucket item to support audit and governance requirements.
- Unused person-days will be carried over to subsequent years, except where specifically agreed in writing by the Bank. All CR Bucket activities shall be managed transparently, with regular reporting provided to Bank stakeholders.

Exclusions:

The CR Bucket shall not be applied to the following activities, which remain covered under facility management support, warranties, or standard maintenance terms:

- Correction of software bugs, defect resolution, and remediation of issues in the platform, business applications, data pipelines, or analytics components.
- Incident response and management, problem resolution, and root cause analysis relating to systems, applications, or infrastructure.

- Infrastructure-related matters including, but not limited to, performance optimization, capacity upgrades, hardware replacement, system recovery, backup and restoration, network configuration, patching, and preventive maintenance.
- Security incident management, vulnerability remediation, and other compliance-related corrective actions.
- Any activity necessary to maintain the availability, reliability, maintainability, and performance of the solution as defined within the Service Level Agreements (SLAs) under Facility Management Support.
- Major or minor version upgrades for the proposed solution, which must be provided at no additional cost to the Bank during the contract term. Minor versions cover incremental updates and patches according to the OEM's release plan and are included within ATS/Subscription services.
- Implementation or changes related to statutory or regulatory requirements as mandated by the Government of India (GOI), Reserve Bank of India (RBI), UIDAI, or other designated regulatory bodies, which shall be provided at no extra cost within the contract period.

The CR Bucket shall be utilized exclusively for business-driven feature evolution and new requirements, with all support, maintenance, and regulatory compliance activities managed under the principal service delivery agreement.

6.13 Regulatory Compliance

6.13.1 Adherence to Regulatory and Statutory Guidelines

- Ensure that the proposed solution, platform, and implementation architecture adhere to guidelines issued by regulatory and statutory bodies, including but not limited to:
 - Government of India (GOI)
 - Reserve Bank of India (RBI)
 - UIDAI, SEBI, IRDAI, TRAI
 - RBI Working Group Document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" (January 2011)
 - RBI Cyber Security Guidelines (June 2016)
 - RBI Master Circular on Digital Payments Security (February 2021)
 - RBI Circular on "Storage of Payment System Data" (April 6, 2018)
 - RBI Master Directions on Outsourcing of Information Technology Services (April 10, 2023)
 - Digital Personal Data Protection (DPDP) Act 2023 of Government of India
 - ISO 27001, ISO 22301, and ISO 27701 standards.
 - RBI Free AI Framework
- Implement all changes, customizations, and enhancements required to comply with existing and future statutory and regulatory directives issued by GOI, RBI, MeITY, Cert-In, UIDAI, and other relevant authorities during the entire contract period, without any additional cost to the Bank.

- Observe, adhere to, and comply with all applicable laws in force or introduced in the future, including those related to their business, employees, or obligations, as applicable to the scope of work.

6.13.2 Audit and Risk Management

- Permit audits by internal and external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in managing the outsourced activity or arrangement.
- Support the Bank in periodic reviews of the outsourced processes to identify and address new outsourcing risks as they arise.

6.13.3 Warranty and AMC Support

- Provide warranty and AMC support for the proposed software, which shall include:
 - Version upgrades, patches, and fixes.
 - Compliance with mandates issued by legal and regulatory authorities, including GOI and RBI.
 - Maintenance support, troubleshooting, performance fine-tuning, and problem resolution for the operating system, database, middleware, and application software.
 - Comprehensive support for the total solution provided by the SI.

6.13.4 Backup, Storage, and Restoration

- Carry out backup, storage, and restoration activities as part of the scope of the RFP, ensuring compliance with:
 - The Bank's ISMS and BCMS policies.
 - RBI guidelines.
 - NCIIPC (National Critical Information Infrastructure Protection Centre) guidelines.

6.14 Data Protection

6.14.1 Compliance with Data Protection Regulations

- Ensure compliance with the Data Protection Act for the solution offered, including its architecture, implementation, and ongoing maintenance.
- Adhere to the Bank's Data Protection Policy, ensuring that sensitive data, including customer Personally Identifiable Information (PII), is stored exclusively within the Bank's premises (at the Data Center (DC) and Disaster Recovery Center (DRC)) and is not moved to any cloud location during its lifecycle.
- Ensure compliance with Digital Personal Data Protection Act 2023 and other regulations as and when released by the regulatory bodies

6.14.2 Deployment of Data Protection Components

- Ensure the solution includes a security component responsible for performing cryptographic techniques (e.g., encryption, hashing) using algorithms such as AES, RSA, ECC, and SHA-2 to protect sensitive data, including customer PII, in accordance with:
 - The Bank's data protection guidelines.
 - Prevailing regulatory, statutory, and legal frameworks.

6.14.3 Cryptographic Key Management

- Integrate with the Bank's existing KMS system for secure generation, storage, and management of cryptographic keys used for encryption, decryption, tokenization, and de-tokenization, if required.
- Leverage the Bank's existing HSM system for storing cryptographic keys, certificates, passwords, and tokens.
- Ensure that the internal design of the component and cryptographic techniques proposed are reviewed and signed off by the Bank's team, including the Chief Information Security Officer (CISO).

6.14.4 Data Protection Functionalities

- Ensure the solution encrypts, tokenizes, and masks sensitive and PII data.
- Ensure the solution supports real-time and bulk batch processing for tokenization, encryption, and masking of sensitive and PII data via APIs or other required means.
- Ensure tokenized data is retrievable on-premises only through APIs or other secure methods by passing the required token.
- Ensure the solution supports digital signing and verification operations to maintain data integrity and authenticity.

6.14.5 Historical Data Management

- Ensure historical data (upto 10 years) is maintained as per the Bank's requirements.
- Implement a data purging and archiving process to manage historical data securely.
- Provide an encrypted data backup and restoration mechanism to ensure data availability and security.

6.15 Documentation

6.15.1 Creation and Maintenance of Documentation

The SI shall create comprehensive documentation for the entire scope of work, including but not limited to below mentioned list of documents and share the same with Bank Team.

All documentation must be version-controlled, continuously updated, and delivered in editable formats with diagrams

- Project Plan: Covering scope, schedule, resources, quality, risk, and communications.
- Business Requirement Document (BRD).
- Non-Functional Requirement Document (NFRD).
- Functional Design Document (FDD).
- Technical Design Document (TDD).
- Interface Design Document (IDD).
- Architecture Diagrams with detailed specifications.
- Migration Strategy document (including current state, gap analysis, script and target state architecture)
- Data Dictionary for each source system including migrated tables and new platform
- Data Governance related documents (Policies for Quality, Catalog, Lineage etc)
- Comprehensive Documentation: Including user manuals, operational guidelines, and compliance reports.
- Requirement Traceability Matrix (RTM).
- Test Plans and Test Scripts with comprehensive test cases.
- Test Summary Reports: Including defect status and details.
- Test Reports and Validation Results for all implemented use cases.
- Performance Test Reports.
- Deployment Plan.
- Installation Qualification or Deployment Manual.
- Release Notes.
- User Handbook: Including screen/report layouts, business workflows, key actions, and support details.
- Security Scan Reports: Covering SAST, DAST, and other relevant scans.

6.15.2 Additional Documentation Requirements

- Provide a System Administrator Handbook, which includes:
 - System security guidelines.
 - User/system access management.
 - Application monitoring and audit trail monitoring.
 - Database administration, including backup, restoration, and archival.
 - Patch deployment and content management.
 - Other maintenance and operational activities.
- Provide maintenance and support documentation, including:
 - Bug fix reports.
 - Root cause analysis (RCA) reports.
 - Workaround implementation reports.
- Document the Business Continuity Planning (BCP) process, including design aspects and operational workflows.
- Document Disaster Recovery (DR) drills, including:
 - Process followed.
 - Reports on outcomes, observations, and action items.
 - Demonstration and documentation of Business Continuity for all DR failure scenarios.
- Provide FAQ documentation and demo videos to enhance understanding of the Data Platform's features.

- Ensure all documentation includes diagrams, screenshots, flowcharts, and simple language for ease of understanding by Bank stakeholders.

6.15.3 Documentation Updates and Accessibility

- Ensure all documentation is updated during upgrades, patching, customizations, or other changes, and provide the updated versions to the Bank free of cost in a timely manner.
- Upload all documentation to the Bank's centralized document repository, always ensuring accessibility to all Bank stakeholders and team members.

6.15.4 Incident Reporting and Root Cause Analysis

- Submit a detailed Root Cause Analysis (RCA) report to the Bank for any incident reported by the Bank related to the supplied hardware or software.

6.16 Training and knowledge transfer

6.16.1 Training

- Training shall be completed within Six months of platform Go-live and should cover all the technical aspects to ensure staff proficiency of the Data Lakehouse platform and tools.
- Develop training materials and conduct training sessions (in-person, within Bank's premises) for bank staff on using the Platform
- Provide training sessions for users and administrators on using the new platform
- Develop documentation including user guides, FAQs, and troubleshooting tips
- Provide ongoing support and guidance to ensure staff proficiency
- Provide technical, functional, operational, and user-level training to Bank staff at the Bank's premises, as and when required by the Bank, during the contract period.
- Deliver user manuals, system requirement documents, system procedure manuals, business requirement documents, implementation methodology, architecture documentation, UAT scenarios, test cases, and sign-off documentation during the contract period.
- Training shall include hands-on, role-based, classroom-style with labs, assignments, sandbox access, and practical exercises. Minimum 40 hours of hands-on technical training per role (Data Engineer, MLOps, AI Engineer, Admin, BI Developer, etc.).

6.16.2 Knowledge Transfer

- Document all processes, configurations, and customizations related to the data platform
- Ensure a smooth handover of the platform to the Bank's IT team, post signoff from the Bank on the completion of the Knowledge Transfer.

6.17 Disaster Recovery

SI must conduct quarterly DR drills, including Full failover, Full failback, Application validation, Data reconciliation, CDC verification, Pipeline run validation, BI dashboard validation and Model Validation.

6.17.1 Disaster Recovery Strategy and Procedures

- The SI must design and implement an adaptable and comprehensive disaster recovery strategy, including detailed procedures for data and application recovery in the event of a disaster.
- The DRC setup must meet the defined Recovery Point Objective (RPO), Recovery Time Objective (RTO), and Service Level Agreements (SLAs).
- The proposed Lakehouse solution must ensure that, in the event of a disaster, any data generated within the defined 10-minute RPO window is automatically recoverable from the source, ensuring zero data loss and full data consistency upon recovery.
- SI must submit DR Architecture, Runbooks, Switchover/Failback SOPs, Network DR Design, and Replication Topology Diagrams.

6.17.2 Infrastructure Resilience and Redundancy

- The infrastructure solution must include dynamic load balancing and automatic path failover capabilities across all components and layers to ensure high availability and fault tolerance.
- Redundant connectivity must be established for all remote locations, connected smart devices, edge devices, and between the Bank's DC (Mumbai) and DRC (Hyderabad) via leased circuits. This redundancy must meet the SLA requirements.

6.17.3 Replication and Data Consistency

- The SI must provide and configure the necessary replication software and disaster recovery management tools to facilitate seamless replication between the DC and DRC sites.
- The storage system must support data replication between similar storage systems in synchronous or asynchronous modes.
- The replication software must ensure data consistency at the DRC site under all circumstances, including link failures and controller failures.
- The DC/DRC infrastructure must support multiple path I/O capabilities from the host and include automatic detection and recovery of failed paths.

6.17.4 Data Ownership and Retention

- The Bank will retain ownership of all data, even if the management of the DC, DRC, and local backup sites is fully outsourced to the SI.
- The SI must propose and implement a data replication and archival strategy that ensures data availability for a minimum of 10 years, as required by the Bank.

6.17.5 DRC Infrastructure Requirements

- The DRC site must replicate 100% of the DC in terms of infrastructure and environment.
- The SI must use modeling techniques to determine the optimal placement of racks in the DC, DR, and local backup server rooms.

6.17.6 Monitoring and Reporting

- The proposed solution must include workflow-based management, monitoring, and reporting capabilities for real-time tracking of DR parameters, such as RPO (at the database level), RTO, and replication status. Alerts (via SMS and email) must be provided for any deviations.

- A unified dashboard must be provided to track the DR readiness status of all applications under DR.
- The SI must provide incident-wise reporting, link availability, loss of link availability, and historical trends for availability to the Bank.

6.17.7 Operational Scenarios

- Business as Usual: Ensure the primary site functions as required, with procedures in place to maintain data consistency and availability at the secondary site.
- Disaster Declaration: In the event of a disaster, the SI must ensure the DRC site is made live for production, enabling user accessibility to the secondary site.
- Operations from DRC Site: The secondary site must perform all required functionalities as expected during disaster recovery operations.

6.17.8 Zero Data Loss and SLR Adherence

- The SI must ensure compliance with all service levels and the zero data loss requirement. Replication across the solution must be maintained as per the Service Level Requirements

6.17.9 Additional Solution Features

- The proposed solution must provide dynamic load balancing and automatic path failover capabilities.
- The solution must offer a single dashboard for tracking DR readiness and provide real-time monitoring and alerts for DR solution parameters.
- The SI must ensure that the proposed solution supports incident reporting, link availability tracking, and historical trend analysis for availability.

6.18 Project Execution Location

- The project must be executed from onsite i.e. at Bank premises.
- Project Manager should be available ONSITE on all regular days and should update the project status on daily basis.
- The complete Implementation Team should also be stationed at Bank's location in Mumbai/Navi-Mumbai.

6.19 Hardware and Software Warranty & AMC

6.19.1 Warranty and AMC/ATS Support

- Provide comprehensive onsite warranty and AMC/ATS for a total of five years for the solutions provided under the scope of the RFP, including hardware, software, associated modules, and services. The warranty shall commence from the date of implementation and sign-off by the Bank.
- Ensure that the warranty and AMC cover version upgrades, patches, fixes, and compliance with mandates, including legal guidelines issued by the Government of India, regulatory authorities, and RBI, as well as maintenance support, troubleshooting, performance fine-tuning, and problem resolution for the OS, database, middleware, and application software.
- Ensure that the warranty and AMC for hardware include preventive maintenance, performance fine-tuning, error rectification, and replacement of parts for all hardware components.

- Provide mission-critical 24x7x365 warranty and AMC support, including proactive and preventive measures and site engineers for hardware and software.
- Ensure that the warranty and AMC cover free provision of spares, parts, kits, and software upgrades to ensure the equipment functions in a trouble-free manner. Faults and failures in the equipment shall be corrected, and defective parts shall be repaired or replaced on a 24x7x365 basis at no additional cost to the Bank.

6.19.2 Roadmap and End-of-Life Management

- Ensure that the proposed hardware and software solutions have a roadmap for at least seven years from the date of going live.
- Ensure that the proposed hardware infrastructure is not declared end-of-service life for a minimum of seven years from the date of going live. Supporting documentation to this effect shall be provided.
- Replace any hardware or software that goes out of support, end-of-life, or sunset during the warranty or AMC period with the next version at no additional cost to the Bank. Such replacements shall be planned to avoid downtime.

6.19.3 Problem Resolution and Service Levels

- Provide assurance that any problem arising during the warranty or AMC period will be rectified immediately without any additional cost to the Bank.
- Guarantee that the services provided under the contract meet the Service Level Requirements specified in the RFP.
- Repair, replace, reconfigure, or re-provision defective equipment or services with all reasonable speed upon receiving written notice from the Bank.
- Ensure that if notified defects are not remedied within a reasonable period, the Bank may take remedial action at the SI's risk and expense, without prejudice to any other rights under the contract.

6.19.4 Licensing and Legal Compliance

- Guarantee that all software supplied is licensed and legally obtained.
- Be fully responsible for the manufacturer's warranty regarding the proper design, quality, and workmanship of all equipment and accessories covered under the offer.
- Warrant all equipment, accessories, and spare parts against manufacturing defects during the warranty period and repair or replace defective components at no additional charge to the Bank.
- Ensure that the warranty remains valid even if the Bank procures supplemental hardware from a third party and installs it with the provided equipment.

6.19.5 AMC/ATS and Payment Terms

- Ensure that the AMC/ATS rates quoted in the Commercial Bid remain valid for two years after the expiry of the five-year contract period.
- Bank at its discretion may extend the AMC/ATS contract upto 2 years after the contract tenure of five years from Go-live.

- Ensure that AMC/ATS charges cover in scope hardware, operating system software, database, application software, and other components, including patches, version upgrades, compliance with mandates and maintenance support.
- Ensure that payments for AMC/ATS are made quarterly in Arrear or Annual advance (on submission of Bank Guarantee of equivalent amount) upon Submission of the Invoice and adjusting any penalty (if any) on account of non-compliance of service level requirements, and any deviation from the proposed payment terms shall not be accepted.
- Agree that the Bank reserves the right to withhold payments in case of delays or defaults by the SI/Bidder. Such withholding shall not constitute a default on the part of the Bank.

6.19.6 Equipment Replacement and Maintenance Standards

- Replace peripherals, components, or equipment with equivalent or higher-capacity items at no cost to the Bank if they are unavailable, difficult to procure, or delayed during the warranty or AMC period.
- Ensure that the same maintenance standards specified for the warranty period are applicable during the AMC period.

6.19.7 ATS for Software

- Ensure that the ATS rates quoted in the Commercial Bid remain valid for two years after the expiry of the five-year contract period.
- Ensure that for subscription licenses, the year-wise subscription price is either the same or higher than that of the preceding year.
- The bidder shall provide assistance for major software upgrades and version changes during the contract term, ensuring smooth transitions and minimal disruption to the Bank's operations. This includes assessing compatibility with existing systems and ensuring user training or documentation for any new features.
- The bidder shall ensure that the software is kept up to date with the latest security patches, bug fixes, and minor version updates throughout the AMC/ATS period. The bidder shall manage the installation of updates and ensure that the software remains secure and compliant with industry standards.
- All patches, upgrades, RBI/NPCI/Other regulators and government agencies' mandate changes and DPDP-compliance updates delivered at no extra cost; deployment coordinated through DevSecOps pipeline

6.20 Certifications

6.20.1 Attainment of ISO Certifications

- The SI shall provide necessary support and technical feasibility to assist Bank in attaining the following ISO certifications for the implemented solution within the specified timelines:
 - ISO/IEC 27001:2022 – For the security of the proposed solution(s), to be achieved by the end of the first six months of the Operations & Maintenance phase.

- ISO 9001:2015 – For operations, to be achieved by the end of the first year of the Operations & Maintenance phase.
- ISO 20000 – For service management, to be achieved by the end of the first year of the Operations & Maintenance phase.

Any observations raised during the process must be closed within the stipulated timelines.

7 Required Artefacts

The SI is required to submit the following documents as part of the technical solution overview, demonstrating their compliance with the defined scope of work and responsibilities

7.1 Platform Architecture

1. Solution Architecture (High-Level and Detailed)
2. Technology Stack and Tools
3. Integration and Security Framework
4. Data Governance and AI/ML Deployment Strategy
5. Scalability and Performance Benchmarking

7.2 Infrastructure Sizing

1. Infrastructure Sizing and Capacity Planning Document (including a detailed description of the methodologies and computations used for determining the sizing and capacity requirements for Infrastructure)

7.3 Implementation Approach

1. Overall Implementation Plan and Roadmap (including Use Case Enablement)
2. Risk and Mitigation Plan
3. Test, Migration, and Deployment Strategy
4. Training and Knowledge Transfer Plan

7.4 Commercials

1. Detailed Cost Breakdown
2. Licensing and Subscription Costs
3. Bill of Materials (BoM)
4. Ongoing Support and Maintenance Plan
5. Total Cost of Ownership for 5 years

7.5 Team and Resources

1. Team Structure and Resource Allocation Plan
2. Resource Deployment Plan

7.6 Case Studies and References

1. Relevant Case Studies
2. Client References

8 Project Timelines

The successful SI/Bidder is expected to adhere to the following timelines concerning the implementation of the solutions/services in Bank:

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Project Planning and Kickoff	2	1.Project Charter. 2.Stakeholder Identification and Communication Plan. 3.Project Scope Document. 4.Work Breakdown Structure (WBS). 5.Project Plan. 6.Risk Management Plan. 7.Resource Plan. 8.Technical Architecture Overview. 9.Governance Framework. 10.Kickoff Meeting Agenda and Minutes.
LLD-platform	8	1.Signed-off Low-Level Design (LLD) for Data Architecture: Approval of the LLD for scalable data architecture, pipelines (ETL/ELT), and integration of structured, semi-structured, and unstructured data. 2.Signed-off LLD for Data Consumption Framework: Approval of the framework covering BI tool integration, concurrent user support, query optimization, caching, and resource utilization strategies. 3.Signed-off Framework for Monitoring: Approval of the framework for monitoring pipelines, models, and overall system health. 4.Signed-off LLD for Governance Framework: Approval of the LLD detailing SOPs, metrics, Data Quality, and Data Lineage tracking mechanisms. 5. Signed-off Consistency and Transparency Documentation: Approval of the framework to identify, map, govern, and ensure transparency and consistency in Data Quality practices. 6. Signed-off Data Security Design: Approval of the design detailing measures to protect sensitive data and ensure compliance throughout the Lakehouse lifecycle.

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
LLD - AI/Gen AI Capabilities	8	1.Signed-off Low-Level Design (LLD) for AI and GenAI Frameworks: Approval of the LLD for the overall AI and GenAI architecture. 2.Infrastructure and Environment Design: Approved LLD details covering infrastructure setup and GPU-enabled training environments. 3.Model Deployment Architecture Design: Approved LLD details defining the model deployment architecture. 4.Data Pipeline and Networking Design: Approved LLD details covering AI/GenAI data pipelines and networking specifications 5.Lakehouse Integration Design: Approved LLD details ensuring seamless Lakehouse integration for efficient ML and AI operations. 6.MLOps Design: Approved LLD details defining the MLOps framework, covering model versioning, automated testing, continuous integration/continuous deployment CI/CD pipelines for models, model monitoring, and automated model retraining/rollback mechanisms.
Delivery of On-Prem Hardware	8	Delivery of Hardware Infrastructure at Bank's DC & DRC along with delivery challan, original invoices, insurance documents etc
Delivery of Software	8	Submission of the Software License along with the License details, product/part code, proof of entitlement on the name of Bank.
Installation of On-Prem Hardware	12	Completion of Hardware Installation and POST Reports for all environments
Completion of Hardware and Software Installation and commissioning for all environments	16	1. Technology Stack Installation Plan. 2. Infrastructure Provisioning and Setup. 3. Configuration Documentation. 4. Technology Stack Architecture Diagram. 5. System Integration Plan. 6. Installation and Configuration Validation Report. 7. Performance Benchmarking Results. 8. Security and Compliance Validation. 9. Monitoring and Alerting Setup.

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Acceptance Test and UAT sign off on implementation of Lakehouse Platform	24	1.UAT Sign-off: Formal approval by the Bank confirming successful completion of all User Acceptance Testing for the Lakehouse platform. 2.Operational Pipeline Validation: Sign-off on the reliable operation of all Data Pipelines and Data Processing workflows. 3.Governance Framework Validation: Sign-off confirming the full implementation and functioning of Data Governance and Data Quality frameworks. 4.Security Framework Sign-off: Confirmation that the defined Security Frameworks are fully implemented and validated. 5.BI and Consumption Validation: Confirmation of seamless data consumption by Reporting and Analytics layers and validated Integration with BI tools. 6.System Integration Sign-off: Confirmation of successful Lakehouse integration with all source and target systems/applications.
Acceptance Test and UAT sign off on implementation of Gen AI capabilities	28	1.UAT Sign-off (AI/GenAI): Formal approval by the Bank confirming successful completion of all UAT for the implemented AI/GenAI use cases 2.Operational Pipeline Validation: Sign-off on the reliable operation of the dedicated AI/GenAI data pipelines and data processing workflows. 3.Security Framework Sign-off: Confirmation that all AI/GenAI specific security frameworks are implemented and validated. 4.ML/AI Environment Validation: Sign-off on the readiness and functionality of the training environments and model deployment architecture. 5.Networking and Integration Sign-off: Confirmation that the networking setup and Lakehouse integration are optimized and validated for efficient AI/GenAI operations. 6.MLOps Sign-off: Confirmation that the MLOps framework is operational, validating model versioning, automated CI/CD, model monitoring, and automated retraining/rollback mechanisms.

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Completion of compliance to IS Audit/VAPT for the Solution	32	Audit/VAPT Closure Report from Bank's Security Team
Production deployment and sign off on implementation of Lakehouse Platform	34	1. Deployment Plan. 2. Operational Data Flow Validation Report. 3. Performance Testing Results. 4. Security and Compliance Validation. 5. Defect Resolution and Open Issues Tracker. 6. Final Acceptance Criteria Checklist. 7. Sign-Off on Successful Production deployment by Bank
Production deployment and sign off on implementation of Gen AI capabilities	36	1. Deployment Plan. 2. Operational Data Flow Validation Report. 3. Performance Testing Results. 4. Security and Compliance Validation. 5. Defect Resolution and Open Issues Tracker. 6. Final Acceptance Criteria Checklist. 7. Sign-Off on Successful Production deployment by Bank
Facility Management Support	2 Weeks from the date of confirmation by the Bank	FMS will start upon Go Live of the Lakehouse Platform, only after obtaining confirmation from the Bank
Migration		
Design and define the migration strategy from the existing DWH to the target Lakehouse platform	10	1.Signed-off Low-Level Migration Plan: Approval of the comprehensive plan covering the migration of data, existing reports, data assets, applications, and analytics models. 2.Scope and Strategy Documentation: Approved documentation detailing the scope, migration approach, tools, and schema mapping strategy. 3.End-State Operational Design: Approved design document detailing the final operational data flow in the new Data Lakehouse platform. 4.Data Migration Playbook: Approved playbook outlining the step-by-step procedures for executing the data migration. 5.Testing and Validation Plan: Approved plan detailing the methodology for testing and validating the migrated data and assets.

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
		6.Risk Assessment and Mitigation Plan: Approved plan identifying potential risks during migration and outlining corresponding mitigation and rollback strategies.
Acceptance Test and UAT sign off on migration from existing DWH infrastructure	36	1. Test Case Documentation. 2. Test Execution Report. 3. Data Validation Report. 4. Defect Log and Resolution Tracker. 5. UAT Test Plan. 6. UAT Test Scenarios and Results. 7. Sign-Off on Successful UAT completion by Bank 8. Operational Data Flow Validation. 9. Performance Testing Results. 10. Migration Success Metrics
Production deployment and sign off on migration from existing DWH infrastructure	38	1. Test Case Documentation. 2. Test Execution Report. 3. Data Validation Report. 4. Final Data Migration Report 5. Defect Log and Resolution Tracker. 6. Production Smoke Test Plan. 7. Production Smoke Test Scenarios and Results. 8. Sign-Off on Successful Production completion by Bank 9. Operational Data Flow Validation. 10. Migration Success Metrics.
Use Case		
Low-Level Design for Wave 1 Use Cases	32	1. Low-Level Design Document: - Detailed design of data flow, pipelines, model integration, and infrastructure. 2. Data Ingestion and Processing Design: - Batch/real-time pipelines for structured, semi-structured, and unstructured data. 3. Feature Engineering Framework: - Design for feature generation, storage, and reuse via a feature store. 4. Model Training and Deployment Design: - Workflow for training, deploying, and serving AI/Gen AI models. 5. Testing and Validation Plan: - Validation of pipelines, features, and model outputs.

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
		6. Technical Architecture Diagram: - Visual representation of the use case workflows.
Low-Level Design for Wave 2 Use Cases	42	1. Low-Level Design Document: - Detailed design of data flow, pipelines, model integration, and infrastructure. 2. Data Ingestion and Processing Design: - Batch/real-time pipelines for structured, semi-structured, and unstructured data. 3. Feature Engineering Framework: - Design for feature generation, storage, and reuse via a feature store. 4. Model Training and Deployment Design: - Workflow for training, deploying, and serving AI/Gen AI models. 5. Testing and Validation Plan: - Validation of pipelines, features, and model outputs. 6. Technical Architecture Diagram: - Visual representation of the use case workflows.
Acceptance Test and UAT sign off on Wave 1 use cases	48	1. Test Case Documentation. 2. Test Execution Report. 3. Defect Log and Resolution Tracker. 4. UAT Test Plan. 5. UAT Test Scenarios and Results. 6. Sign-Off on Successful UAT completion by Bank 7. Reporting and Dashboard Validation. 8. Analytics and Gen AI Model Validation. 9. Performance Testing Results. 10. Training and Knowledge Transfer Materials. 11. Final Acceptance Criteria Checklist.
Production deployment sign off on Wave 1 use cases	50	1. Deployment Plan. 2. Report and Dashboard Validation. 3. Analytics and Gen AI Model Validation. 4. Performance Testing Results. 5. Security and Compliance Validation. 8. Defect Resolution and Open Issues Tracker. 9. Final Acceptance Criteria Checklist. 10. Sign-Off on Successful Production deployment of Wave 1 use cases completion by Bank

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Low-Level Design for Wave 3 Use Cases	52	- Low-Level Design Document: - Detailed design of data flow, pipelines, model integration, and infrastructure. - Data Ingestion and Processing Design: - Batch/real-time pipelines for structured, semi-structured, and unstructured data. - Feature Engineering Framework: - Design for feature generation, storage, and reuse via a feature store. - Model Training and Deployment Design: - Workflow for training, deploying, and serving AI/Gen AI models. - Testing and Validation Plan: - Validation of pipelines, features, and model outputs. - Technical Architecture Diagram: - Visual representation of the use case workflows.
Acceptance Test and UAT sign off on Wave 2 use cases	58	- Test Case Documentation. - Test Execution Report. - Defect Log and Resolution Tracker. - UAT Test Plan. - UAT Test Scenarios and Results. - Sign-Off on Successful UAT completion by Bank - Reporting and Dashboard Validation. - Analytics and Gen AI Model Validation. - Performance Testing Results. - Training and Knowledge Transfer Materials. - Final Acceptance Criteria Checklist.
Production deployment sign off on Wave 2 use cases	60	- Deployment Plan. - Report and Dashboard Validation. - Analytics and Gen AI Model Validation. - Performance Testing Results. - Security and Compliance Validation. - Defect Resolution and Open Issues Tracker. - Final Acceptance Criteria Checklist. - Sign-Off on Successful Production deployment of Wave 2 use cases completion by Bank

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Low-Level Design for Wave 4 Use Cases	60	- Low-Level Design Document: - Detailed design of data flow, pipelines, model integration, and infrastructure. - Data Ingestion and Processing Design: - Batch/real-time pipelines for structured, semi-structured, and unstructured data. - Feature Engineering Framework: - Design for feature generation, storage, and reuse via a feature store. - Model Training and Deployment Design: - Workflow for training, deploying, and serving AI/Gen AI models. - Testing and Validation Plan: - Validation of pipelines, features, and model outputs. - Technical Architecture Diagram: - Visual representation of the use case workflows.
Acceptance Test and UAT sign off on Wave 3 use cases	70	- Test Case Documentation. - Test Execution Report. - Defect Log and Resolution Tracker. - UAT Test Plan. - UAT Test Scenarios and Results. - Sign-Off on Successful UAT completion by Bank - Reporting and Dashboard Validation. - Analytics and Gen AI Model Validation. - Performance Testing Results. - Training and Knowledge Transfer Materials. - Final Acceptance Criteria Checklist.
Production deployment sign off on Wave 3 use cases	72	- Deployment Plan. - Report and Dashboard Validation. - Analytics and Gen AI Model Validation. - Performance Testing Results. - Security and Compliance Validation. - Defect Resolution and Open Issues Tracker. - Final Acceptance Criteria Checklist. - Sign-Off on Successful Production deployment of Wave 3 use cases completion by Bank

Milestones	Timeline in Weeks from the Date of Acceptance of PO	Deliverables
Acceptance Test and UAT sign off on Wave 4 use cases	78	1. Test Case Documentation. 2. Test Execution Report. 3. Defect Log and Resolution Tracker. 4. UAT Test Plan. 5. UAT Test Scenarios and Results. 6. Sign-Off on Successful UAT completion by Bank 7. Reporting and Dashboard Validation. 8. Analytics and Gen AI Model Validation. 9. Performance Testing Results. 10. Training and Knowledge Transfer Materials. 11. Final Acceptance Criteria Checklist.
Production deployment sign off on Wave 4 use cases	80	1. Deployment Plan. 2. Report and Dashboard Validation. 3. Analytics and Gen AI Model Validation. 4. Performance Testing Results. 5. Security and Compliance Validation. 8. Defect Resolution and Open Issues Tracker. 9. Final Acceptance Criteria Checklist. 10. Sign-Off on Successful Production deployment of Wave 4 use cases completion by Bank

Staggered Delivery of Hardware, Associated Components and Software for GenAI:

This is minimum requirement, however, SI/Bidder has to supply the GPUs along with required Infrastructure, associated hardware, software components to meet the use case requirement specified in RFP. Further, the supplied Chassis to be scalable upto 8 GPUs. High Availability is not required for the DC, DR & Sandbox environment. Sandbox should be physically separated.

Year-wise Breakup	DC	DR	Sandbox	Total
Year-1	0	0	2	2
Year-2	3	3	0	6

For Year-3, Bank may purchase additional GPUs, if required at the per unit cost mentioned for the GPU.

The Bank, at its discretion, shall have the right to alter the delivery, implementation schedule and quantities based on the implementation plan. This will be communicated

formally to the SI/Bidder during the implementation, if a need arises. As there are many applications covered under this RFP, Bank will schedule the implementation plan and accordingly for some of the application above schedule will start from the date of intimation by the Bank.

9 Maintenance Support

The SI/Bidder must provide uninterrupted availability of the system and ensure that the problem is resolved within the time schedule as prescribed in the Service Level Agreement (SLA). For any major break down such as crash, the SI/Bidder must arrange for immediate on-site support for recovery and resumption of operations. The re-installation of the software if required is the sole responsibility of the SI/Bidder, which should be treated as service provided under. Maintenance support will also include installation of system updates and upgrades, providing corresponding updated manuals, and follow-up user training. During the ATS period, all upgrades should be free and implemented. All regulatory / statutory changes should be done without any additional cost to the Bank.

Bank will conduct regular Information Security (IS) audit, VAPT, RBI audit, internal audits etc which the successful SI has to support and close, comply all the open observations without any additional cost to the Bank.

Bank also conducts quarterly DR drills which the successful SI has to perform and support without any additional cost to the Bank.

Section-3

Terms & Conditions

10 Liquidated Damage

The successful SI/Bidder must strictly adhere to the schedules for completing the assignments. Failure to meet these Implementation schedule, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the successful SI/Bidder's performance. In that event, the Bank is forced to cancel an awarded contract (relative to this RFP) due to the successful SI/Bidder's inability to meet the established delivery dates, and also the Bank may take suitable penal actions as deemed fit.

Penalty: The successful SI/Bidder shall agree to the penalties structure in accordance with the following:

The Liquidated Damages (LD) shall be 1% of amount for Goods or Services including Delivery, Installation and Implementation of the Hardware, Software, Tools etc. which have been delayed for each week or part thereof for delay until actual delivery or performance.

However, for delay in migration and usecase delivery the below liquidated damages will be applicable:

A. Delay Penalty for Migration Completion

If the 'production deployment and sign-off for the migration of all data assets from the existing Data Warehouse infrastructure', as agreed in writing by the Bank, is not completed within the project timelines specified in Section 8 ("Project Timelines"), unless otherwise agreed in writing by the Bank, the Vendor shall be liable to pay a penalty.

The penalty shall be calculated on the **TCO** for each full week of delay, subject to the following escalating rates:

1. **Initial Rate:** The penalty shall commence **0.1%** of the Sub Total (Item J in Section 19) for each full week of delay during the **first four (4) weeks** following the agreed completion date.
2. **Escalation Rate:** Thereafter, the penalty rate shall **increase by an additional 0.1%** for every subsequent continuous period of four (4) weeks of delay. (e.g., 0.2% per week starting from week 5, 0.3% per week starting from week 9, and so on).

For the purposes of this clause:

1. A "week of delay" refers to a continuous period of seven (7) calendar days beyond the agreed completion date.
2. The penalty shall be applied on a pro-rata basis for any partial week of delay.

The Bank reserves the right to deduct the applicable penalty amount from any payments due to the Vendor under this Agreement or to recover the same.

B. Penalty for Delay in Production Deployment and Use Case Sign-Off for Each Wave

If the 'production deployment and sign-off for use cases in any wave', as agreed in writing by the Bank, is not completed within the project timelines specified in Section 8 ("Project Timelines"), unless otherwise agreed in writing by the Bank, the Vendor shall be liable to pay a penalty.

The penalty shall be calculated on the **TCO** for each full week of delay, subject to the following escalating rates:

1. **Initial Rate:** The penalty shall commence **0.1%** of the Sub Total (Item J in Section 19) for each full week of delay during the **first four (4) weeks** following the agreed completion date.
2. **Escalation Rate:** Thereafter, the penalty rate shall **increase by an additional 0.1%** for every subsequent continuous period of four (4) weeks of delay. (e.g., 0.2% per week starting from week 5, 0.3% per week starting from week 9, and so on).

For the purposes of this clause:

1. A "week of delay" refers to a continuous period of seven (7) calendar days beyond the agreed Go Live date for the specific wave.
2. The penalty shall be applied on a pro-rata basis for any partial week of delay.
3. The penalty shall be calculated and applied separately for each wave where a delay occurs.

The Bank reserves the right to deduct the applicable penalty amount from any payments due to the Vendor under this Agreement or to recover the same.

However, the total amount of Liquidated Damages deducted will be pegged at 10% of TCO quoted by the SI/Bidder of the Summary Sheet of **Annexure 2**.

Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

In this context Bank may exercise both the rights simultaneously or severally. In case the Bank exercises its right to invoke the Bank guarantee and not to terminate the contract, the Bank may instruct to concerned SI/Bidder to submit fresh Bank guarantee for the same amount in this regard.

In the event the Bidder claims that the delay is attributable to the Bank, the Bidder must produce proper, documented evidence to substantiate the claim..

11 Land Border Sharing Clause

The SI/Bidder must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 Order (Public Procurement No. 1), Order (Public Procurement No. 2) dated 23.07.2020 and Order (Public Procurement No. 3) dated 24.07.2020. SI/Bidder should submit the undertaking in **Annexure17: Land Border Sharing**

Undertaking in this regard and also provide copy of registration certificate issued by competent authority wherever applicable.

Para 1 of Order (Public Procurement No. 1) dated 23-7-2020 and other relevant provisions are as follows:

- 1) Any SI/Bidder from a country which shares a land border with India will be eligible to bid in this tender only if the SI/Bidder is registered with Competent Authority.
- 2) "SI/Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of SI/Bidders stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.
- 3) "SI/Bidder from a country which shares a land border with India" for the purpose of this Order means: -
 - i. An entity incorporated, established, or registered in such a country; or
 - ii. A subsidiary of an entity incorporated, established or registered in such a country; or
 - iii. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 - iv. An entity whose beneficial owner is situated in such a country; or
 - v. An Indian (or other) agent of such an entity; or
 - vi. A natural person who is a citizen of such a country; or
 - vii. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

The beneficial owner for the purpose of (iii) above will be as under.

- 1) In case of a company or limited liability partnership, the beneficial owner is the natural person(s). who, whether acting alone or together, or through one or more judicial person, has a controlling ownership interest or who exercises control through other means.

Explanation

- i "Controlling ownership interests" means ownership of or entitlement to more than twenty-five per-cent of shares or capital or profits of the company.
- ii "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.
- iii In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
- iv In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or

through one or more judicial person, has ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.

- v Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
- vi In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- vii An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

12 Monitoring & Audit

Compliance with security best practices may be monitored by periodic computer security audits/Information Security Audits/Statutory and Regulatory audit 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 successful SI/Bidder must provide the Bank access to various monitoring and performance measurement systems. The successful SI/Bidder 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 Successful SI/Bidder. These tools should be a part of the proposed solution.

13 Bid Submission

- 1) SI/Bidders satisfying the eligibility conditions (mentioned in Eligibility Criteria) and General terms and conditions specified in this document, may submit their bid through Government e-Marketplace (GeM) on or before the time-line stipulated in Invitation for Tender Offers.
- 2) All responses received after the due date/time be considered late and would be liable to be rejected. Government e Marketplace (GeM) portal will not allow lodgement of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any SI/Bidder who lodges a late RFP response for any reason whatsoever.
- 3) Bank will not accept the bid through any other mode except GeM.
- 4) Bid Security / Earnest Money Deposit: "Earnest Money Deposit" shall be paid through RTGS (Real Time Gross Settlement) / NEFT (National Electronic Fund Transfer) in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no **GEM/2026/B/7203650** in favour of "Central Bank of India" or by way of Bankers Cheque/Demand Draft/Pay Order favouring Central Bank of India, payable at Mumbai/Navi Mumbai.
- 5) The scanned copy of the receipt of making transaction is required to be uploaded on GeM portal at the time of "final online bid submission The RFP response without proof of amount paid towards Bid Security are liable to be rejected.
- 6) Guarantee of an equal amount issued by a scheduled commercial Bank (other than Central Bank of India) located in India, valid in the form provided in the RFP (**Annexure 13: Bid Security (Earnest Money Deposit)**). The Demand Draft should be of a Commercial Bank only (other than Central Bank of India) and will be accepted subject to the discretion of the Bank.

Tender Schedule (Key Dates):

The SI/Bidders are strictly advised to follow the Dates and Times as indicated in the Time Schedule in the detailed tender Notice (mentioned in page No.____)for the Tender. Ensure that no activity or transaction can take place outside the Start and End Dates and time of the stage as defined in the Tender Schedule.

- 1) At the sole discretion of the tender Authority, the time schedule of the Tender stages may be extended.

14 Integrity Pact

- Each Participating SI/Bidders shall submit Integrity Pact, as per attached **Annexure 9**
- duly stamped for ₹500 (Rupees Five Hundred Only). Integrity pact should be submitted by all participating SI/Bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact, as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process. Hard copy of the Integrity Pact to be submitted to Bank prior to bid opening.
- Bank has appointed Independent External Monitor (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:
 - i. Shri Anant Kumar [anant_in@yahoo.com]
 - ii. Mr. Nirmal Anand Joseph Deva [mail: meghanadeva2022@gmail.com]
- IEM's task shall be to review – independently and objectively, whether and to what extent the parties comply with the obligations under this pact.
- IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently.
- Both the parties accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

15 Technical and Commercial Offers

Technical Offer

- 1) The Technical Offer (TO) should be complete in all respects and contains all the information asked for, in this document.
- 2) It should not contain any price information. But a copy of the commercial bid without mentioning the price should be attached with Technical Offer (TO). However, any mention of price in Technical Offer (TO) will result in disqualification of the bid.
- 3) The Technical Offer (TO) must be submitted in an organized and structured manner. All the product brochures / leaflets / manuals etc. should be submitted along with the Technical Offer (TO). The technical offer should be in compliance with technical requirement / specifications.
- 4) The Technical Offer (TO) must contain proof of submission of bid security. Without any of these two, the SI/Bidder will be disqualified, and bid submitted by them will not be considered for process.

Commercial Bids of only technically qualified SI/Bidders shall be opened on the basis of technical proposal.

The Commercial Offer (CO) should be complete in all respect. It should contain only the price information as per **Annexure 2: Commercial Bill of Materials**.

- 1) The commercial offer should be in compliance with Technical configuration / specifications as per SOW and **Annexure 12: Minimum Technical Specifications**.
- 2) The price to be quoted for all individual items and it should be unit price in Indian rupees.
- 3) In case there is a variation between numbers and words, the value mentioned in words would be considered. The SI/Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the commercial Bid inclusive of all costs. GST (Goods and Services Taxes) shall be payable as per applicable structure laid down under GST Law. The Bank will not pay any other taxes, cost or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, and GST etc. Any increase in GST will be paid in actuals by the Bank or any new tax introduced by the government will also be paid by the Bank. The entire benefits/ advantages, arising out of fall in prices, taxes, duties or any other reason, must be passed on to Bank. The price quoted by the SI/Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out of pocket expense. The Selected SI/Bidder will be entirely responsible for license fee, road permits, NMMC cess, LBT, Octroi, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning. Payment of

Octroi, entry-tax, etc., alone, if applicable, will be made at actuals, on production of suitable evidence of payment by the SI/Bidder.

- 4) **The price is inclusive of taxes like Goods and Services Tax, which shall be paid as per actuals.**

16 Evaluation & Acceptance

- 1) Technical offers will be evaluated by an Evaluation Committee or sub-committee set up for this purpose by the Bank on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those SI/Bidders who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.
- 2) The Minimum Qualifying Marks in the Technical Evaluation is 60% to qualify for the next stage which is commercial opening.
- 3) The Evaluation will be QCBS (Quality Cum Cost Based Solution) which is 70:30 (Technical: Commercial) i.e. The Technical Evaluation and the Commercial Evaluation shall have the weightage of 70% and 30% respectively, and this weightage shall be taken into consideration for arriving at the Successful SI/Bidder.
- 4) In case, any of the successful SI/Bidder is unable to honour in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful SI/Bidder(s) equally or in any ratio decided by the Bank.
- 5) Bank reserves the right to reject the bid offer under any of the following circumstances:
 - i. If the bid offer is incomplete and / or not accompanied by all stipulated documents.
 - ii. If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.
 - iii. If there is a deviation in respect to the technical specifications of hardware items.
- 6) The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons.

17 Evaluation Process

All bids shall be evaluated by an Evaluation Committee or sub-committee set up for this purpose by the Bank. The evaluation shall be on the basis of technical competence and the price quoted.

The Technical Evaluation and the Commercial Evaluation shall have the weightage of 70% and 30% respectively, and this weightage shall be taken into consideration for arriving at the Successful SI/Bidder. The assessment methodology is covered in the next section. The proposals will be evaluated in three stages.

Stage 1 – Eligibility Criteria

Stage 2 – Technical Bid

Stage 3 – Commercial Bid

17.1 Stage 1-Eligibility Criteria

Eligibility criterion for the SI/Bidders to qualify this stage is clearly mentioned in Section-I Eligibility Criteria to this document. The SI/Bidders who meet all these criteria would only qualify for the second stage of evaluation. The SI/Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the SI/Bidder necessarily need to be relevant to the Indian market.

The decision of the Bank shall be final and binding on all the SI/Bidders to this document. The bank may accept or reject an offer without assigning any reason whatsoever.

17.2 Stage 2-Technical Evaluation Criteria

The technical evaluation criterion would broadly involve the below major areas:

1) **Technical Bid Submission:**

- a) **SI Experience:** SI/Bidder must submit the relevant documents demonstrating their experience in implementing the solution, as outlined in Table 1.1.1.1 and 1.1.1.2 for evaluation by the bank.
- b) **Client Credentials:** SI/Bidder to submit all the relevant credentials as mentioned in (**Annexure 27**) which meet the evaluation criteria mentioned in **Client Reference Check** of Table 1.1.1.3; the Bank will evaluate the same and may ask for additional information / clarification if the information is not sufficient. It will however be the sole discretion of the Bank whether the submission is eligible or not for the said evaluation criteria.
- c) **Approach and Methodology:** SI/Bidder to Submit the required Writeup/ documents as per Table 1.1.1.4
- d) **SI Team Skill Set:** SI/Bidder to submit the relevant documents as per Table 1.1.1.5

2) SI Presentation:

- a) SI/Bidder to submit the Document as mentioned in **Evaluation of Solution Architecture** Table 1.1.1.6

SI/Bidder to give Presentation to the Bank's Committee (Date, Time and Venue will be intimated to the SI/Bidder at suitable time by the Bank). The Presentation should cover the Points mentioned in **Walkthrough of Proposed Solution and Implementation Methodology** of Table 1.1.1.7, **Project Timelines** of Table 1.1.1.8, **Resource Deployment for the Project and FM services for the Project** of Table 1.1.1.9 and **Reference Implementation** of Table 1.1.1.10

3) Compliance to the bill of materials as in Annexure 2: Masked Commercial Bill of Material

The SI/Bidder is expected to provide their "compliance" against each item stated in the Bill of material (which should be Masked for the Commercial / price), this means that the SI/Bidder confirms to the provisioning of the stated product / service and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.

4) Compliance to the minimum technical specifications as in Annexure 12: Minimum Technical Specifications

The SI/Bidder is expected to provide their "compliance" against each line item stated in the Minimum Technical Specifications, this means that the SI/Bidder confirms compliance to the stated specifications and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.

- The Technical Bids will be evaluated by the Evaluation Committee based on the technical evaluation criteria and sub-criteria outlined below.
- If deemed necessary, the Evaluation Committee may request clarifications from the SI on relevant aspects of the bid. However, such clarifications shall not permit the SI to alter or make any changes to the substance of the submitted bid or the quoted price.
- Bids will be evaluated for compliance with the requirements outlined in this RFP. Any bid that does not meet 100% compliance with the Minimum Technical Specifications (**Annexure 12**) will be disqualified from further consideration. The Bank also reserves the right to reject bids that fail to meet key mandatory requirements, as determined by the Bank, regardless of their compliance percentage.

Overall Technical Bid Evaluation Parameters

Sr No	Headings	Max Score
1.0	Technical Bid Submission	450
1.a	SI Experience *-	320
	i. Platform setup for Data	100
	ii. Platform setup for Analytics & Gen AI/Agentic AI	50
	iii. Data Transformation (which includes Data Quality, Data cleansing and Data Governance, Data Pipelines etc.)	40
	iv. Data Migration	40
	v. Facility Management	10
	vi. Implementation of Use cases	50
	vii. Experience of Implementing the proposed Lakehouse Solution	30
1.b	Client Reference Check	30
1.c	Approach & Methodology	50
1.d	SI Team Skill Set proposed for the Bank	50
2.0	SI Presentation	350
2.a	Solution Architecture	100
2.b	Implementation Methodology	100
2.c	Timelines for Implementation	50
2.d	Resource Deployment for the Project and FM services for the Project	50
2.e	Reference Implementation	50
	Total	800

17.2.1 Technical Bid Submission

The Technical Bid submitted by the SI/Bidder will be evaluated under as per below parameters:

17.2.1.1 1.a SI Experience

The SI will be evaluated based on its prior experience, as outlined in the criteria detailed in the table below.

All the SI experience will be evaluated for **Implementation or Under Implementation in BFSI sector, RBI, NSE, BSE, Central Government organisation like CBDT, GST, Income Tax etc in India**

Table 1.1.1.1			
#	Criteria	Marks	
	Criteria	Implementation or Under Implementation in BFSI sector, RBI, NSE, BSE, Central Government organisation like CBDT, GST, Income Tax etc in India	
		Count of Implementations / Credentials	Total Score
1.a.i	<u>Platform Setup for Data</u>		
1	<u>On-Premises Data Lakehouse Platform Implementation</u> Successful completion OR under implementation for more than one year of an on-premises Data Lakehouse / Data Lake implementation (minimum size 100 TB) encompassing end-to-end infrastructure setup and other activities like implementation of tools, design and implementation of data ingestion and processing pipelines, execution of ETL/ELT processes, establishment of data governance frameworks, implementation of security measures, integration of data access mechanisms, and development of interactive data visualization and reporting solutions		30 marks per implementation Subject to Max 60 marks
2	<u>On Prem Data Warehouse Platform Implementation</u> Successful completion OR under implementation for more than one year of a On premise Data warehouse implementation (minimum size 500 TB) , encompassing end-to-end infrastructure setup, implementation of tools, design and implementation of data ingestion and processing pipelines, execution of ETL/ELT processes, establishment of data governance frameworks, implementation of security measures, integration of data access mechanisms, and development of interactive data visualization and reporting solutions		20 marks per implementation Subject to Max 40 marks



1.a.ii.	<u>Platform Setup for Analytics and AI/GenAI</u>		
1	<u>On-Prem Platform Setup for Analytics</u> Successful implementation OR under implementation for more than one year of an on-premises hosted Enterprise Platform , incorporating Advanced Analytics capabilities along with ML Model , designed to deliver high-performance data processing, intelligent decision-making, and seamless integration with existing enterprise systems.		10 marks per implementation Subject to Max 20 marks
2	<u>On prem/cloud Platform Setup for AI/Gen AI / Agentic AI</u> Successful implementation OR under implementation for more than one year of an on – premises/cloud based enterprise platform, for AI/Generative AI (GenAI) / Agentic AI functionalities , designed to deliver high-performance data processing, intelligent decision-making, and seamless integration with existing enterprise systems. a) Successful Implementation of the Platform setup b) Under Implementation of the Platform setup		a) 10 marks per implementation Subject to Max 20 marks b) 5 marks per implementation Subject to Max 10 marks
1.a.iii	<u>Data Transformation</u> Successful implementation of a comprehensive data transformation framework on Data Warehouse or Data Lakehouse, especially focussed on Data Quality, Data cleansing and Data Governance, Data Pipelines etc of at least 100 TB implementation size		10 marks per implementation Subject to Max 40 marks
1.a.iv	<u>Migration</u> Successful completion of a comprehensive migration activities like seamless transition of data assets, ETL Jobs, analytical models, associated workflows etc. from an existing data platform to a modern, on-premises Data Lakehouse or Data Warehouse platform of at least 100 TB implementation size		10 marks per implementation Subject to Max 40 marks
1.a.v	<u>Facility Management Services</u> Successful completion OR on-going project of		5 marks per implementation

	a multi-year (minimum contract period of 3 consecutive years) Facility Management Services for an on Premise hosted Enterprise Data Lakehouse or Data Warehouse Platform of at least 100 TB implementation size		Subject to Max 10 marks
--	--	--	-------------------------

Table 1.1.1.1		
#	Criteria	Marks
	Criteria	Implementation in BFSI sector, RBI, NSE, BSE, Central Government organisation like CBDT, GST, Income Tax etc in India
1.a.vi	<u>Implementation of Use Cases</u> (Any 10 out of below mentioned 15 use cases)	
1.a.vi.1	Retail product recommendation system using customer data	5
1.a.vi.2	Creating unified 360-degree view of customer consolidating data from various sources	5
1.a.vi.3	Identifying Customer journey drop-off for various applications like customer on boarding, account opening etc and trigger interventions	5
1.a.vi.4	Customer Churn analytics	5
1.a.vi.5	Building Customer lifetime value scorecard	5
1.a.vi.6	GenAI use cases for generation of tailored sales pitch for RMs, BMs etc.	5
1.a.vi.7	Call summarization using GenAI to extract key insights from customer interaction	5
1.a.vi.8	Autofill for customers with existing data, such as personal details, account information, and transaction history to reduce manual input, minimize errors, and accelerates processes	5
1.a.vi.9	Design and execute personalised digital marketing campaigns	5
1.a.vi.10	Credit risk scoring model	5
1.a.vi.11	Forecasting model for sales target	5
1.a.vi.12	Anomaly detection in customer transaction to identify frauds	5
1.a.vi.13	Underwriting model for loans like unsecured retail loans, housing loan etc.	5
1.a.vi.14	Predelinquency models for customer default	5
1.a.vi.15	Analysing customer transaction to recommend tailor made products for distress MSME customers	5

** For the purpose of evaluation, the SI is required to submit the following evidence for each Project:

- Copy of Purchase Order¹ and Completion Certificate from Client or Under Implementation Certificate for more than one year from the Client
OR
- Email Confirmation¹ from the Client's executive.
OR
- Any other document to the satisfaction of the Bank. However, the Bank reserves the right to contact the client's representative in person or over Call to verify the authenticity of the submitted documentation.

¹ The start date of the referenced Project must be no earlier than five (5) years or if it is more than 5 years, then it should be ongoing project.

1.a.vii Experience of Implementing the proposed Data Lakehouse Solution

Table 1.1.1.2			
#	Criteria	Marks	
	Criteria	Implementation in BFSI sector, RBI, NSE, BSE, Central Government organisation like CBDT, GST, Income Tax etc in India	
		Count of Implementations / Credentials	Max Score
1.a.vii	<u>Experience of Implementing the proposed Data Lakehouse Platform</u> Successful implementation OR under implementation (for more than one year) of the proposed Lakehouse Platform* in the current bid submitted by the SI/Bidder	15	30

* For the purpose of evaluation, the SI is required to submit the following evidence for each Project:

- Copy of Purchase Order¹ and Completion Certificate from Client or Under Implementation Certificate for more than one year from the Client
OR
- Email Confirmation¹ from the Client's executive.
OR
- Any other document to the satisfaction of the Bank

¹ The start date of the referenced Project must be no earlier than five (5) years or if it is more than 5 years, then it should be ongoing project.

17.2.1.2 1.b Client Reference Check

Table 1.1.1.3			
S. No	Focus Area	Maximum marks for each Client	Maximum Score
1.b.1	Designing the Solution and Architecture (of min 100TB size) for Data Lakehouse/ Data Warehouse Feedback on the product/solution implemented, the SI's involvement in Solution designing the architecture, as well as their contributions to the product, solution, use cases, and visualization.	5	10
1.b.2	Implementation Capabilities, timelines adherence and Quality of Implementation (of min 100TB size) for Data Lakehouse/ Data Warehouse Feedback on the SI's capabilities in implementation, adherence to timelines, quality of deliverables, and effectiveness in resolving issues	5	10
1.b.3	Post Implementation Support (of min 100TB size) for Data Lakehouse/ Data Warehouse Feedback on the SI's capabilities in post-implementation support, adherence to SLAs, quality of training provided, and any proposed solution accelerators.	5	10
Total Marks		30	

- The SI must provide the official email addresses of client representatives **for Best 2 implementations.**
- The bank will seek confirmation from the referred clients via email regarding the above-mentioned focus areas.
- The bank may request client visits or telephonic discussions to validate client references (any expenses related to online or on-site client reference checks will be borne by the bank)

17.2.1.3 1.c Evaluation of Approach and Methodology

The SI must include a detailed Project Approach and Methodology, encompassing the work plan and training approach, as part of the Technical Bid.

The Evaluation will be done based on Comprehensiveness, Quality of the **Solution proposed in the current bid** with elaborate Details.

Table 1.1.1.4			
S.No	Criteria	Marks	Supporting Documentation
1.c.1	Detailed work plan	15	Comprehensive implementation plan outlining detailed timelines, specific activities, structured approaches, and methodologies.
1.c.2	Infrastructure Setup, Architecture / Approach	5	The SI must share the Infrastructure design, deployment roadmap, HA/DR plans, and security measures as a part of the bid submission
1.c.3	Platform Setup Architecture / Approach	5	The SI must share a step-by-step methodology, tools/frameworks list for the platform setup as a part of the bid submission
1.c.4	Use case Implementation Approach	10	The SI must share implementation and impact measurement approach for use cases as a part of the bid submission
1.c.5	Innovation and Value-Added Services	5	The SI must highlight innovative approaches, automation, cost optimization strategies, and case studies, if any, as a part of the bid submission
1.c.6	Risk Management and Mitigation Strategies	5	The SI must provide a risk register, mitigation strategies, and contingency plans, as a part of the bid submission
1.c.7	Proposed Knowledge Transfer approach	5	The SI will be required to provide detailed information regarding the Knowledge Transfer approach and strategy, the manpower allocated for conducting and delivering the Knowledge Transfer, the infrastructure and facilities to support training, as well as the processes for delivering, monitoring, managing, and measuring the effectiveness of the Knowledge Transfer.
Total Marks		50	

17.2.1.4 1.d SI Team Skill Set proposed for the Bank

SI/Bidder to submit the Organogram of the Proposed Team structure along with the Roles and Responsibilities. It should be submitted along with the CVs.

Table 1.1.1.5				
S.No	Criteria	Maximum Marks	Total Marks	Supporting Documentation
1.d.1	Organogram Structure along with Roles and Responsibilities i. Team Structure during Implementation period (20 marks) ii. Team Structure Post Implementation period (10 marks) The evaluation will be based on the submission Comprehensiveness, Quality and Coverage etc.	----	30	
1.d.2	Quality of proposed profiles of Key Resources mentioned below who are Responsible to drive the Project along with their Qualification, Relevant Experience, Skills and Domain Expertise. (refer to Annexure 31) i. Project Director ii. Over all Solution Architect iii. In Charge for Data Transformation activity iv. In Charge for AI / Gen AI v. In Charge for Use Case development and implementation In case the Resource for any reasons is not available for the Project an equivalent Resource acceptable to the Bank to be on boarded to the current Project.		20	Quality of proposed profiles as per CV Evaluation Criteria given in RFP
	Total Marks		50	

Indicative Roles along with Experience is broadly mentioned below, however the SI/Bidder / SI can submit suitable Roles and Responsibilities that are required to successfully Implement the Project and Deliver key performance Indicators (KPIs):

	Role	Evaluation criteria
1	Product Owner	1. Experience in implementation of platform with data lake house, Analytics, Generative, Agentic AI capabilities, in the same role, for an Indian BFSI customer. 2. Over 5 years of professional experience as a Product owner, with an overall experience of more than 10 years. 2. Understanding of data, analytics platforms and technologies 3. Proficient in tools like planning and collaboration tools like JIRA and Confluence etc.
2	Scrum Master / Project Manager	1. Experience in similar scale implementation of data and analytics platforms in India (preferably for commercial banks) in the same role 2. Over 5 years of professional experience as a Product owner, with an overall experience of more than 15 years. 2. Understanding of data, analytics platforms and technologies 3. Proficient in tools like planning and collaboration tools like JIRA and Confluence etc.
3	Solution Architect	1. Experience in implementation of an on-premises hosted platform with data lake house, Analytics, Generative, Agentic AI capabilities, in the same role, for an Indian BFSI customer. 2. Ssuccessfully led at least four end-to-end implementations of on-premises Lakehouse platform using the proposed technology, including two for a Bank in India, as a Solution Architect. 2. Proficiency in systems design and architecture of large-scale data and analytics platform - including but not limited to infrastructure, network, platforms, applications and integration 3. Low level design capability - data modelling, APIs, databases, Data Platform, Data governance, SLM / LLM models etc.

	Role	Evaluation criteria
4	Data Engineer	1. Experience in fresh implementation of data lake house with data lake house, Analytics capabilities. 2. Proficiency in SQL, database management and ETL tools 3. Experience with data processing frameworks 4. Strong programming skills (e.g., Python, Java)
5	Database and Platform Administration Lead	1. Experience in fresh implementation of an on-premises hosted large-scale data lake house and analytics platforms 2. Proficiency in database management systems, Enterprise distributed data processing systems. 3. Strong understanding of database security and compliance 4. Experience with performance monitoring tools 5. Knowledge of scripting languages (e.g., Shell, Python)
6	Infrastructure Lead Engineer	1. Experience in fresh implementation of an on-premises hosted large-scale data lake house and analytics platforms the same role 2. Experience with infrastructure design, planning and setup - server hardware, virtualization 3. Proficiency in designing, building and managing infrastructure automation solutions using automation tools 4. Strong understanding of networking concepts and protocols 5. Experience of having installed and configured monitoring tools
7	DevOps Lead Engineer	1. Experience in fresh implementation of large-scale data, analytics platforms in India in the same role 2. Experience in designing, developing and maintaining CI/CD pipeline using DevSecOps best practices and tools 3. Experience and proficiency with infrastructure as code tools 4. Strong proficiency in MLOps setup and management
8	Quality Assurance Lead	1. Experience in fresh implementation of large-scale data lake house, analytics and GenAI platforms (preferably for commercial banks) in India in the same role 2. Experience in test planning and design of framework for unit, integration, system, performance, resiliency, data quality and integrity check 3. Strong programming skills for test automation and expertise in using performance and security testing tools

	Role	Evaluation criteria
9	Security Specialist	1. Experience in fresh implementation of large-scale data lake-house, analytics, GenAI and Agentic AI platforms (preferably for commercial banks) in India in the same role 2. Proficiency in using and integrating with security tools (e.g., firewalls, IDS/IPS, SIEM) 3. Strong understanding of cybersecurity principles and best practices 4. Experience with security standards and compliance 5. Knowledge of penetration testing and vulnerability assessment tools
10	Data Scientist and Machine Learning Engineer	1. Experience in similar sized and natured implementation engagement for commercial banks in India in the same role 2. Proficiency in programming languages (e.g., Python, R) 3. Experience with machine learning frameworks (e.g., TensorFlow, Scikit-learn) 4. Experience with big data technologies 5. Experience in using foundational SLM / LLM models, available on-premises and building GenAI and Agentic AI applications

17.2.2 Scoring of SI Presentation and Solution Evaluation

As part of the evaluation process, the Bank will invite the SI to deliver a presentation, approximately two and half hours in duration, on the proposed solution. Specific details regarding the presentation will be shared with the qualifying SIs at a later stage. The Bank will evaluate the presentations and assign scores accordingly. The scoring of the SI presentation will focus on the following key areas.

17.2.2.1 2.a Solution Architecture

Table 1.1.1.6		
S.No	Criteria	Marks
2.a.i	Technical understanding and coverage of RFP Scope	20
2.a.ii	Utilization of standard design principles, industry-standard frameworks, modern tools, and technologies for building the Platform, implementing data governance, ensuring data quality, enabling MLOps, developing and operationalizing use cases, and the migration strategy, among other aspects	15
2.a.iii	Technology Stack and Tools - Appropriateness of the proposed technology stack	10

Table 1.1.1.6		
S.No	Criteria	Marks
2.a.iv	Demonstration of how Agentic and GenAI capabilities will be integrated into the Lakehouse platform.	10
2.a.v	Design for high availability, fault tolerance, and disaster recovery and Proposed Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	5
2.a.vi	Accuracy and methodology of infrastructure sizing based on data volume, concurrency, and workload requirements. Consideration of scalability for future data growth and increased user demand.	15
2.a.vii	Strategy for migrating data and other assets from the existing platform to the proposed Lakehouse platform.	10
2.a.viii	Testing strategy for Lakehouse implementation, covering functional (analytics, BI, reporting, GenAI validation) and non-functional (performance, scalability, security, reliability) testing through rigorous automated and manual testing processes.	10
2.a.ix	Security strategy covering encryption, access control, data masking, compliance, auditing, and vulnerability management	5
	Total Marks	100

17.2.2.2 2.b Evaluation of Walkthrough of Proposed Solution and Implementation Methodology

Table 1.1.1.7		
S.No	Criteria	Marks
2.b.1	Proposed implementation methodology for Data Lakehouse and Gen AI Platforms setup	40
2.b.2	Implementation plan for Migration of existing Data Warehouse of the Bank to the new setup	20
2.b.3	Implementation plan for Data Transformation which includes Data Quality, Data Governance, ETL Jobs, Data lineage, catalogue etc.	20
2.b.4	Implementation of Use cases, AI/ ML /Gen AI Models, ML Ops etc.	10
2.b.5	Innovative features or approaches proposed by the SI that differentiate their solution from competitors.	10
	Total Marks	100

17.2.2.3 2.c Evaluation of Project Timelines

Table 1.1.1.8		
S.No	Criteria	Marks
2.c.1	a) Proposed timeliness, Milestone based Deliverables with acceleration and overall implementation plan for completion of the Project, delivering key performance Indicators (KPIs), Business Outcomes. b) The Bidder to also submit tangible Business outcomes which they can commit in the Project Year Wise (Year 2 to Year 5) from this Project	50
	Total Marks	50

17.2.2.4 2.d Evaluation of Resource Deployment for the Project and Facility Management Services for the Project.

Table 1.1.1.9		
S.No	Criteria	Marks
2.d.1	Resource Planning for the Implementation of the Project along with their Qualification, Relevant Experience, Skills, Domain Expertise, etc a. Project Director b. Data c. Over all Solution Architect d. In Charge for Data Transformation activity e. In Charge for AI / Gen AI f. In Charge for Use Case development and implementation	30
2.d.2	Proposed Resource Plan for delivering post implementation of Facility Management Services , including roles, responsibilities, covering the Relevant Resources, Experience etc..	20
	Total Marks	50

17.2.2.5 2.e Reference Implementation

Table 1.1.1.10		
S.No	Criteria	Marks
2.e.1	Walkthrough (Detailed Case Study) of at least two references for implementation or under Implementation for atleast 1 year of similar nature (Data Lakehouse/ Data Warehouse) and size (minimum 1PB) in BFSI sector, RBI, NSE, BSE, Central Government organization like CBDT, GST, Income Tax etc in India, hosted <i>preferably</i> on premises, highlighting the technology architecture, methodology, team structure, timelines and KPIs delivered.	25 marks per Implementation
	Total Marks	50

- The SI Presentation will be conducted at a location chosen by the Bank, and the cost of setting up the SI Presentation will be borne by the Bank.
- The SI's responses will be duly recorded and scored. Any workarounds suggested by the SI for functionality may be reviewed by the Bank, and the details will be documented.
- The responses provided by the SI to the functional and technical requirements outlined in the RFP may be subject to questioning and verification during the SI Presentation process.

17.2.3 Final Scoring of Technical Bid Evaluation of Technical Bids

The final Technical Evaluation Score will be calculated as follows:
Technical Bid Evaluation Score (T) = SI Experience + Client Reference Check + Approach & Methodology + SI Team Skill Set proposed for the Bank + SI Presentation

Only those Bidders who have qualified after Stage 2 i.e. Technical evaluation will be eligible for the Commercial Evaluation Stage. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 5 years.

17.3 Stage 3 – Commercial Evaluation Criteria

- Only those SI/Bidders who have qualified after Stage 2 of technical evaluation will be eligible for the further participation in the Procurement process. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 5 years, (total cost of products & services).

- b) The score(s) will be calculated for all technically qualified SI/Bidders using the formula:
- c) $S = (30 \times C_minimum/C_quoted) + (70 \times T_obtained/T_highest)$
- d) $(Minimum\ Commercial\ Quote/Quoted\ Price) \times 30 + (Technical\ Score/Highest\ Technical\ Score) \times 70$.
- e) Technical will carry 70% weightage and Commercial will carry weightage of 30%)
- f) Bank will award the contract to the successful SI/Bidder whose score "S" is the highest as per the above-mentioned formula.
- g) The SI/Bidder shall not add any conditions / deviations in the Commercial Bid. Any such conditions / deviations may make the bid liable for disqualification.
- h) The commercial evaluation would cover Compliance to the Commercial Bid as in **Annexure 2**: The SI/Bidder is expected to provide their "compliance" against each item stated in the Commercial Bid, this means that the SI/Bidder confirms to the provisioning of the stated product or service and the terms of the RFP and subsequent addendums.
- i) The Total cost of Ownership of this tender will be the Grand Total - TCO quoted by the SI/Bidder of the Summary Sheet of **Annexure 2** Commercial Bill of Material.
- j) The SI/Bidder shall not add any conditions / deviations in the commercial bid. Any such conditions / deviations may make the bid liable for disqualification.

Normalization of Bids

The Bank may go through a process of technical and/ or commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that SI/Bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that any of the bids need to be normalized and that such normalization has a bearing on the commercial bid; the Bank may at its discretion ask all the technically shortlisted SI/Bidders to resubmit the updated technical and commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission till the Bank is reasonably satisfied. The SI/Bidders agree that they have no reservation or objection to the normalization process and all the technically short listed SI/Bidders will, by responding to this detailed document, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The SI/Bidders, by submitting the response to this detailed document, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned Bidder.

Bank may call for any clarifications/ additional particulars required, if any, on the technical/ commercial bids submitted. The Bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The Bidder's offer

may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. Bank reserves the right to call for presentation(s), product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. Central Bank of India also reserves the right to conduct reference site visits at the Bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final commercial bidding.

Note: Tendering process need not be cancelled merely on the grounds that a single tender was received provided that the single bid received is evaluated to be substantially responsive and deemed fit for award. Bank reserves right to proceed and award the tender to single bidder in case only one bidder participates in the tender / qualifies in the technical bid evaluation. Bank can negotiate with such single bidder, if required.

During Technical Evaluation the score of the Bidders will not be shared

Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the Commercial Bid. Bank may, at its sole discretion, waive any non-conformity or deviations.

In case, any of the successful bidder is unable to honor in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful bidder(s) equally or in any ratio decided by the Bank.

Bank reserves the right to reject the bid offer under any of the following circumstances:

- i). If the bid offer is incomplete and / or not accompanied by all stipulated documents.
- ii). If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.
- iii). If there is a deviation in respect to the technical specifications of hardware items.

The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons.

18 General Terms

18.1 Important Terms & Conditions:

- a) No open-source software component will be considered in the solution without Enterprise License and OEM's Support.
- b) In case bidder quotes open-source software for any requirement given in the RFP, then it is mandatory for the bidder to quote rightful subscription and support charges to ensure compliance with the service levels defined in the RFP.
- c) Bank reserves a right to extend the AMC, ATS, Subscription and FMS of the proposed Data and Gen AI platform along with the Tools, Licenses and other Solutions for 2 more years i.e. 6th and 7th year on the same terms and conditions wherein enhancements quoted for 4th and 5th year would be taken as the price reference for the extension.
- d) For each of the above items provided the vendor is required to provide the cost for every line item where the vendor has considered the cost in Bill of Material (BOM).
- e) Bank reserves the right to implement or drop any of the listed items without assigning any reason. 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.
- f) The price quoted for the project should be an all-inclusive price including any taxes, expenses and levies but excluding GST and is a fixed price.
- g) Bank will deduct applicable TDS, if any, as per the law of the land.
- h) The quoted fixed cost against each item shall remain unchanged till the completion of the Project(s).
- i) The base project location will be Mumbai/Navi Mumbai.
- j) The TCO in words is amount on which the commercial evaluation will be conducted.
- k) All prices to be valid for a period of 5 years from the date of contract execution / signing / Go-Live.
- l) Bidder should factor all the expenses like travelling, boarding, lodging etc. Apart from amount specified in Commercials, no other expenses will be paid by the Bank.
- m) Bidder shall depute resources on-site of the project implementation location(s) for carrying out the task as specified in this document.
- n) The cost quoted is in fixed price and no increase in rate will be admissible by the Bank for whatsoever reasons during the contract period.
- o) The cost quoted also includes the cost of deliverables for all the phases of the Project.
- p) Further, we confirm that we will abide by all the terms and conditions mentioned in the Request for Proposal document.
- q) Fee is payable only on actual availing of services and no minimum or fixed fees are payable.
- r) Bidder is expected to provide detail bill of material along with the commercial proposal for the proposed hardware and appliances.
- s) Additional Per Man-day rates (applicable in case of enhancement of scope in future). The same will be as per the rate for the respective year quoted in the Commercial Bill of Material. The amount shall be paid on pro-rata basis based on the actual usage. Any unused person-days shall be carry forwarded to the next year.
- t) The AMC cost of Hardware should be minimum 8% of the Product Cost.
- u) The ATS cost System Software shall be minimum 15% of Product Cost.
- v) Bank's may take assistance from Bank's Consultants, Advisors or such Professional Services from any agency in the complete RFP process which includes scrutiny of the Documents, design, Technology, Architecture, Sizing, Implementation Methodology,

Presentations, Final evaluation of the Bids as well as overseeing the Implementation of the Project.

- w) The successful SI shall closely work with the existing DWH- SI / Bank team in complete understanding of the existing landscape of Data warehouse and wherever required, need to optimize the existing jobs for any scope in improving the performance.

18.2 Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision thereto will be applicable for this RFP. As the evaluation of successful bidder is on basis of "Technical Competence and the Price Quoted", the margin of purchase preference to Class-I local supplier shall not be applicable under this RFP.

19 Payment Terms

Payment will be released by the Central office from where the purchase order is issued. All the Payment shall be made in INR only.

The payments will be released only on completion of respective milestones/schedules and signoffs by Bank Team towards Product, License, Subscription, Implementation, AMC, ATS, FMS and any other Cost as under:

Sr No	Category	Milestone	% of Total Hardware Cost
A	Hardware Cost (DC, DR, Dev, UAT, Sandbox)	Delivery acceptance by Bank	30%
		Completion of Hardware Installation and Commissioning	50%
		Sign off on the Production Readiness (after VAPT compliance) for the corresponding new hardware by the Bank.	10%
		180 days post sign-off of the Production Readiness (DR environment)	10%

	Category	Milestone	% of Total Software / License Cost
B	Software Cost (DC, DR, Dev, UAT, Sandbox)	Submission of the License	30%
		Completion of Software Installation and Commissioning	50%

	Category	Milestone	% of Total Software / License Cost
		Sign off on the Production Readiness (after VAPT compliance) for the corresponding new hardware by the Bank.	10%
		180 days post sign-off of the Production Readiness (DR environment)	10%

Sr No#	Category	Milestone	% of Total Lakehouse Implementation Cost
C	Implementation of Lakehouse Platform and Data Transformation (DC, DR, Dev, UAT, Sandbox)	Sign-off on the low-level design document for scalable data architecture, pipelines, and ETL/ELT processes to integrate structured, semi-structured, and unstructured data from source systems into the Data Lakehouse, Framework for data consumption by Reporting and Analytics layers and Integration with BI tools and support for concurrent users, query optimization, caching, and resource utilization strategies and Framework for monitoring pipelines, models, and system health.	5%
		Sign-off on the low-level design document for framework with SOPs, metrics, Data Governance, Data Quality, Data Lineage tracking to identify, Map, Govern, and ensure transparency and consistency in Data Quality practices within the Data Lakehouse ecosystem.	5%
		Sign off on the design for Data Security measures to protect sensitive data and ensure compliance throughout the Data Lakehouse lifecycle.	5%
		Sign-off on UAT completion of the Lakehouse implementation including operationalized Data pipelines, Data processing, Data governance, Data quality, Security	30%

		frameworks, training environments, model deployment architecture, data consumption by Reporting and Analytics layers and Integration with BI tools, ML enablement and Lakehouse integration with source and target systems/application.	
		Sign-off on Production Go Live of the Lakehouse (including operationalized Data pipelines, Data processing, Data governance, Data quality and security frameworks), training environments, model deployment architecture, data consumption by Reporting and Analytics layers and Integration with BI tools, ML enablement and Lakehouse integration with source and target systems/application by the Bank	30%
		3 months post Sign-off by the Bank, on Production Go-Live of the Lakehouse implementation and Successful Testing of Switchover from DC to DR and DR to DC.	25%

Milestone	% of Total AI/GenAI capabilities
Sign-off on the low-level design document for AI and GenAI frameworks, detailing infrastructure setup, GPU - enabled training environments, model deployment architecture, data pipelines, networking, and Lakehouse integration for efficient AI operations.	5%
Sign-off on UAT completion of the AI/GenAI capabilities implementation including operationalized data pipelines, data processing, data governance, data quality, security frameworks, training environments, model deployment architecture, data pipelines, networking, and Lakehouse integration for efficient AI operations	30%

Sr No#	Category	Milestone	% of Total AI/GenAI capabilities
		Sign-off on Production Go Live of the AI/GenAI (including operationalized data pipelines, data processing, data governance, data quality and security frameworks), training environments, model deployment architecture, data pipelines, networking, and Lakehouse integration for efficient AI operations by the Bank	40%
		3 months post Sign-off on Production Go-Live of AI/GenAI capabilities implementation and Successful Testing of Switchover from DC to DR and DR to DC by the Bank.	25%

	Category	Milestone	% of Migration Cost
E	Migration Cost	Sign-off on the low-level migration plan (for data, existing reports, data assets and applications, and analytics models), including scope, approach, tools, schema mapping, testing, and rollback plan, end-state operational data flow design, data migration playbook, testing and validation plan and risk assessment and mitigation plan, by the Bank.	20%
		Sign-off on UAT completion of the migration of data, data hydration pipelines, existing reports, data assets and applications, and analytics models, from existing Data platform to the proposed Platform, by the Bank.	20%
		Sign-off on UAT completion of the operationalized, data processing, data governance like Metadata, Data Catalogue, Data Lineage, Data quality, security frameworks, etc.	20%
		Sign-off on Production Go-Live of the migration of data, data hydration pipelines, existing reports, data assets and applications, and analytics models, from existing Data platform to the proposed Platform, by the Bank.	40%

	Category	Milestone	% of Total Implementation cost for Use cases
F		Wave 1 (comprising 5 Use Cases)	

	Category	Milestone	% of Total Implementation cost for Use cases
	Implementation Cost of Use Cases	Sign-off on the low-level design document for the implementation of use cases	4%
		Sign-off on UAT completion of the implementation of the use cases	6%
		Sign-off on production go-live of the use cases	10%
		3 months of stabilization period after sign-off on production go-live, and sign-off by the Bank	5%
		Wave 2 (comprising 5 Use Cases)	
		Sign-off on the low-level design document for the implementation of use cases	4%
		Sign-off on UAT completion of the implementation of the use cases	6%
		Sign-off on production go-live of the use cases	10%
		3 months of stabilization period after sign-off on production go-live, and sign-off by the Bank	5%
		Wave 3 (comprising 5 Use Cases)	
		Sign-off on the low-level design document for the implementation of use cases	4%
		Sign-off on UAT completion of the implementation of the use cases	6%
		Sign-off on production go-live of the use cases	10%
		3 months of stabilization period after sign-off on production go-live, and sign-off by the Bank	5%
		Wave 4 (comprising 6 Use Cases)	
		Sign-off on the low-level design document for the implementation of use cases	4%
		Sign-off on UAT completion of the implementation of the use cases	6%

	Category	Milestone	% of Total Implementation cost for Use cases
		Sign-off on production go-live of the use cases	10%
		3 months of stabilization period after sign-off on production go-live, and sign-off by the Bank	5%

	Category	Milestone	% of ATS for Software and AMC
G	**ATS for Software and AMC for Hardware (will be paid on respective renewal dates.)	Quarterly in Arrear or Annual advance (on submission of Bank Guarantee of equivalent amount) upon Submission of the Invoice and adjusting any penalty (if any) on account of non-compliance of service level requirements	100%

	Category	Milestone	% of Quarterly Facility Management Services
H	Facility Management Services	Quarterly in Arrear upon Submission of the Invoice and adjusting any penalty (if any) on account of absence from the requisite Bank working days	100%

	Category	Milestone	% of Training cost
I	Training and Knowledge Transfer	Paid on actuals after successful completion of training by respective OEM's/SI and after acceptance and signoff received from the bank	100%

	Category		In INR
J	Change Request	Sign-off on UAT completion of the implementation	60%

		Sign-off on production go-live	40%
	Category		in INR
K	***Sub Total	Sub Total for the entire duration of the contract Hardware Cost + Software Cost+ Implementation of Lakehouse platform + Implementation of AI/GenAI capabilities + Migration Cost + Implementation Cost of Use Cases + ATS for Software and AMC for Hardware + Facility Management Services + Training and Knowledge Transfer + Change Request	

	Category	Milestone	% of 'Sub Total'
K	KPI adherence for early Migration	Paid on achieving Migration milestone at least 1 month prior to the stipulated timelines	2.5 %
	KPI adherence for Use cases	Sign-off on Demonstrated KPI ² adherence ³ (applicable for 2 ¹ out of 5 use cases), following sign off on the Production Go-Live of Wave 1 use cases (5 in total), by the Bank.	0.5% ⁴
		Demonstrated KPI ² adherence ³ , following Production Go-Live of Wave 2 use cases (5 in nos), and sign-off by the Bank (for 2 ¹ out of 5 use cases)	0.5% ⁴
		Demonstrated KPI ² adherence ³ , following Production Go-Live of Wave 3 use cases (5 in nos), and sign-off by the Bank (for 2 ¹ out of 5 use cases)	0.5% ⁴
		Demonstrated KPI ² adherence ³ , following Production Go-Live of Wave 4 use cases (6 in nos), and sign-off by the Bank (for 4 ¹ out of 6 use cases)	1% ⁵
		1. The SI will have the option to select use cases from the list of use cases for a particular wave, to which KPI measurement will apply, before the start of the wave's implementation. 2. The KPI for the use case, focused on quantifiable business results, will be jointly defined by the Bank and the SI before the start of the wave's implementation. The SI will be responsible for developing a mechanism to automatically measure and visualize KPI adherence before the production	

		go-live of the use case. 3. KPI measurement: a. KPI measurement will commence from the start of the Calendar month, following the sign off on Production deployment of the use case by the Bank. 4. Conditional, based on KPI adherence a. 0.5% - Sign-off by the Bank on demonstrated KPI adherence (applicable to use cases with defined KPIs) within the first 3 calendar months, as per the 'KPI measurement' mechanism outlined above c. 0% - For non-adherence to KPIs beyond 3 calendar months, for use cases with defined KPIs, as per the 'KPI measurement' mechanism outlined above. 5. Conditional, based on KPI adherence a. 1% - Sign-off by the Bank on demonstrated KPI adherence (applicable to use cases with defined KPIs) within the first 3 calendar months, as per the 'KPI measurement' mechanism outlined above c. 0% - For non-adherence to KPIs beyond 3 calendar months, for use cases with defined KPIs, as per the 'KPI measurement' mechanism outlined above.
--	--	--

***Bidder is expected to quote the cost for each component.**

****AMC cost should be quoted minimum 8% of the Hardware Cost and ATS (if any) should be quoted minimum 15% of Software Cost. If applicable AMC/ATS cost is not quoted by the bidder, then bidder will have to re-adjust the equivalent amount from the product cost of Hardware and Software to the AMC cost without changing the TCO.**

*****Bidder is expected to quote 5% of TCO against the Sub-Total cost**

Go live will be considered upon operationalization of all respective technical and functional features specified in the RFP document and sign off by Bank.

The bidder will estimate and provide a list of the required Hardware, Software licenses, Subscriptions, Implementation, AMC, ATS, FMS etc required for the Data Lakehouse and Gen AI Solution during the contract period as per the format in Commercial Bid: **Annexure 2** Bill of Material.

1. The Bidder must accept the payment terms mentioned in the RFP document. The Commercial Bid submitted by the Bidder must be in conformity with the payment terms. Any deviation from the payment terms would not be accepted. The Bank shall have the right to withhold any payment due to the bidder, in case of delays or defaults on the part of the bidder. Such withholding of payment shall not amount to a default on the part of the Bank.
2. 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 cost quoted by the bidder in the price bid against such activity / item.
3. All payments will be released within 30 days from the date of receipt of invoice subject to submission of proof of acceptance/signoffs of the respective deliverables by concerned Bank officials and other related documents. Successful Bidder has to submit the invoices, milestone sign-off & other documents required for release of payment.
4. The Bank will pay of undisputed invoices. Any dispute regarding the invoice will be communicated to the selected bidder within 30 days from the date of receipt of the invoice. After the dispute is resolved. Bank shall make payment within 30 days from the date the dispute stands resolved.
5. The required documents to be provided along with original invoice. Original delivery Challans /UAT sign off / Go Live signoff/ DR Drill completion etc as per applicable milestone duly stamped and signed by the Bank Official.
6. The payments will be released on submission of invoice to Bank's Office at CBD- Belapur through NEFT / RTGS/account credit after deducting the applicable LD/Penalty, TDS if any. The Successful Bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code, GSTIN, State Code, State Name, HSN Code etc.

Change Requests / Enhancements in the Application:

1. Any major and minor version upgrades for the proposed solution should be provided without any cost to the bank during the contract period. A minor version is a small incremental version / patching provided by the OEM of the implemented software and does not call for any additional module or licenses. It comes as per the product release plans of the OEM and to be covered under ATS/Subscription.
2. Any implementation/changes forming part of future statutory/ regulatory changes as required under the directives of Government of India (GOI), Reserve Bank of India (RBI), UIDAI etc. should be carried out during the entire contract period without any cost to the Bank.
3. Any version upgrades for the proposed solution should be provided without any cost to the bank during the contract period.

Fixed Price

The commercial offer shall be on a fixed price basis, exclusive of all taxes and levies. No price variation relating to increases in customs duty, excise tax, dollar price variation

etc. will be permitted. The bidder shall pay any other applicable Taxes being applicable after placement of order, during currency of the project only.

Taxes

1. The consolidated fees and charges required to be paid by the Bank against each of the specified components under this RFP shall be all-inclusive amount with currently (prevailing) applicable taxes. The bidder shall provide the details of the taxes applicable in the invoices raised on the Bank. Accordingly, the Bank shall deduct at source, all applicable taxes including TDS from the payments due/ payments to bidder. The applicable tax shall be paid by the bidder to the concerned authorities.
2. In case of any variation (upward or downward) in Government levies / taxes / etc. up-to the date of providing services, the benefit or burden of the same shall be passed on or adjusted to the Bank. If the service provider makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.
3. Goods and Services Taxes (GST) and its Compliance: -
Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Bidder shall have to follow GST Law as per time being enforced along with certain mandatory feature mentioned hereunder.
4. TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the supplier of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person.
5. It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to the Bank by way of commensurate reduction in the prices under the GST Law.
6. If bidder as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.
7. Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

20 Service Level Agreement

1. SI shall ensure compliance with the SLAs defined in the RFP. This section describes the service levels that has been established for the Services offered by SI to the Bank. SI

shall monitor and maintain the stated service levels to provide quality customer service to the Bank.

2. SI understands the magnitude of this Project and that it would require tremendous commitment to financial and technical resources for the same, for the tenure of Contract under this RFP. The SI therefore agrees and undertake that an exit resulting due to expiry or termination of Contract under this RFP or for any reason whatsoever would be a slow process over a period of six (6) months, after the completion of the notice period, and only after completion of the SIs obligations under a reverse transition mechanism. During this period of Reverse Transition, the SI shall continue to provide the Deliverables and the Services in accordance with the contract under this RFP and shall maintain the agreed Service levels. The Bank shall make payment for these services as per terms.
3. The Bank expects the successful SI to adhere to the following minimum Service Levels:
 - i. Any fault/ issue/ defect failure intimated by Bank through any mode of communication like call/e-mail are to be acted upon, to adhere to the service levels. Business/ Service Downtime and Deterioration shall be the key considerations for determining "Penalties" that would be levied on the Successful SI.
 - ii. The selected SI should have 24X7X365 days monitoring, escalation and resolution mechanism.
 - iii. Time bound problem addressing team (onsite) for the complete contract period.
 - iv. SI to arrange for updates required in the system to meet the changes suggested by RBI/Govt. of India/Regulatory/Statutory authorities towards compliance as part of ATS at no extra cost to bank for the entire contract period. Any delay in meeting the timelines would result in a penalty.

The following set of dimensions and key metrics are defined to monitor the performance of the proposed solution, services of selected SI and overall success of the project.

The project timeline, the metrics mentioned in the techno-functional features and the KPIs should be achieved by the successful SI.

Note: It is necessary to meet the specified thresholds given in the metrics for each individual component separately.

Delivery and Implementation:

SL	Metrics	Threshold
1	Achievement of milestones delivered on time	100% of milestones should be delivered by stated timeline mentioned in the RFP document

2	Achievement of use-cases	100% of the use cases should be delivered as per the milestone phases
---	--------------------------	---

Key Metrics:

Category	SLA Metric	Target	Penalty Applicable	Penalty details
Data Ingestion and Processing	Data Availability SLA	Newly ingested data available for querying within 15 minutes (real-time) or 1 hour (batch) in Curated Zone	Yes	0.001 % of the TCO amount per hour or part thereof.
Data Storage and Management	Data Availability (Ability to read and write data to the storage layer without interruptions)	99.9% (monthly) availability of data storage services	Yes	98 % ≤ Data Availability < 99.9 %: 0.01 % of the TCO amount Data Availability < 98 %: 0.025 % of the TCO amount
Support and Incident Management	Severity 1 Incidents - Response Time	Up to 60 minutes	Yes	
	Severity 1 Incidents - Resolution Time	Up to 4 hours	Yes	4 hrs < Resolution Time ≤ 6 hrs: 0.01 % of the TCO amount 6 hrs < Resolution Time ≤ 8 hrs: 0.025 % of the TCO amount 8 hrs < Resolution Time: 0.04 % of the TCO amount
	Severity 1 Incidents - RCA* Time	Up to 24 hours	Yes	
	Severity 2 Incidents - Response Time	Up to 120 minutes	Yes	

Category	SLA Metric	Target	Penalty Applicable	Penalty details
	Severity 2 Incidents - Resolution Time	Up to 8 hours	Yes	8 hrs < Resolution Time ≤ 12 hrs: 0.01 % of the TCO amount 12 hrs < Resolution Time ≤ 16 hrs: 0.025 % of the TCO amount 16 hrs < Resolution Time: 0.04 % of the TCO amount
	Severity 2 Incidents - RCA* Time	Up to 48 hours	Yes	
	Severity 3 Incidents - Response Time	Up to 8 hours	Yes	
	Severity 3 Incidents - Resolution Time	Up to 48 hours	Yes	48 hrs < Resolution Time ≤ 60 hrs: 0.01 % of the TCO amount 60 hrs < Resolution Time ≤ 72 hrs: 0.025 % of the TCO amount 72 hrs < Resolution Time: 0.04 % of the TCO amount
	Severity 3 Incidents - RCA* Time	Up to 72 hours	Yes	
	Severity 4 Incidents - Response Time	Up to 24 hours	Yes	
	Severity 4 Incidents - Resolution Time	Up to 4 Calendar days	Yes	
	Severity 4 Incidents - RCA* Time	Up to 5 Working days	Yes	
System Availability	Uptime of Platform (including underlying Infrastructure,	≥ 99.95% (Monthly) < 21.91 minutes of downtime per month	Yes	Refer to the table 'Penalty for Downtime of Production environment of the Platform' below

Category	SLA Metric	Target	Penalty Applicable	Penalty details
	System, Software, Software tools, ingestion tool, processing, access, consumption capabilities)			
Disaster Recovery	RPO - Recovery Point Objective	Up to 10 mins	No	
	RTO - Recovery Time Objective	Up to 120 mins	No	
Backup Success Rate	Backup Job Success Rate	99.95% success rate for all backup jobs (daily, weekly, fortnightly, monthly etc) measured and enforced monthly, for applicable penalty.	Yes	98 % ≤ Backup Success Rate < 99.95 %: 0.01 % of the TCO amount Backup Success Rate < 98 %: 0.025 % of the TCO amount
Restore Success Rate	Restore Job Success Rate	99.95% success rate for all restore jobs.	Yes	98 % ≤ Restore Success Rate < 99.95 %: 0.01 % of the TCO amount Restore Success Rate < 98 %: 0.025 % of the TCO amount
Monitoring and Alerting	System Monitoring SLA	99.95% uptime for monitoring tools	Yes	98 % ≤ Restore Success Rate < 99.95 %: 0.01 % of the Tool Cost Restore Success Rate < 98 %: 0.025 % of the Tool Cost
	Alerting SLA	Alerts for critical issues triggered within less than 10s detection	**	
Compliance and Audit	Regulatory Compliance SLA	100% compliance with applicable regulations	**	
	Audit SLA	Audit logs retained for a minimum of 1 year and accessible	**	

Category	SLA Metric	Target	Penalty Applicable	Penalty details
		within 5 minutes of request		
	Audit SLA beyond period of 1 year	To be retained and made available within Maximum 24 hours	**	
Query	Query latency	Simple Query-1 < 10s Simple Query-2 < 30s Moderate Query-1 < 48s Complex Query-1 < 2.5 mins Complex Query-2 < 10mins Complex Query-2 < 30 mins	**	Refer to the table for "Query Definition"
	BI Refresh Rate	Less than 2s	**	
BI Dashboard	Report Generation Time	Standard Reports < 5s Complex Reports < 10s	**	
Adhoc Reports (beyond period of 3 years)	Report Generation Time	Maximum 24 hours	**	
Model	Training Jobs except GenAI	Less than 12 hrs	**	
	Inference	Less than 100ms	**	

***Support and Incident Management** - Upon completion of the Root Cause Analysis (RCA), the SI will need to submit a final Corrective and Preventive Action Plan with defined timelines to ensure that such incidents do not occur again.

**Bank will monitor these parameters on adhoc basis - based on incident/ issue /complaints etc, Wherever the SLA is not met in any of the parameters for 2 consecutive months due to Hardware/ Software/ Configuration/Performance issues then the Successful bidder must enhance / upgrade the Infrastructure/ fine-tune the application and / or Solution accordingly without any additional cost to the Bank within a months' time Failing which, Penalty amount of 0.001 % of the TCO amount per week or part thereof will be levied till actual resolution.

Query Definition:

Query Category	Query Complexity	Data Volume (Base → Result)	Result Size Range	Performance SLA
Simple Query-1	2-3 table joins with Primary Index	1 crore → 25,000 records	10 MB – 10 GB	≤ 10 seconds (2000 concurrent connections)
Simple Query-2	2-3 table joins with Primary Index	30 crores → 10 crores records	10 MB – 100 GB	≤ 30 seconds (2000 concurrent connections)
Moderate Query-1	3-4 table joins with interim spool (10-50 crores), sort & group by	50 crores → 10 crores records	100 GB – 500 GB	≤ 48 seconds (2000 concurrent connections)
Complex Query-1	4-5 table joins with/without spool (≥50 crores), sort & group by	≥50 crores → 10 crores records	100 GB – 500 GB	≤ 2.5 minutes (2000 concurrent connections)
Complex Query-2	>5 table joins with spool (≥50 crores), includes 1 table of 3650 crores	≥50 crores → 30 crores records	500 GB – 5 TB	≤ 10 minutes (2000 concurrent connections)
Complex Query-3	>5 table joins with spool (≥50 crores)	≥50 crores → 50 crores records	100 GB – 5 TB	≤ 30 minutes (2000 concurrent connections)

- a) Successful SI will have to guarantee a minimum up time for the Platform and its components, calculated monthly.

The penalty will be calculated as per the details given below:

- Downtime percentage - Unavailable Time divided by Total Available Time, calculated monthly.
- Total Available Time – 24 hrs. per day for seven days a week excluding planned downtime (planned downtime must be explicitly agreed with the bank and to be only provided for exceptional conditions. Ideally, the platform should be designed in a manner that minimizes the need for planned downtime)

- iii) Unavailable Time - Time involved while the solution is inoperative or operates inconsistently or erratically.
- b) The successful SI should demonstrate that the proposed solution meets the required key metrics.
- c) The following definition of severity will apply:

Severity Level	Number of users impacted	Effective Downtime
Severity 1	Issues that entirely prevent the platform and/or dependent business critical use cases, applications, and regulatory reports from being utilized, significantly impair critical functionalities without an available workaround, or severely disrupt the solution's performance for all or a majority of users..	100%
Severity 2	Issues that result in a significant loss of functionality for the platform and/or business critical use cases, dependent applications, and regulatory reports, or degrade functionalities for the majority of users, even if a workaround is available.	90%
Severity 3	Issues that cause a moderate loss of functionality for the platform and/or non-critical business use cases, non-critical dependent applications, and non-critical reports, or degrade functionalities for the majority of users, even if a workaround is available.	80%
Severity 4	Issues related to low-impact functionality of the platform and/or implemented use cases, or informational requests that do not affect core functionality but may influence peripheral activities.	50%

Penalty for Downtime of Production environment of the Platform

Uptime Range (measured Monthly)	Penalty Details (will be deducted from the payable amounts during the contract duration)
100% =< A <= 99.95 %	No Penalty
99.95% < A <= 99.30 %	0.01% of Total Hardware Cost
99.30 % < A <= 99.00 %	0.015% of Total Hardware Cost
A <= 99.00 %	0.02% of Total Hardware Cost

Penalty for Downtime of Development/SIT and UAT environment of the Platform

Uptime Range (measured Monthly)	Penalty Details (will be deducted from the payable amounts during the contract duration)
---------------------------------	--

100% =< A <= 99.00 %	No Penalty
99.00% < A <= 97.00 %	0.005% of Total Hardware Cost
97.00 % < A <= 95.00 %	0.001% of Total Hardware Cost
A <= 95.00 %	0.0015% of Total Hardware Cost

The SI is responsible for performing sizing and provisioning hardware to ensure that the utilization of Compute, Memory, and Storage for all production hardware infrastructure at both the DC and DRC remains below 70% throughout the contract period. If the utilization threshold is breached, a penalty of ₹10,000 per instance per day will be imposed.

Others compliance related:

Description	Penalty Time above resolution time	Penalty Details (will be deducted from the payable amounts during the contract duration)
Quarterly VAPT/any other Compliance Confirmation	Up to 10 Days	NIL
	11 to 20 days	3.0%
	>20 days	5.0%

Penalty for Non-performance:

- a) If the up time for the platform and/or implemented use cases/migrated data assets falls below the guaranteed level, the Bank will impose a penalty as specified. Additionally, if the uptime of the platform and/or implemented use cases/migrated data assets falls below 95% in any given month, the Bank will withhold payment for that month.

Availability Service Level Default

- a) Service Levels will be measured on a monthly basis. The SI's performance to Service Levels will be assessed against Minimum Expected Service Level requirements for each criterion mentioned in the Availability measurement table.
- b) Service Levels will include Availability measurements and Performance parameters.
- c) SI will provide Availability Report on monthly basis and a review shall be conducted based on this report. A monthly report shall be provided to the Bank at the end of every month containing the summary of all incidents reported and associated SI performance measurement for that period.
- d) Performance measurements would be accessed through reports, as appropriate to be provided by SI e.g., utilization reports, response time measurements report, etc.
- e) Cost Reference that is mentioned is billing value for the defaulted period & defaulted component for which SLA will be calculated.

- f) In case of any service default by the SI, the OEM has to take up and deliver the work as defined in the SLA for the contract period.
- g) If selected Vendor materially fails to meet SLA uptime of Production environments for three (3) consecutive months, the Bank may have the right to terminate the contract.
- h) SI is required to provide evidence for ascertaining Severity Levels in absence of which Severity level for the incident would be considered as 1 for the purpose of penalty calculation.

Availability Service Level Default for Facility Management

- a) SI will have to guarantee a minimum attendance of 99 % per resource (i.e., attendance of each of the resources), calculated on a monthly basis. Attendance percentage will be calculated as (100% less Person Non-attendance Percentage) Person non-attendance percentage will be calculated as (Unavailable Time divided by Total Available Time), calculated on a monthly basis.
- b) The attendance percentage would be calculated on monthly basis and the calculated amount would be adjusted from every subsequent quarter payment.
- c) A Service Level Default will occur when the Service Provider fails to meet Minimum uptime (99%), as measured on a monthly basis.
- d) In case any resource is not available continuously for more than 4 hours a day (Under normal circumstances) or 1 day in case of unplanned / emergency leave of any resource then the SI should immediately provide the Bank with an equivalent standby resource for that resource.
- e) If SI fails to meet the onsite Resource Availability in any month, then SI will have to pay the following compensation adjusted with every subsequent quarter payment:

(Minimum attendance Percentage – attendance Percentage) x Current Years Monthly Contract value)

System Availability

- a) System availability is defined as $\frac{\{(\text{Scheduled operation time} - \text{system downtime})\}}{(\text{scheduled operation time})} * 100\%$.
- Where:
- b) Scheduled operation time means the scheduled operating hours of the System for the month. All planned downtime on the system will be deducted from the total operation time for the month to give the scheduled operation time.
- c) System downtime subject to the SLA, means accumulated time during which the System is not available to the Bank 's users or customers due to in-scope system or infrastructure failure, and measured from the time the Bank and / or its customers log a call with the SI's help desk of the failure or the failure is known to SI from the

availability measurement tools to the time when the System is returned to proper operation.

- d) Critical and Key infrastructure of Data Centre and Disaster Recovery Centre will be supported on 24x7x365 days basis.
- e) Downtime shall commence when the respective hardware and or its associated software fails.
- f) Uptime will be computed based on the service availability of the in-scope components. Also, non-compliance with performance parameters for business and system / service degradation will be considered for downtime calculation.
- g) Response may be telephonic or onsite. In case the issue cannot be resolved telephonically, SI (as per the criticality and nature of the issue) will provide onsite assistance at respective locations (DC and DRC) within response resolution window.
- h) If any one or more of the components defined in –Critical at the Data Centre and Disaster Recovery Facility are down resulting in non-availability of Solution, then affected services / components listed in the –Critical availability measurements table shall be considered for calculating the system downtime.
- i) Real time replication of application and data should happen between the DC and DRC.
- j) Service Levels will be complied with irrespective of the customizations that would undergo during the tenure of the Contract.
- k) Typical Resolution time will be applicable if services are not available to the Bank's users and customers and there is a denial of agreed services.
- l) The SI to provide warranty & AMC support on all days (24X7X365 days) for period of contract.
- m) Bank has defined in-scope services and corresponding SLAs as under, Bank shall evaluate the performance of the SI on these SLAs compliance as per the periodicity defined.
- n) SI shall provide reports to verify the SI's performance and compliance with the SLAs. Automated data capturing and reporting mechanism will be used for SLA reporting. The bank will leverage existing/future EMS tools to monitor and manage the Solution/IT Infrastructure.
- o) If the level of performance of Successful SI for a particular metric fails to meet the minimum service level for that metric, it will be considered as a Service Level Default.
- p) The maximum cumulative amount deductible by the Bank under penalties (excluding Liquidated Damages) over the tenure of the contract shall not exceed 10% of the TCO quoted by the SI/Bidder of the Summary Sheet of **Annexure 2**. The liability for Liquidated Damages shall be capped separately as mentioned in Section 10, and this 10% penalty ceiling is exclusive of that LD amount.

- q) Penalties if any, as defined by SLAs, shall be adjusted in the payment of a quarter. Balance penalties, if any, shall be levied in the payment for the subsequent quarter.
- r) The SI to provide Support contract backline to OEM for the complete duration of contract period. Letter to be provided by service for the backline proof, prior to release of payment.
- s) SI agrees to ensure that all the items / products used for delivering services to the Bank including all components are new and are using state-of-the-art technology. SI shall provide such proof of the new equipment (e.g., Copy of invoice etc.) to the Bank. In the case of software supplied with the system, Successful SI shall ensure that the same is licensed and legally obtained in the name of end customer i.e., Bank with valid documentation made available to the Bank.
- t) Note: All service level penalties will be reconciled at the end of every quarter.

Other terms and Penalties

- a) In case of temporary substitute equipment installation, the temporary substitute equipment should be replaced by the original equipment duly repaired or replaced with similar equipment of the same capacity or higher capacity, failing which a penalty of 0.5% per day of the item cost will be imposed for the number of days the device is down subject to a maximum of 10% of the equipment cost.
- b) The amount of penalty will be recovered from the SI from payments due to them. In case no payments are due, the SI has to remit the same within 15 days of claim from the Bank failing which the Bank shall be at liberty to invoke Bank Guarantees provided for during warranty period by the successful SI. However, if the Platform and/or implemented use cases and/or migrated data assets is/are down due to the reasons attributable to the Bank, the SI has to submit proof for the same for not levying the penalty.

Availability Service Credit Computation

- a) In the event of an Availability Service Level Default, SI shall pay the Bank an Availability Service Credit that will be computed in accordance with the following formula:
- b) $\text{Monthly Service Level Default} = \text{Minimum Service Level} - \text{Monthly Actual Service Level}$
- c) $\text{Availability Service Credit} = \text{Quarterly Service level default} \times (\text{Summation of Cost References})$
- d) If an Availability Service Level Default has occurred for more than one service level requirement, the sum of the corresponding Availability Service Credits shall be

credited to the Bank. SI shall review with the Bank, monthly from the start of Contract Execution, any entitlement of the Bank to an Availability Service Credit.

- e) The total amount of Availability Service Credit that SI is obligated to pay the Bank shall be reflected in the invoice provided to the Bank in the quarter after the quarter in which the Service Levels were assessed.
- f) The Bank shall be entitled to deduct the Availability Service Credit amount from the amounts payable by the Bank to the SI as per the invoice. In case if there are no pending invoices to be paid by the Bank to the SI, the SI has to submit Credit Note / pay order / cheque payable at Navi Mumbai in favor of Central Bank of India for the same within 15 days from the notice period from the Bank.
- g) SI has to note that the total cost of products and services is exclusive of taxes for the purpose of computation of the service level and service credit.

Service Levels during Post implementation phase

- a) The SI is expected to complete the new changes / functionalities / responsibilities that have been assigned as per the agreed Change order timelines, for new deliverables.
- b) Penalty would be levied for implementation delays for new requirement and shall be a maximum of 50% of the total cost of that change solution finalized between the bank and vendor.

Tables of Incident Matrix

Incident to be reported within (if unresolved)	Escalation Hierarchy
15 min	Senior Manager-Cent Neo of the Bank
1 hour	Chief Manager –Cent Neo of the Bank
2 hours	Assistant General Manager Cent Neo / Deputy General Manager Cent Neo
> 4 hours	General Manager Cent Neo

21 Reporting of Material Adverse Events and Incident Management

The Bidder shall promptly report any material adverse events, including but not limited to data breaches, denial of service attacks, service unavailability, security vulnerabilities, unauthorized access, system failures, or any other incidents that may impact the Bank's operations or data integrity. Such incidents shall be reported to the Bank immediately upon identification, enabling the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines. The service provider shall provide all relevant details and updates regarding the incident, including the nature, scope, impact, and

corrective actions taken, in accordance with the Bank's incident reporting procedures.

22 Insurance

The equipment (hardware/software, etc.) supplied under the contract shall be fully insured by the Service Provider against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery, and installation. The insurance shall be obtained by the Service Provider, naming Central Bank of India as the beneficiary, for an amount equal to 100% of the invoiced value of the goods on an "all risks" basis, covering risks such as damage, theft, fire, or natural disasters. The period of insurance shall remain in effect until the supplied components are accepted by the Bank, and the rights to the property are transferred to the Bank at its premises. In the event of any loss or damage, the Service Provider shall initiate and pursue the claim until settlement. Additionally, the Service Provider must promptly make arrangements for the repair and/or replacement of any damaged items, irrespective of the settlement of the claim by the underwriters. Furthermore, the Service Provider shall ensure that the insurance policy remains valid throughout the supply, transportation, and installation period, and any gaps in coverage shall be rectified immediately. The Service Provider shall also provide the Bank with necessary documentation of the insurance policy, claim details, and any associated correspondence with the underwriters.

23 Order Cancellation

Bank reserves the right to cancel the contract placed on the service provider and recover expenditure incurred by the Bank under the following circumstances. If the service provider commits a breach of any of the terms and conditions of the bid, or if the service provider goes into liquidation, voluntarily or otherwise, the Bank reserves the right to cancel the contract. Additionally, if an attachment is levied or continues to be levied for a period of seven days upon the effects of the bid, the Bank may take appropriate action. If the service provider fails to complete the assignment as per the timelines prescribed in the RFP and any extension allowed, it will be considered a breach of contract, and the Bank reserves its right to cancel the order in the event of delay and forfeit the bid security/performance Bank guarantee as liquidated damages for the delay. If deductions on account of liquidated damages exceed more than 10% of the total TCO quoted by the SI/Bidder of the Summary Sheet of **Annexure 2**, the Bank reserves the right to cancel the contract.

After the award of the contract, if the service provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the service provider is bound to make

good the additional expenditure that the Bank may have to incur in executing the balance contract. This clause is applicable if, for any reason, the contract is cancelled. The Bank reserves the right to recover any dues payable by the service provider from any amount outstanding to the credit of the service provider, including pending bills and/or invoking the Bank guarantee under this contract.

In addition to the cancellation of the purchase order, the Bank reserves the right to appropriate the damages from the Bid Security / Performance Bank Guarantee given by the service provider and/or foreclose the Bank guarantee given by the service provider against the advance payment and may take appropriate action. Further, in case of failure to adhere to the terms and conditions of the RFP in totality, concealment of facts in the tender documents, or failure to fulfill the contractual obligations of the Purchase order, the Bank may debar/blacklist the service provider from participating in future tender processes. The Bank reserves the right to inform IBA/other Banks about blacklisting the service provider in case of default in service or delay leading to financial or reputational loss, loss of time of the Bank.

24 Indemnity

24.1 General Indemnity

- i. The Bidder shall indemnify, defend, and hold harmless the Bank, its employees, personnel, officers, directors, agents, and representatives from and against all losses, liabilities, claims, actions, damages, costs, and expenses (including legal fees) arising directly or indirectly from or in any way related to any of the following:
 - a. The Bank's authorized or bona fide use of the Deliverables and/or Services provided by the Bidder under this RFP, or any terms and conditions stipulated in the SLA (Service Level Agreement) or Purchase Order (PO).
 - b. Any act, omission, or failure by the Bidder, its employees, agents, or subcontractors in the performance of the Bidder's obligations under this RFP, SLA, or PO.
 - c. Any claims made by employees, agents, or subcontractors of the Bidder against the Bank.
 - d. Any breach of any term or condition of this RFP or any representation, warranty, or assurance made by the Bidder under this RFP, SLA, or PO.
 - e. Any claims arising out of the Deliverables or Services infringing any patents, trademarks, copyrights, or other intellectual property rights.

- f. Any breach of the confidentiality obligations by the Bidder under this RFP, SLA, or PO.
- g. Any negligence, gross misconduct, or failure to exercise reasonable care by the Bidder or its employees, agents, or subcontractors.

24.2 Patent, Copyright, Trademark, and Intellectual Property Infringement

- i. The Bidder shall, at its own cost and expense, defend or settle any claim that the Deliverables and Services provided under this RFP infringe upon any patent, utility model, industrial design, copyright, trade secret, mask work, trademark, or any other intellectual property right in the country where such Deliverables and Services are used, sold, or received. The Bank shall:
 - a. Notify the Bidder in writing of any such claim as soon as practicable; and
 - b. Cooperate with the Bidder in the defence and settlement of the claim.
- ii. The Bidder shall not settle or compromise any such claim in a manner that would diminish the rights of the Bank or increase the obligations of the Bank under this Agreement, without obtaining prior written consent from the Bank. If the Bidder elects not to defend the claim, the Bank shall have the right to defend or settle the claim, at the Bidder's cost, and the Bidder shall reimburse the Bank for all associated costs, including any damages, settlements, legal fees, and other expenses. Should the amount payable to the Bidder be insufficient to cover the costs incurred by the Bank, the Bidder shall promptly reimburse the Bank for all such amounts.
- iii. The Bidder shall indemnify the Bank in the event of any mismatch in Input Tax Credit (ITC) in the GSTR-2A, especially where the Bank does not opt for retention of GST components on supplies.
- iv. If the Bidder fails to fix bugs, provide required modifications, enhancements, or customizations, or fails to meet the Service Levels as agreed upon in this RFP, SLA, or PO, the Bidder shall compensate the Bank for any direct financial loss suffered by the Bank due to such failure.
- v. The Bidder shall indemnify, protect, and save the Bank against all claims, losses, costs, damages, expenses, actions, suits, and proceedings resulting from any infringement of intellectual property rights (including patents, trademarks, copyrights, etc.), or statutory infringements under laws such as the Copyright Act, 1957, Information Technology Act, 2000, or any other applicable law, in respect of any Hardware, Software, network

equipment, or other systems supplied by the Bidder to the Bank. The Bank must notify the Bidder in writing upon becoming aware of any such claims.

- vi. The Bidder shall have sole control over the defence of such claims and settlement negotiations.

The Bank shall provide reasonable assistance, information, and authority to the Bidder for defending these claims.

- vii. Indemnity under this Agreement shall be limited to the damages awarded by the court or in arbitration, and shall exclude any indirect, incidental, or consequential damages. However, indemnity shall cover all damages, losses, or liabilities arising from claims made by regulatory authorities.
- viii. The indemnity obligations of the Bidder shall survive the expiration or termination of this Agreement and shall apply to any claims made during or after the term of the Agreement.
- ix. The **Bidder** shall be responsible for managing the risks associated with the use of subcontractors and shall indemnify the **Bank** against any loss, damage, or claims arising from the subcontractors' failure to meet the obligations or standards outlined in the agreement.

25 Confidentiality & Non-Disclosure

- 1) The bidder is bound by this agreement for not disclosing the Banks data and other information. Resources working in the premises of the Bank are liable to follow the rules and regulations of the Bank.
- 2) The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to the internal business and operational information of the Bank, affiliates, and/or business partners, disclosure of receipt of this tender or any part of the aforementioned information to parties not directly involved in providing the requested services could result in the disqualification of the bidders, premature termination of the contract, or legal action against the bidder for breach of trust.
- 3) No news release, public announcement or any other reference to the order, relating to the contracted work if allotted with the assignment or any program hereunder shall be made without written consent from the Bank.
- 4) As the bidder providing support services for multiple Banks, the bidder at all times should take care to build strong safeguards so that there is no mixing together of information/ documents, records and assets is happening by any chance.
- 5) The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts.

- 6) The Non-Disclosure Agreement (NDA) should be entered into between the Bank and the successful bidder within a period of 21 days from, the date of acceptance of purchase order.

Guarantee on Software License

The bidder shall guarantee that the software supplied under this contract to the Bank is licensed and legally obtained. Software supplied should not have any embedded malicious and virus programs. Bidder must comply RBI circular on "Cyber Security Framework for Banks" and assurance from the respective OEMs/Application providers that the application is free from embedded malicious/fraudulent code

26 Force Majeure

- 1) The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the parties, as a result of force majeure. For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the parties, including but not limited to, due to or as a result of or caused by acts of God, wars, epidemic/pandemic, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.
- 2) In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within seven business days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/dischage other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.
- 3) In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavour to find a solution to the problem. However bidder shall be entitled to receive payments for all services actually rendered up to the date of termination of date of agreement. The financial constraints by way of increased cost to perform the obligations shall not be treated as a force majeure situation if the obligations can otherwise be performed.

27 Resolution of Disputes

- 1) The Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, the Bank and the Bidder have been unable to

resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

- 2) All questions, disputes or differences arising under and out of, or in connection with the contract shall be referred to a sole arbitrator to be appointed mutually by the parties and in case of failure to appoint a sole arbitrator within 15 days from the raising of dispute the same shall be referred to the Arbitration Tribunal: one Arbitrator to be nominated by the Bank and the other to be nominated by the Bidder and the Presiding Arbitrator shall be appointed by the two Arbitrators appointed by the parties.
- 3) The decision of the Arbitration Tribunal shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai. The Language of Arbitration will be English. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, bidder will continue to perform its contractual obligations and the Bank will continue to pay for all products and services that are accepted by it, provided that all products and services are serving as per the agreed scope between the parties.
- 4) If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission, by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) on the date of acknowledgment signed by the receiver or (iii) the business date of receipt, if sent by courier.
- 5) This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP.

28 Format of the Letter of undertaking of Authenticity to be submitted by the Bidder.

The successful bidder has to submit the letter of undertaking of Authenticity and Undertaking at the time of acceptance of the letter of intent. The undertaking from OEMs needs to be provided to the Bank for the activities owned by them in coordination with the bidder as per the details mentioned in the document along with the pricing. The format for the same is as below.

"We undertake that all the components/parts/software used in the supplied devices shall be original, new components/ parts/ software only, from respective OEM/OSDs of the products and that no refurbished/ duplicate/ second hand components/ parts/ software are being used or shall be used.

We also undertake that in respect of licensed operating system, if asked for by you in the Purchase Order, the same shall be supplied along with the authorized license certificate and also that it shall be sourced from the authorized source.

We hereby undertake to produce the certificate from our OEM/OSD supplier in support of above undertaking at the time of implementation. It will be our

responsibility to produce such letters from our OEM/OSD suppliers at the time of release of PO or within a reasonable time. In case of default and we are unable to comply with the above at the time of delivery or during installation, for the software items already billed, we agree to take back the software/items without demur, if already supplied and return the money, if any paid to us by you in this regard".

29 Sub-Contractor/ Independent Contractor

Nothing herein contained will be construed to imply a joint venture, partnership, principal agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA (Non-Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. Bidder should take Bank's prior written permission before subcontracting/ resource outsourcing of any work related to the performance of this RFP or as the case may be, which permission shall not be unreasonably withheld by the Bank. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

30 Assignment

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever; (iv) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is

only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract/project.

31 Execution of Contract, SLA & NDA

The bidder and Bank should execute:

- 1) Contract, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and
- 2) Non-disclosure Agreement.
- 3) The bidder should execute the contract, SLA and NDA within 21 days from the date of acceptance of the Purchase Order. In case of any discrepancy among the RFP, SLA and Purchase Order, the RFP clauses shall prevail.

32 SI / Bidder's Liability

The Bidders aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of contract. The Bidder's liability in case of claims against the Bank resulting from **wilful misconduct** or gross negligence of the Bidder, its employees, or subcontractors, or from infringement of patents, trademarks, copyrights (if any), or breach of confidentiality obligations shall be unlimited. In no event shall Bank be liable for any indirect, incidental, or consequential damages or liability under, in connection with, or arising out of this tender and subsequent agreement or services provided. The bidder should ensure that the due diligence and verification of antecedents of employees/ personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

Subject to any law to contrary, and to the maximum extent permitted by law neither party shall be liable to other for any remote and indirect loss or damages arising out of this tender and subsequent agreement or services provided.

33 Change in Location/ Merger/Amalgamation

Bank reserves the right to change the location of services to be provided by the Service Provider by serving prior notice 30 days without assigning any reason and without altering any other terms & conditions of the RFP.

Bank also reserves the right to continue or discontinue the availment of product / services without assigning any reason, in case of its merger or amalgamation and the merged or amalgamated entity shall have the same rights.

34 Information Ownership

All information transmitted by successful Bidder belongs to the Bank. The Bidder does not acquire implicit access rights to the information or rights to redistribute the information unless and until written approval sought in this regard. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately, which is proved to have caused due to reasons solely attributable to bidder. Any information considered sensitive by the Bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The Bank's decision will be final if any unauthorized disclosure have encountered. Types of sensitive information that will be found on Bank system's which the Bidder plans to support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc. The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any of the Bank location. The Bidder will have to also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

35 Inspection, Audit, Review, Monitoring & Visitations

All OEM/Bidder records with respect to any matters / issues covered under the scope of this RFP/project shall be made available to the Bank at any time during normal business hours, not more than 2 audits per year, to audit, examine, and make excerpts or transcripts of all relevant data. Such records are subject to examination. The cost of such audit will be borne by the Bank. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/BIDDER outsourced process to identify new outsourcing risks as they arise. The BIDDER shall be subject to risk management and security and privacy policies that meet the Bank's standard. In case the BIDDER outsourced to third party, there must be proper Agreement / purchase order with concerned third party. The Bank shall have right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations. Access to books and records/Audit and Inspection would include:-

- 1) Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the BIDDER. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.
- 2) Provide the Bank with right to conduct audits on the BIDDER whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the Bank.

- 3) Include clause to allow the reserve Bank of India or persons authorized by it to access the Bank's documents: records of transactions, and other necessary information given to you, stored or processed by the BIDDER within a reasonable time. This includes information maintained in paper and electronic formats.
- 4) Recognized the right of the reserve Bank to cause an inspection to be made of a service provider of the Bank and its books and account by one or more of its officers or employees or other persons. Banks shall at least on an annual basis, review the financial and operational condition of the BIDDER. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the BIDDER. Such assessment and reports on the BIDDER may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.
- 5) Any such audit shall be conducted expeditiously, efficiently, and at reasonable business hours after giving due notice to the Bidder which shall not be less than 10 days. The Bank shall not have access to the proprietary data of, or relating to, any other customer of Bidder, or a third party or Bidder's cost, profit, discount and pricing data. The audit shall not be permitted if it interferes with Bidder's ability to perform the services in accordance with the service levels, unless the Bank relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit.

36 Monitoring

Compliance with Information security best practices may be monitored by periodic Information security audits performed by or on behalf of the Bank and by the RBI. 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, physical security controls, backup and recovery procedures, network security controls and program change controls. To the extent that the Bank deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Service Provider shall afford the Bank's representatives access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Bidder must provide the Bank access to various monitoring and performance measurement systems (both manual and automated). The Bank has the right to get the monitoring and performance measurement systems (both manual and automated) audited by prior notice to the Bidder.

37 Visitations

The Bank shall be entitled to, either by itself or its authorized representative, visit any of the Bidder's premises by prior notice to ensure that data provided by the Bank is not misused.

The Bidder shall cooperate with the authorized representative(s) of the Bank and shall provide all information/ documents\required by the Bank.

38 Information Security

System should have standard input, communication, processing and output validations and controls. System hardening should be done by bidder. Access controls at DB, OS, and Application levels should be ensured. Bidder should comply with the Information Security Policy of the Bank. The Product offered should comply with regulator's guidelines. The bidder shall disclose security breaches if any to the Bank, without any delay.

39 Intellectual Property Rights

- The Bank intends to procure and own the Data Lakehouse & Gen AI Solution developed by the successful bidder.
- The successful bidder should provide comprehensive warranty for the application and Bank will be paying the AMC/ATS if required thereafter completing the warranty period.
- In case the OEM/Bidder is unable to provide the service/support as mentioned in the RFP document, Bank will reserve the right to continue the usage of the Data Lakehouse & Gen AI Platform and the Solution till completion of the contract period plus the extended period.
- The bidder to provide the IP Rights for the customizations done for the Bank. Bidder undertakes that the solution developed and exclusively built for the Bank including customizations, knowledge gained, insights, intelligence as part of implementation of this project should remain confidential and be the proprietary to the Bank. The same shall not be reused by the Bidder in any other Bank/organization without explicit written permission from the Bank.
- Source code for customization done for Bank in the Data Lakehouse & Gen AI Platform and the Solution and for other related services shall be provided by the bidder to the Bank for unlimited and unrestricted use by the Bank.
- Bidder shall also provide all related material but not limited to flow charts, annotations, design documents schema, development, maintenance and operational tools and all related documentation.
- The Bank should have the rights to modify the platform and source code without any restrictions.
- In case the successful bidder is coming with software, which is not its proprietary software, then the bidder must submit evidence in the form of agreement it has entered with the software vendor, which includes support from the software vendor for the proposed software for the full period required by the Bank.
- If the successful bidder has used any specific proprietary platform or components, an escrow agreement needs to be executed.

- The core source code of the solutions in scope would be kept in escrow arrangement and complete information regarding the arrangement shall be provided by the bidder.
- Bidder shall transfer all Intellectual Property Right on non - exclusive basis for all the customizations done for Bank for the Data Lakehouse & Gen AI Platform and the Solution.
- The Bank and the bidder shall appoint an escrow agent approved by the Bank to provide escrow mechanism for the deposit of the source code for the solution supplied/procured by the bidder to the Bank to protect the Bank's interests in an eventual situation
- The Bank and the bidder shall enter into a tripartite escrow Agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent
- As a part of the escrow arrangement, the bidder shall be required to provide a detailed code documentation which has been duly reviewed and certified by an external independent organization
- All costs for the Escrow will be borne by the bidder.
- The escrow code along with all documentation shall be periodically updated every one year by the bidder. Bidder shall submit a self-certificate confirming the same after every update
- The Bank shall also have the right to conduct source code audit by third party auditor
- The Bank shall have right to audit of the complete solution proposed by the successful bidder, and inspection by the regulators of the country
- The successful bidder shall provide complete and legal documentation of all subsystems, licensed operating systems, licensed system software, licensed database and licensed utility software and other licensed software
- The successful bidder shall also provide licensed software for all software products whether developed by it or acquired from others
- The successful bidder shall also indemnify the Bank against any levies / penalties on account of any default in this regard.

The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Bank agrees and acknowledges that same as expressly provided in this RFP, all Intellectual Property Rights in relation to the Hardware, Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to

fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder or its licensor. During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Bidder a right to use at no cost or charge the Hardware and Software licensed to the Bank, solely for the purpose of providing the Services.

The Bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Hardware and Software used by Bidder in performing its obligations under this Project. If a third party's claim endangers or disrupts the Bank's use of the Hardware and Software, the Bidder shall at no further expense, charge, fees or costs to the Bank,

- Obtain a license so that the Bank may continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or
- Modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or
- Replace the Software with a compatible, functionally equivalent and non-infringing product. All third party Hardware/software / service/s provided by the bidder in the scope of the RFP will be the responsibility of the bidder if any discrepancy or infringement is encountered. The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied by the Bidder as part of this Project.

Bidder's Proprietary Software and Pre-Existing IP:- Bank acknowledges and agrees that this is a professional services agreement and this agreement is not intended to be used for licensing of any Bidder's proprietary software or tools. If Bidder and Bank mutually agree that the Bidder provides to Bank any proprietary software or tools of Bidder or of a third party, the parties shall negotiate and set forth the applicable terms and conditions in a separate license agreement and the provisions of this Clause shall not apply to any deliverables related to customization or implementation of any such proprietary software or products of Bidder or of a third party. Further, Bank acknowledges that in performing Services under this Agreement Bidder may use Bidder's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by Bidder prior to or independent of the Services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the Services hereunder, ("Bidder Pre-Existing IP"). Notwithstanding anything to the contrary contained in this Agreement, Bidder shall continue to retain all the ownership, the rights title and interests to all Bidder Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting Bidder from using Bidder Pre-Existing IP in any manner. To the extent that any Bidder Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under this Agreement, Bidder hereby grants to Bank a non-exclusive, perpetual / subscription, royalty free, fully paid up, irrevocable license, with the right to sublicense through multiple tiers, to use, copy, install, perform, display,

modify and create derivative works of any such Bidder Pre-Existing IP in connection with the deliverables and only as part of the Deliverables in which they are incorporated or embedded. The foregoing license does not authorize Bank to (a) separate Bidder Pre-Existing IP from the deliverable in which they are incorporated for creating a stand-alone product for marketing to others; (b) independently sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Bidder Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or (c) except as specifically and to the extent permitted by the Bidder in the relevant Statement of Work, reverse compile or in any other way arrive at or attempt to arrive at the source code of the Bidder Pre-Existing IP.

Residuary Rights. Each Party shall be entitled to use in the normal course of its business and in providing same or similar services or development of similar deliverables for its other clients, the general knowledge and experience gained and retained in the unaided human memory of its personnel in the performance of this Agreement and Statement of Work(s) hereunder. For the purposes of clarity the Bidder shall be free to provide any services or design any deliverable(s) that perform functions same or similar to the deliverables being provided hereunder for the Client, for any other customer of the Bidder (including without limitation any affiliate, competitor or potential competitor of the Bank. Nothing contained in this Clause shall relieve either party of its confidentiality obligations with respect to the proprietary and confidential information or material of the other party

40 Enterprise License:

39.1 The proposed Data Lakehouse & GenAI Platform and Solution should follow enterprise-wide licenses for all modules offered without any constraint and as per the Volumetrics / Projections / Use Cases mentioned in this RFP during the entire period of contract

39.2 Licenses for the Data Lakehouse & GenAI Platform and Solution should cover all installations like primary site, DR, other environments like Development, UAT etc. based on Bank's requirements without any constraint and as per the Volumetrics / Projections / Use Cases mentioned in this RFP during the entire period of contract

39.3 All software that is envisaged for delivery of Data Lakehouse & GenAI Platform and Solution is required to be licensed to Bank.

39.4 The successful bidder must:

- a) Provide licensing policy to the Bank covering the platform, solution, hardware, software, or any other component supplied as part of this RFP.

- b) Ensure the software supplied must be the latest version of the software supplied by the OEM. Beta versions of any software shall not be accepted.
- c) Consider the disaster recovery environment while proposing the software licenses.
- d) Offer technical and functional support of the service for contract tenure post implementation of solution.
- e) Provide complete functional and technical solution for any new platform, model, and OS and DB upgrade within thirty days of launch in India without any extra cost.
- f) Ensure Data Lakehouse & GenAI Platform and Solution along with final customization should be VAPT certified at no extra cost to Bank. Bank will not pay any customization charges till Go Live of respective solution.
- g) Ensure support contract for the Data Lakehouse & GenAI Platform and Solution should include program updates, patches, fixes, and critical security alerts as required.

41 Termination

41.1 Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 60 (Sixty) days written notice of default sent to the Successful Bidder, may terminate this Contract in whole or in part:

- 1) if the Successful Bidder fails to deliver any or all of the deliverables / milestones within the period(s) specified in the Contract, or within any extension thereof granted by the Bank provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure; or;
- 2) If the Successful Bidder fails to perform any other material obligation(s) under the contract provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure.
- 3) If the Successful Bidder, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

Prior to providing a written notice of termination to the Selected Bidder, Bank shall provide the selected bidder with a written notice of 30 days to cure any breach of the Contract. The decision to terminate the contract shall be taken only if the breach continues or remains unrectified, for reasons within the control of Bidder, even after the expiry of the cure period.

In case the contract is terminated then all undisputed payment for the services delivered till the date of termination will be given to successful bidder, but disputed payment shall be discussed and will be paid once the dispute is resolved.

41.2 Termination for Insolvency

If either party becomes Bankrupt or insolvent, has a receiving order issued against it, with its creditors, or, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if either party takes or suffers any other analogous action in consequence of debt; then other party plans to, at any time, terminate the contract by giving written notice of 60 days to the party becoming Bankrupt etc. If the contract is terminated by either party in terms of this Clause, Bank shall be liable to make payment of the entire amount due under the contract for which services have been rendered by the Selected Bidder.

41.3 Termination- Key Terms & Conditions

The Bank reserves the right to terminate the agreement with the other party at any time by giving 30 (thirty) days prior written notice to the other party.

Either Party shall also be entitled to terminate the agreement at any time by giving notice if the other party -

- 1) has a winding up order made against it; or
- 2) has a receiver appointed over all or substantial assets; or
- 3) is or becomes unable to pay its debts as they become due; or
- 4) enters into any arrangement or composition with or for the benefit of its creditors; or
- 5) Passes a resolution for its voluntary winding up or dissolution or if it is dissolved.

41.4 Right to Transfer IT Outsourcing Arrangements

In the event of termination, the Bank reserves the right to orderly transfer the proposed IT outsourcing arrangement to another service provider, if necessary or desirable, to ensure minimal disruption of services. This transfer shall be managed in an efficient manner, with the bidder cooperating fully with the Bank to facilitate this process, including transferring knowledge, data, and providing assistance as required.

41.5 Exit Option & Contract Re-Negotiation

The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:

- 1) Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 21 days of receipt of purchase contract.
- 2) Substantial delay in delivery, performance or implementation of the solution beyond the specified period.
- 3) Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of The Bank. Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by The Bank. (60 days will be construed as the notice period)

In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.

Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder will be expected to continue to provide services to the Bank as per the contract. Bank will continue to pay for all products and services that are accepted by it provided that all products and services as serving as per the agreed scope between the parties. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration. The Bank and the Bidder shall together prepare the Reverse Transition Plan. However, The Bank shall have the sole decision to ascertain whether such Plan has been complied with. Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Bidder to The Bank or its designee to ensure smooth handover and transitioning of Bank's deliverables, maintenance and services.

42 Privacy & Security Safeguards

- 1) The Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location. The Bidder will have to develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The Bidder will have to also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.
- 2) The Bidder hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.
- 3) The Bidder hereby agrees that they will preserve the documents.
- 4) The Bidder shall provide to the Bank, the details of all data related to the Bank and its customers that the service Provider captures, Processes and stores.
- 5) The Bidder may only share customer data with third parties when legally required, with prior consent, or for necessary operational purposes, ensuring compliance with confidentiality and data protection agreements.

43 Governing Law and Jurisdiction

The provisions of this RFP and subsequent Agreement shall be governed by the laws of India. The disputes, if any, arising out of this RFP/Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

Statutory and Regulatory Requirements

The solution must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall supersede the responses provided by the Bidder in the technical response. During the period of warranty / ATS Bidder should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the Bank during the tenure of the contract.

44 Compliance

- 1) The Service Provider (SP) agrees to comply with all applicable laws, regulations, and industry standards, including but not limited to the **Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, RBI's various Direction on Outsourcing of Information Technology Services** and any other relevant data protection or privacy laws. The SP shall ensure that the products and services provided under this agreement comply with all regulatory requirements, including guidelines set by authorities such as the **Reserve Bank of India (RBI)** and **FEMA**.

The clauses under RBI (Commercial Banks-Managing Risk in Outsourcing Directions, 2025 are the following :-

i. Type of material adverse events and the incidents required to be reported to Bank by the service provider:

The Vendor shall promptly report any material adverse events, including (but not limited to)

- b. Data breaches
- c. Denial of service attacks
- d. Service unavailability
- e. Security vulnerabilities
- f. Unauthorized access
- g. System failures
- h. Any other incidents that may impact Bank's operations or data integrity.

Such incidents shall be reported to the Bank immediately upon identification, enabling the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.

The Vendor shall provide all relevant details and updates regarding the incident, including the nature, scope, impact, and corrective actions taken, in accordance with the Bank's incident reporting procedures.

- iii. **Compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data:** The Vendor shall ensure compliance with the provisions of the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023 and all other applicable legal, regulatory, and industry requirements, including but not limited to data protection laws and privacy requirements, to protect the

confidentiality, integrity, and security of customer data handled or processed under this Agreement. The Vendor shall be fully responsible for any non-adherence from applicable laws or regulations and shall indemnify and hold the Bank harmless from any claims, losses, damages, or penalties arising out of such non-compliance.

- iv. **Storage of data (as applicable to the concerned Banks) only in India as per extant regulatory requirements:** The Vendor shall ensure that Bank's data processed or handled under this agreement, is stored exclusively within India, in compliance with the extant regulatory requirements.
- v. **Service provider to provide details of data (related to Bank and its customers) captured, processed and stored:** The Vendor shall provide the Bank with details of all data related to the Bank and its customers that it captures, processes, and stores, upon receiving an approved request.
- vi. **Controls for maintaining confidentiality of data of Bank's and its customers', and incorporating service provider's liability to Bank in the event of security breach and leakage of such information:** With related to confidentiality of data,
 - a) The Vendor shall treat all data of the Bank and its customers as confidential and shall not disclose or allow access to such data to any unauthorized third party without the prior written consent of the Bank.
 - b) The Vendor shall implement all necessary measures to protect the confidentiality and integrity of the data throughout the term of this Agreement and thereafter.
 - c) The Vendor shall implement and maintain industry-standards controls to safeguard Bank related data.
- vii. **Types of data/information that the service provider (vendor) is permitted to share with Bank's customer and/or any other party:** The Vendor shall define and ensure the types of data/information that is shared with the Bank's customers and/or any other parties:
 - i. Is shared with explicit written consent or authorization from the Bank.
 - ii. Is required by law or regulation, including legal processes such as subpoenas.
 - iii. Is shared with approved third-party vendor or sub-processors.
- viii. **Right to seek information from the service provider about the third parties (in the supply chain) engaged by the former:** The Bank reserves the right to seek information from the Vendor about its third parties or sub-contractors engaged in the supply chain or any sub-contracted work.
- ix. **Making the service provider contractually liable for the performance and risk management practices of its sub-contractors:** The Vendor shall be contractually liable for the performance and risk management practices of its sub-contractors. The Vendor will remain fully responsible for ensuring that its sub-contractors adhere to the same performance standards, security protocols, and risk management practices as outlined in the agreement with the Bank. The

Vendor should be obligated to manage and mitigate any risks arising from its sub-contractors' actions or failures, and to promptly address any issues related to sub-contractor performance that could impact the quality of service or compliance with the agreement.

- x. **Need of prior approval/consent of the Bank for use of sub-contractors by the service provider for all or part of an outsourced activity:** The Vendor shall obtain the Bank's prior written consent before sub-contracting or outsourcing all or part of activities covered under this agreement.
- xi. **Termination rights of the Bank, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable:** In the event of termination, the Bank shall have the right to transition of the IT outsourcing arrangement to another sub-vendor, either in whole or in part, at its discretion. The Vendor agrees to fully cooperate with the Bank to ensure an orderly and seamless transfer of services, including the transfer of data, systems, and knowledge, and to provide necessary support to the new Service Provider. The Vendor shall also assist in mitigating any risks associated with the transition and shall ensure that all customer data and confidential information is securely handled during the transition process.
- xii. **Obligation of the service provider to co-operate with the relevant authorities in case of insolvency/resolution of the Bank:** If the Bank becomes subject to insolvency proceedings, financial restructuring, or resolution by relevant authorities (e.g., governmental bodies, regulatory agencies, or liquidators), the Vendor shall co-operate fully with the relevant authorities in accordance with applicable laws and regulations.
- xiii. **Provision to consider skilled resources of service provider who will provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations):**
 - The Vendor shall designate and maintain a pool of skilled resources who will be considered "essential personnel" for the delivery of core services under this agreement.
 - These personnel will be responsible for ensuring the continuity of critical functions, particularly during exigent circumstances such as emergencies, natural disasters, or pandemics.
 - In the event of such situations, the Vendor shall implement necessary backup arrangements to ensure that a limited but enough essential personnel are available to work on-site to support critical operations.
 - The Vendor shall make reasonable efforts to ensure the safety and well-being of these personnel while maintaining the uninterrupted delivery of critical services.
 - The Vendor shall notify the Bank promptly of any significant changes to the availability or capacity of essential personnel, as well as any potential impact on service delivery.

- xiv. **Suitable back-to-back arrangements between service providers and the OEMs:** The Vendor shall ensure that suitable back-to-back arrangements are in place with Original Equipment Manufacturers (OEMs) to guarantee the provision of required products, services, and support. These arrangements must align with the terms and service levels defined in this agreement, ensuring that the Vendor can meet its obligations to the Bank and address any issues related to the OEM products or services in a timely and efficient manner. The Vendor is responsible for ensuring that the OEM's support and performance meet the agreed-upon standards, and for providing any necessary escalations or resolutions in the event of failure by the OEM to meet such standards.
- xv. **Non-disclosure agreement with respect to information retained by the service provider:** The Vendor shall keep all confidential information of the Bank secure and will not disclose or use it for any purpose other than fulfilling this agreement, both during and after the term, as outlined in the Non-Disclosure Agreement.

The SP shall adhere to the Bank's **Information Security Policy** and implement necessary controls for system security, including access control, data protection, and encryption, at all levels (e.g., database, operating system, application). The SP must also ensure the hardening of systems to protect against vulnerabilities.

- xvi. **Sustainable Sourcing:** The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labor practices and compliance with relevant local and international regulations. The Supplier shall provide documentation or certifications demonstrating their commitment to Sustainable Sourcing upon request. Failure to comply with these requirements may result in contract termination
- xvii. **No relationship of master and servant or employer and employee:** Notwithstanding what is stated elsewhere in this agreement, this agreement does not create any relationship of Master and servant or Employer and employee as between the Bank on the one hand and the Vendor and/or the personnel employed/engaged by the Vendor on the other hand. The parties expressly understand and agree that this agreement broadly covers in respect of specific job/s to be performed by the Service Provider.

44.1 Adherence to Cyber Security Policy

- 43.1.1 Vendors are responsible for complying with the security standards or desired security aspects of all the ICT resources in line with regulatory guidelines from time to time as well as Bank's IT/Information Security / Cyber Security Policy guidelines. Such guidelines will be shared with Vendor.
- 43.1.2 Vendor should ensure Data Security and protection of facilities/application managed by them. The deputed persons should be aware about Bank's IT/IS/Cyber security policy guidelines and have to maintain the utmost secrecy &

confidentiality of the Bank's data including process performed. At any time, if it comes to the notice of the Bank that data has been compromised/disclosed/misused/misappropriated then Bank would take suitable action as deemed fit and selected vendor would be required to fully compensate the Bank of loss incurred by the Bank.

43.1.3 Vendor has to agree and provide undertaking not to disclose any Bank information and will maintain confidentiality of Bank information as per policy of the Bank and will sign "Non-Disclosure Agreement" document provided by Bank.

43.1.4 The Service provider shall put in place necessary controls within its organization for maintaining confidentiality of the Bank's and its customer's data.

44.2 Compliance with Laws

43.2.1 Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.

43.2.2 Compliance in obtaining approvals/permissions/licenses: Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project.

45 Violation of Terms

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained under the RFP/Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

46 Corrupt & Fraudulent Practices

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution AND

"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 offer submission) designed to establish offer prices at artificial non-competitive levels and to deprive The Bank of the benefits of free and open competition.

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. 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.

47 Publicity

Any publicity by either party in which the name of the other party is to be used should be done only with the explicit written permission of such other party.

48 Entire Agreement; Amendments

This RFP sets forth the entire agreement between the Bank and the Successful bidder and supersedes any other prior proposals, agreements and representations between them related to its subject matter, whether written or oral. No modifications or amendments to this Agreement shall be binding upon the parties unless made in writing, duly executed by authorized officials of both parties.

49 Survival and Severability

Any provision or covenant of the RFP, which expressly, or by its nature, imposes obligations on successful bidder shall so survive beyond the expiration, or termination of this Agreement. The invalidity of one or more provisions contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof; and in the event that one or more provisions shall be declared void or unenforceable by any court of competent jurisdiction, this Agreement shall be construed as if any such provision had not been inserted herein.

50 Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Document. Submission of a bid not responsive to the Bidding Document in every respect will be at the bidder's risk and may result in the rejection of its bid without any further reference to the bidder.

50.1 Amendments to Bidding Documents

At any time prior to the last Date and Time for submission of bids, the Bank may, for any reason, modify the Bidding Document by amendments at the sole discretion of the Bank. All amendments will be either uploaded in the website or shall be delivered by hand / post / courier or through e-mail or faxed to all prospective bidders, who have received the bidding document and will be binding on them. For this purpose bidders

must provide name of the contact person, mailing address, telephone number and FAX numbers on the covering letter sent along with the bids.

In order to provide, prospective bidders, reasonable time to take the amendment if any, into account in preparing their bid, the Bank may, at its discretion, extend the deadline for submission of bids.

50.2 Period of Validity

Bids shall remain valid for 180 days from the last date of bid submission. A bid valid for shorter period shall be rejected by the Bank as non-responsive.

50.3 Last Date and Time for Submission of Bids

Bids must be submitted not later than the specified date and time as specified in the Bid Document. Bank reserves the right to extend the date & time without mentioning any reason.

50.4 Late Bids

Any bid received after the deadline for submission of bids will be rejected and/or returned unopened to the Bidder, if so desired by him.

50.5 Modifications and/or Withdrawal of Bids

- 1) Bids once submitted will be treated as final and no further correspondence will be entertained on this.
- 2) No bid will be modified after the deadline for submission of bids.
- 3) No bidder shall be allowed to withdraw the bid, if the bidder happens to be a successful bidder.

50.6 Clarification of Bids

To assist in the examination, evaluation and comparison of bids the Bank may, at its discretion, ask the bidder for clarification and response, which shall be in writing and without change in the price, shall be sought, offered or permitted.

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

The Bank reserves the right to accept or reject any bid and annul the bidding 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 ground for the Bank's action.

51 Signing of Contract

The successful bidder(s) to be called as bidder, shall be required to enter into an Agreement with the Bank, within 21 days of the award of the work order (when provided) or within such extended period as may be specified by the Bank.

52 Sustainable Sourcing

The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labor practices and compliance with relevant local and international regulations. The Supplier shall provide documentation

or certifications demonstrating their commitment to Sustainable Sourcing upon request. Failure to comply with these requirements may result in contract termination.

53 Remote Access

Any type of remote access will not be allowed outside Bank's Network.

54 Business Continuity and Disaster Recovery

54.1 Business Continuity Plan (BCP)

The Service Provider shall have a documented Business Continuity Plan in place, which outlines the strategies for maintaining service availability in the event of an unexpected incident. The BCP should include, but is not limited to:

- 1) Detailed procedures for mitigating and recovering from various business disruptions.
- 2) Identification of key personnel, roles, and responsibilities in a crisis.
- 3) Communication plans to inform both the Service Provider and Customer of significant disruptions and progress towards recovery.

54.2 Disaster Recovery Plan (DRP)

The Service Provider shall maintain a Disaster Recovery Plan to restore critical services and infrastructure in the event of a disaster, including:

- 1) Specific recovery objectives, such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), to be met for each service.
- 2) Procedures for data backup, storage, and retrieval.
- 3) Clear steps to restore services to full functionality, including resource allocation and escalation procedures.

55 Obligation to Co-operate with relevant authorities in case of Insolvency/Resolution

55.1 Insolvency

In the event that Bank becomes subject to insolvency proceedings, financial restructuring, or resolution by relevant authorities (including, but not limited to, governmental bodies, regulatory agencies, or liquidators), the Service Provider shall cooperate fully with such authorities, in accordance with applicable laws and regulations.

55.2 Cooperation

The Service Provider agrees to provide all necessary information, documentation, and assistance as requested by the relevant authorities, including but not limited to access to data, records, systems, and personnel, to ensure a smooth transition or orderly resolution process.

55.3 Continued Service During Resolution

In the event of insolvency or resolution of the Bank, the Service Provider shall continue to perform its obligations under this Agreement unless otherwise directed by the relevant authorities or instructed by Bank.

55.4 Notification

The Service Provider shall notify the Bank promptly upon learning of any insolvency, liquidation, or resolution proceedings involving the Bank, and shall comply with any directions provided by the relevant authorities.

56 Data Localization

The Bidder shall ensure that all data, as applicable to the concerned Bank, is stored exclusively within India, in full compliance with the extant regulatory requirements set forth by the relevant authorities. The Bidder shall not store or process any data outside of India without prior written consent from the Bank and approval from regulatory bodies.

57 Authorized Signatory

The Bidder shall indicate the authorized signatories who can discuss and correspond with Bank, with regard to the obligations under the contract. The Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the bidder to discuss, sign agreements/contracts with Bank, raise invoice and accept payments and also to correspond. The Bidder shall provide proof of signature identification for the above purposes as required by Bank.

58 Escrow Arrangements

The bidder has to facilitate for Escrow Agreement between all the parties (Bank as beneficiary, ESCROW Agent, OEM and System Integrator as the case may be) as agreed upon by all parties. The escrow agreement shall include provisions that, in the event of a predefined triggering event (such as the OEM going out of business, breach of contract, or any other specified event), the source code will be made available to the Bank in a timely manner, ensuring uninterrupted support and maintenance of the solution.

The Bidder shall bear all costs related to setting up and maintaining the escrow arrangement, including any charges incurred for the services of the Escrow Agent. The Bank shall not be responsible for any costs related to the escrow setup or the escrow agent's services.

In addition, the Service Provider shall ensure regular and secure backups of the source code and other critical data. Backup of all relevant data, including the source code, must be performed and securely stored in accordance with the Bank's Data Security and compliance requirements. The Bank shall have access to these backups upon request to ensure continuity and security of operations.

59 Digital Personal Data Protection Act/Rules

The Bidder/Vendor shall, at all times, comply with the provisions of the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 / Notifications / Guidelines and further rules made thereunder.

The Bidder/Vendor shall implement appropriate technical and organizational measures to ensure lawful processing, secure handling, confidentiality, integrity, availability, and protection of personal data obtained, accessed, shared, or processed in connection with this RFP and the resultant contract.

Further, the Bidder/Vendor shall take due care while collecting and dealing with sensitive personal data or information of Bank and its customer. Any processing of Personal Data by the Service Providers in the performance of the Agreement under this RFP shall be in compliance with the above Act/Rules. The Service Provider shall also ensure that any sub-contractor (if allowed) engaged by it shall act in compliance with the above Act, to the extent applicable.

The Bidder/Vendor shall Act only on documented instructions of the Bank and shall not process personal data for any purpose other than the performance of the obligations under this RFP.

Any data breach, un-authorized access, misuse, loss, or disclosure of personal data must be reported to the Authority/Bank in writing within [24 hours] of occurrence, along with an incident report and remedial action plan.

The Bidder/Vendor shall indemnify and hold harmless the Bank against any loss, liability, penalty, claim, cost, or damages arising out of non-compliance with the DPDP Act and Rules.

60 Labour Law

The Bidder/Vendor shall ensure full compliance with all applicable labour laws, employment laws, industrial relations regulations, social security legislation, and any orders/directions issued by competent Labour Courts/Industrial Tribunals/Authorities / RBI and any other Regulatory/Statutory body in India.

The Bidder/Vendor shall be solely responsible for payment of salaries, wages, statutory contributions, benefits, and all dues to its employees, subcontractors, labour, and statutory personnel deployed for execution of work under this RFP.

No employer-employee relationship shall be deemed to exist between the Bank and the personnel engaged by the Bidder/Vendor.

In case of any claim, demand, dispute, or litigation arising due to non-compliance by the Bidder/Vendor, the same shall be solely borne and resolved by the Bidder/Vendor without any liability upon the Bank.

The Bidder/Vendor shall indemnify the Bank against any losses, costs, or legal liabilities on account of any violation or non-compliance of applicable laws

including any liabilities, costs or expenses arising in connection with any proceedings in respect thereof.

61 Right to alter/ delete Components and Quantities specified in the RFP

The Bank reserves the right to alter / delete the requirements (Components) specified in the Tender document. The Bank also reserves the right to alter / add the quantity from the quantity specified in the Tender.

62 Conflict of Interest

Bank requires that bidder provide professional, objective, and impartial advice and at all times hold 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 Bank.

Bidder have 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 Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if 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.

.....

Section-4

Annexures

Checklist for Submission

#	Particulars	Bidders Remark (Yes/No)
1	Certificate of Incorporation	
2	Audited Balance sheets of last three years - 2022-23, 2023-24, 2024-25	
3	CA certificate for three years average turnover for financial years 2022-23, 2023-24, 2024-25	
4	CA certificate for operating profit for last three financial years 2022-23, 2023-24, 2024-25	
5	CA certificate for net worth for last three financial years i.e. 2022-23, 2023-24, 2024-25	
6	Self-declaration by the Authorized Signatory for not having filed for Bankruptcy in any country including India on company letter head	
7	Self-declaration on Company's letter head stating bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks,	
8	Self-declaration on Company's letter head stating Bidder/OEM should not	
9	Self-declaration on Company's letter head regarding • NPA • Any case pending	
10	Document Cost	
11	Annexure 1: Conformity Letter	
12	Annexure 2: Commercial Bill of Material	
13	Annexure 3: Bidder's Information	
14	Annexure 4: Letter for Conformity of Product as per RFP	
15	Annexure 5: GOI Guidelines with Model wise classification (Make in India)	
16	Annexure 6: Undertaking of Authenticity for Products Supplied	
17	Annexure 7: Undertaking for Acceptance of terms of RFP	
18	Annexure 8: Manufacturer's Authorization Form	
19	Annexure 9: Integrity Pact	
20	Annexure 10: Non-Disclosure Agreement	
21	Annexure 11: Performance Bank Guarantee	
22	Annexure 12: Minimum Technical Specifications	
23	Annexure 13: Bid Security (BG Format - for Earnest Money Deposit)	
24	Annexure 14: Bidders Particulars	
25	Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"	
26	Annexure 16: NPA Undertaking	
27	Annexure 17: Land Border Sharing Undertaking	
28	Annexure 18: Cover Letter	
29	Annexure 19 Escalation Matrix	
30	Annexure 20: Query Format	
31	Annexure 21: Guidelines on Banning of Business Dealing	
32	Annexure 22: Undertaking of Information Security from Bidder	
33	Annexure 23: Software Bill of Material (SBOM) Format	
34	Annexure 24: Template for Third Party Due Diligence Questionnaire	

#	Particulars	Bidders Remark (Yes/No)
36	Annexure 25: List of Hardware and Software Components	
37	Annexure 26: Letter for Refund of EMD	
38	Annexure 27: Format for Submission of Client References by Bidder	
39	Annexure 28: Undertaking for Data Privacy	
40	Annexure 29: Undertaking for 7 Years Roadmap	
41	Annexure 30: Format for Local Content	
42	Annexure 31: Proposed Team Profile	
43	Annexure 32: Volumetrics	
44	Annexure 33: Declaration of Source Code Audit	
45	Annexure 34: Existing Application Details	
46	Annexure 35: Self-Declaration/ Undertaking Regarding Non-Suspension by GeM in the last Six months	
47	Annexure 36: Declaration/ Undertaking from bidder to comply with the Information and Cyber Security Controls	
48	Annexure 37: Information/ Cyber- security Measures/ Controls for selected Service Provider	

Annexure 1: Conformity Letter

Date

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: Tender No. GEM/2026/B/7203650

Further to our proposal dated _____, in response to the RFP document (hereinafter referred to as "RFP DOCUMENT") issued by Central Bank of India ("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 document and the related addendums and other documents including the changes made to the original tender documents 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,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 2: Commercial Bill of Material

Tender No. GEM/2026/B/7203650

The Summary for the Commercial Bill of Material is as under:

Sr. No#	Category	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost	GST	Total Cost with GST
1	Table A: Hardware Cost	XX	XX				XX	XX	XX
2	Table B: Software Cost (One Time & ATS)	XX	XX	XX	XX	XX	XX	XX	XX
3	Table C: Implementation of Lakehouse Platform (DC, DR, Dev, UAT, Sandbox)	XX					XX	XX	XX
4	Table D: Implementation of AI/GenAI capabilities (DC, DR, Dev, UAT, Sandbox)	XX	XX				XX	XX	XX
5	Table E: Data Migration Cost	XX					XX	XX	XX
6	Table F: Implementation Cost of Use Cases	XX	XX				XX	XX	XX
7	Table G: AMC Cost				XX	XX	XX	XX	XX
8	Table H: Facility Management Services Cost	XX	XX	XX	XX	XX	XX	XX	XX

9	Table I: Training and Knowledge Transfer	XX					XX	XX	XX
10	Table J: Change Request Cost	XX	XX	XX	XX	XX	XX	XX	XX
11	Table K: Sub-Total of KPI adherence for Early Migration & Use cases (5 % of Total from Point#1 to 10 above)	XX	XX	XX	XX	XX	XX	XX	XX
	Total Yearly Cost	XX	XX	XX	XX	XX	XX	XX	XX
	Total Cost to Ownership TCO								XX
	TCO in words	<u>XXXXXXXXXXXXXXXXXXXX</u>							

*Bidder is expected to quote the cost for each component.
All cost should flow from the respective tabs of this sheet
The Bidder is expected to ensure compliance with the stated guidance.

S.No	Guidelines
	Cost Summary
1	The bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP and the corrigendum in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully utilise the solution.
2	Important notification for the bidders - The Bank requires that the costs associated with the "Implementation Cost of Use Cases" should not be less than 15% of the "Total cost of Ownership". If in case this cost is quoted less than 15% of TCO, then Bank reserves the right to carve out the difference amount from the product cost of Hardware and Software, which will be paid post Successful Implementation of Use Cases

3	Bank will not be responsible for any arithmetic errors in the commercial bid details sheet committed by the bidders. All formulas & arithmetical calculations will be Vendor's responsibility.
4	The bidder is expected to specify the type of licences along with the details with respect to quantity, rate, etc., wherever applicable.
5	In case the bidder includes/combines any line item as part of any other line item in the commercial bid, then this has to be clearly mentioned in the description indicating the line item which contains the combination
6	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
7	The Bidder may insert additional line items as applicable based on the solution offered in the respective tabs
8	The Bidders should quote as per the format of Bill of Material ONLY and a masked replica of the Bill of Material should be enclosed in the technical bid.
9	Bidder is required to cover component by component licensing details for each of the software components proposed to CBI
10	The masked Bill of Materials which would be submitted as part of the Technical Bill of Material should contain "XX" for ALL the corresponding commercial values that will be present in the unmasked Bill of Material that will be part of the Commercial submission.
11	All amounts in the Bill of Material should be in INR
12	The Bidder should to the extent possible stick to the same structure of the Bill of Material. Hence, the bidder is not expected to delete necessary rows.
13	Any additional items (software, hardware) and services to be procured by the Bank in the future shall be priced on a pro-rata basis, based on the rates specified in the Bill of Material, unless otherwise determined by the Bank at its sole discretion. The Bidder is required to comply with this provision.

14	If the Bidder has not provided a specific quote for any line item listed in the Bill of Material, it shall be deemed that the Bidder has included the cost for such an item within the overall pricing provided in the Bill of Material. No additional charges beyond those specified in the Bill of Material will be payable by the Bank.
15	Bidder is required to submit the commercials during the bid submission and is required to provide the line item wise detailed breakup in the commercial bid.
Table A, B	Hardware & Software
1	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
2	The Bidder can insert additional line items as applicable based on the solution offered in the various tabs
3	The hardware type & software type, model, part number, and detailed configuration has to be clearly described in the Description column
4	The Bidder shall provide the maintenance (Warranty & ATS) for entire contract period and shall be provisioned to extend as mentioned in RFP terms & conditions
4	The Bidder is required to supply implement and provide warranty & AMC/ATS of the hardware & associated software required for the solution for the tenure of the contract
Table A, B, C, D, E, F	Installation, Implementation & Migration
1	Bidder shall comply to the Installation & commissioning, implementation and Migration scope provided in the RFP
2	Bidder should quote for end-to-end Installation & commissioning, implementation and Migration scope as mentioned in the RFP

3	Activities and functions to be undertaken for installation and implementation of the licensed software should be as per the RFP.
Table G	AMC Cost
1	Bidder is expected to provide a detailed break up of all products and services that are under the scope as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management.
2	The AMC, ATS costs for Production DC & DR have to be quoted separately
3	If required, the Bidder has to create additional line items in this section.
4	AMC cost should be quoted minimum 8% of the Hardware Cost and ATS (if any) should be quoted minimum 15% of Software Cost. If applicable AMC/ATS cost is not quoted by the bidder, then bidder will have to re-adjust the equivalent amount from the product cost of Hardware and Software to the AMC/ATS cost without changing the TCO.
Table J	Change Request Cost
1	Bidder is expected to quote for each calendar year
2	For any additional person-days above the 100 person-days, the rate quoted for that year will be considered. i.e. For any additional requirement of person-days and bidder should not make any additions/increase to the yearly rate/charges of the person-days.
3	Bidder to carry forward the unutilized person-days (with same quoted cost) to the subsequent years. No additional cost to be charged to Bank

Table A:
Hardware Cost (DC, DR, Dev, UAT, Sandbox)

	Hardware			YEAR 1		YEAR 2 – GenAI Only			Total Cost for Year 1 & 2	GST	Total Cost with GST
SR. No	Make /Model	PART CODE	Details of the Hardware	Quantity (X)	Total Cost (X x Y)	Quantity (X)	Rate (Y)	Total Cost (X x Y)			
	Data Centre (DC)										
1	Servers	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Storage	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
3	GPU Servers	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
6	SAN Switch	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
7	RACK	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
8	LAN CABLING	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
9	SAN CABLING	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
10				XX	XX	XX	XX	XX	XX	XX	XX

11				XX	XX	XX	XX	XX	XX	XX	XX
12				XX	XX	XX	XX	XX	XX	XX	XX
13				XX	XX	XX	XX	XX	XX	XX	XX
14				XX	XX	XX	XX	XX	XX	XX	XX
15				XX	XX	XX	XX	XX	XX	XX	XX
16	Add more rows for Any other items (Please specify)										
	Total - A			XX	XX	XX	XX	XX	XX	XX	XX
	Disaster Recovery Centre (DRC)										
Server											
1	Servers	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Storage	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
3	GPU SERVERS	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

6	SAN Switch	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
7	RACK	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
8	LAN CABLING	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
9	SAN CABLING	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
10		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
11		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Add more rows for Any other items (Please specify)	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Total - B			XX	XX	XX	XX	XX	XX	XX	XX
	Total- A+B			XX	XX	XX	XX	XX	XX	XX	XX

Hardware Installation Cost (DC, DR, Dev, UAT, Sandbox)

S.No	Hardware Installation		YEAR 1		YEAR 2 – GenAI Only			Total Cost for Year 1 & 2	GST	Total Cost with GST
	Make/Model	Part Code	Quantity (X)	Total Cost (X x Y)	Quantity (X)	Rate (Y)	Total Cost (X x Y)			
	Data Centre (DC)									
1	Servers		XX	XX	XX	XX	XX	XX	XX	XX
2	Storage		XX	XX	XX	XX	XX	XX	XX	XX
3	GPU SERVERS		XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer		XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy		XX	XX	XX	XX	XX	XX	XX	XX
6	SAN Switch		XX	XX	XX	XX	XX	XX	XX	XX
7	RACK		XX	XX	XX	XX	XX	XX	XX	XX
8	LAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX
9	SAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX
10			XX	XX	XX	XX	XX	XX	XX	XX

11								XX	XX	XX
12								XX	XX	XX
13	Add more rows for Any other items (Please specify)							XX	XX	XX
	Total - A		XX	XX	XX		XX	XX	XX	XX
	Disaster Recovery Centre (DRC)									
	Server									
1	Servers		XX	XX	XX	XX	XX	XX	XX	XX
2	Storage		XX	XX	XX	XX	XX	XX	XX	XX
3	GPU SERVERS		XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer		XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy		XX	XX	XX	XX	XX	XX	XX	XX
6	SAN Switch		XX	XX	XX	XX	XX	XX	XX	XX
7	RACK		XX	XX	XX	XX	XX	XX	XX	XX

8	LAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX
9	SAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX
10			XX	XX	XX	XX	XX	XX	XX	XX
11			XX	XX	XX	XX	XX	XX	XX	XX
12	Add more rows for Any other items (Please specify)		XX	XX	XX	XX	XX	XX	XX	XX
	Total - B		XX	XX	XX	XX	XX	XX	XX	XX
	Total-A+B		XX	XX	XX	XX	XX	XX	XX	XX

Table B: SOFTWARE COST (DC, DR, Dev, UAT, Sandbox)

S. No	Software Cost	License Type (Perpetual/ Subscription)	One Time Cost ((in case of Perpetual Licenses)			YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Cost For Year 1, 2, 3, 4 & 5 = A+B+C+D+E+F	G S T	Total with G S T
			Qty (X 0)	One Time Cost (Y 0)	Total Cost [A = (X 0 X Y 0)]	Qty (X 1)	Subscription (Y1)	Total Cost [B = (X 1 X Y 1)]	Qty (X 1)	Subscription (Y1)	Total Cost [C = (X 1 X Y 1)]	Qty (X 1)	Subscription (Y1)	Total Cost [D = (X 1 X Y 1)]	Qty (X 1)	Subscription (Y1)	Total Cost [E = (X 1 X Y 1)]	Qty (X 1)	Subscription (Y1)	Total Cost [F = (X 1 X Y 1)]			
	DATACENTRE																						
1	Data Acquisition - Near Real Time data ingestion (CDC)	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Data Acquisition - Batch	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

	data ingestion																						
3	Data Acquisition Stream data ingestion	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
4	Data Quality Tool Management Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
5	Meta Data Management Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
6	Data Governance Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
7	Audit Based Control	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
8	DevOps/ MLOps	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
9	Analytics Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
10	Analytics Sandbox	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
11	Reporting & Visualization Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX

1 2	Customer Data Platform (CDP)	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
1 3	ETL tool and it's all compo- nents	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
1 4	SSL Certifica- te	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
1 5	Zero Trust Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
	Add more rows for Any other items (Please specify)	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
	Total - A	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
	Disaster Recover- y Centre (DRC)																						
1	Data Acquisiti- on - Near	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX

	Real Time data ingestion (CDC)																						
2	Data Acquisition - Batch data ingestion	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
3	Data Acquisition - Stream data ingestion	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
4	Data Quality Tool Management Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
5	Meta Data Management Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
6	Data Governance Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
7	Audit Based Control	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
8	DevOps/ MLOps	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX

9	Analytics Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
10	Analytics Sandbox	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
11	Reporting & Visualization Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
12	Customer Data Platform (CDP)	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
13	ETL tool and its all components	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
14	SSL Certificate	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
15	Zero Trust Tool	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX
	Add more rows for Any other items (Please specify)	XX	XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX

	Total - B		XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX	
	Total A + B		XX	XX	XX	XX	XX	X X	X X	XX	XX	X X	XX	X X	X X	XX	X X	X X	XX	X X	XX	X X	XX	

SOFTWARE INSTALLATION COST (DC, DR, Dev, UAT, Sandbox)										
	Software Cost	Year 1			Year 2 – GenAI Only			Total Installation Cost A + B	GST	TOTAL COST with GST
S. No	Make /Model	Qty (X)	Rate (Y)	Total Cost [A= (X x Y)]	Qty (X)	Rate (Y)	Total Cost [B= (X x Y)]			
	Data Centre (DC)									
1	Data Acquisition - Near Real Time data ingestion (CDC)	XX	XX	XX	X X	X X	XX	XX	X X	XX
2	Data Acquisition - Batch data ingestion	XX	XX	XX	X X	X X	XX	XX	X X	XX
3	Data Acquisition - Stream data ingestion	XX	XX	XX	X X	X X	XX	XX	X X	XX
4	Data Platform including all components	XX	XX	XX	X X	X X	XX	XX	X X	XX
5	Data Quality Tool Management Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
6	Meta Data Management Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
7	Data Governance Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX

8	Audit Based Control	XX	XX	XX	X X	X X	XX	XX	X X	XX
9	DevOps/ MLOps/LLMOps	XX	XX	XX	X X	X X	XX	XX	X X	XX
10	Analytics Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
11	Analytics Sandbox	XX	XX	XX	X X	X X	XX	XX	X X	XX
12	Reporting & Visualization Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
13	ETL tool and it's all components	XX	XX	XX	X X	X X	XX	XX	X X	XX
14	SSL Certificate	XX	XX	XX	X X	X X	XX	XX	X X	XX
15	Zero Trust Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
	Any other items (Please specify)	XX	XX	XX	X X	X X	XX	XX	X X	XX
	Total - A			XX			XX	XX	X X	XX
Disaster Recovery Centre (DRC)										
1	Data Acquisition - Near Real Time data ingestion (CDC)	XX	XX	XX	X X	X X	XX	XX	X X	XX
2	Data Acquisition - Batch data ingestion	XX	XX	XX	X X	X X	XX	XX	X X	XX
3	Data Acquisition - Stream data ingestion	XX	XX	XX	X X	X X	XX	XX	X X	XX
4	Data Platform including all components	XX	XX	XX	X X	X X	XX	XX	X X	XX
5	Data Quality Tool Management Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX

6	Meta Data Management Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
7	Data Governance Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
8	Audit Based Control	XX	XX	XX	X X	X X	XX	XX	X X	XX
9	DevOps/ MLOps/LLMOps	XX	XX	XX	X X	X X	XX	XX	X X	XX
10	Analytics Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
11	Analytics Sandbox	XX	XX	XX	X X	X X	XX	XX	X X	XX
12	Reporting & Visualization Tool	XX	XX	XX	X X	X X	XX	XX	X X	XX
13	ETL tool and it's all components	XX	XX	XX	X X	X X	XX	XX	X X	XX
14	SSL Certificate	XX	XX	XX	X X	X X	XX	XX	X X	XX
15	Zero Trust Tool									
		XX	XX	XX	X X	X X	XX	XX	X X	XX
	Any other items (Please specify)	XX	XX	XX	X X	X X	XX	XX	X X	XX
	Total - B		X X	XX	X X	X X	XX	XX	X X	XX
	Total- A+B		X X	XX	X X	X X	XX	XX	X X	XX

**Software / Application License
 details (Enterprise-wide
 Perpetual /Subscription License)
 of all the Software Applications in
 the entire solution as per the
 scope of the RFP
 Start date of the subscription license
 would be from the Go-live of Platform**

Table C: Implementation of Lakehouse Platform and Data Transformation (DC, DR, Dev, UAT, Sandbox)					
Sr. No#	Services	Description	Total Cost	GST	Total Cost with GST
1	Implementation of Lakehouse Platform and Data Transformation (DC, DR, Dev, UAT, Sandbox)		XX	XX	XX
2					
3					
4					
5					
	Total		XX	XX	XX

Table D: Implementation of AI/GenAI Capabilities (DC, DR, Dev, UAT, Sandbox)

Sr. No#	Services	Description	Total Cost	GST	Total Cost with GST
1	Implementation of AI/GenAI capabilities (DC, DR, Dev, UAT, Sandbox)		XX	XX	XX
2					
3					
4					
5	Total		XX	XX	XX

Table E: Migration Cost

Sr. No#	Services	Description	Total Cost	GST	Total Cost with GST
1	Migration Cost		XX	XX	XX
2			XX	XX	XX
	Total		XX	XX	XX

Table F: Implementation Cost of Use Cases

Sr. No#	Services	Description	Total Cost	GST	Total Cost with GST
1	Use Cases in Wave 1		XX	XX	XX
2	Use Cases in Wave 2		XX	XX	XX
3	Use Cases in Wave 3		XX	XX	XX
4	Use Cases in Wave 4		XX	XX	XX
	Total		XX	XX	XX

Table G: AMC COST

AMC Cost for Hardware Delivered in YEAR 1 & 2

S.No	Hardware Cost		Details of Hardware	YEAR 4 - AMC cost for HW delivered in Year 1			YEAR 5 - AMC cost for HW delivered in Year 1 & 2			TOTAL AMC COST for Year 4 & Year 5	GST	TOTAL AMC COST with GST
				Qty (X)	Rate (Y)	Total Amount (X x Y)	Qty (X)	Rate (Y)	Total Amount (X x Y)			
	Data Centre (DC)											
1	Servers		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Storage		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
3	GPU SERVERS		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
6	RACK		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
7	LAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

8	SAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
9	SAN Switch		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
10			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
11	Add more rows for Any other items (Please specify)		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
12			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
13			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
14			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
15			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Total - A			XX		XX	XX		XX	XX	XX	XX
	Disaster Recovery Centre (DRC)											
	Hardware Cost			YEAR 4 - AMC cost for HW delivered in Year 1		YEAR 5 - AMC cost for HW delivered in Year 1 & 2		TOTAL AMC COST for Year 4 & Year 5		GST		TOTAL AMC COST with GST

S.No	Make /Model	Part Code	Details of Hardware	Qty (X)	Rate (Y)	Total Amount (X x Y)	Qty (X)	Rate (Y)	Total Amount (X x Y)			
1	Servers		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Storage		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
3	GPU SERVERS		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
4	Load Balancer		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
5	Reverse Proxy		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
6	SAN Switch		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
7	RACK		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
8	LAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
9	SAN CABLING		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
10	Add more rows for Any other items (Please specify)		XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
11			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
12			XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Total - B			XX		XX	XX		XX	XX	XX	XX

	Total A+B	-			XX		XX	XX		XX	XX	XX	XX	XX
--	------------------	---	--	--	----	--	----	----	--	----	----	----	----	----

Table H: Facility Management Services Cost (Post Go-live of Platform)															
	BIDDER FMS		Year 1		Year 2		Year 3		Year 4		Year 5		Total Cost for 5 years	GST	Total Cost with GST
Sl. No	Resources	No. of Resources (a)	Unit Rate (b)	Cost = (a x b)	Unit Rate (c)	Cost = (a x c)	Unit Rate (d)	Cost = (a x d)	Unit Rate (e)	Cost = (a x e)	Unit Rate (f)	Cost = (a x f)			
1	Data Lakehouse	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
2	Scripting Language	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
3	PL/SQL	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
4	Reporting Tools	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
5	Analytical Tools	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
6	Ingestion Tool	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
7	CDC Tool	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
8	Infrastructure and Tools Management	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
9	Backup and Restore	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
10	OS Support	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

11	Network Management	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
12	Security Management	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
13	DBA	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
14	Add more rows for Any other items (Please specify)	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
15															
16															
17															
	TOTAL	xx		xx		xx		xx		xx		xx	xx	xx	xx

Table I:
Training and Knowledge Transfer

Sr. No#	Services	Description	Total Amount	GST	Total Amount with GST
1	Training and Knowledge Transfer		xx	xx	xx
2			xx	xx	xx
3			xx	xx	xx
4			xx	xx	xx
	Total		xx	xx	xx

TABLE J:

Change Request Cost - Post Go-live of Wave 4 Use Case/Post Go-Live of Platform

Sl. No	Description	Year 1		Year 2		Year 3		Year 4		Year 5		Total Cost	GST	Total Cost with GST
		Per Manday Cost	Cost for 100 Mandays	Per Manday Cost	Cost for 100 Mandays	Per Manday Cost	Cost for 100 Mandays	Per Manday Cost	Cost for 100 Mandays	Per Manday Cost	Cost for 100 Mandays			
1	Change Request (100 Mandays per year)	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Total		XX		XX		XX		XX		XX	XX	XX	XX

Table K: Sub-Total of KPI adherence for Early Migration & Use cases

Sr No#	Description	Total Cost	GST	Total Cost with GST
1	KPI adherence for Early Migration (2.5% of Sub-Total)	XX	XX	XX
2	KPI adherence for Use cases (2.5% of Sub-Total)	XX	XX	XX
3		XX	XX	XX
4		XX	XX	XX
	Total	XX	XX	XX

Annexure 3: Bidder's Information

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

#	Particulars	Details
1.	Name of bidder	
2.	Constitution	
3.	Address with Pin code	
4.	Authorized Person for bid	
5.	Contact Details(Mail id & Mob No)	
6.	Years of Incorporation	
7.	Number of years of experience in Data Transformation and AI Banking - Design, Supply, Install, Manage and Maintenance of Data and Gen AI Platform	
8.	Annual Turnover (In Rs.) 2022-23 – 2023-24 – 2024-25 -	
9.	Operating Profits (In Rs.) 2022-23 – 2023-24 – 2024-25 -	
10.	Net Worth (In Rs.) 2022-23 – 2023-24 – 2024-25 -	
11.	Whether OEM or authorized distributor	
12.	Number of service outlets across India	
13.	Good and Service Tax Number	
14.	Income Tax Number	
15.	Whether direct manufacturer or authorized dealers	
16.	Name and Address of OEM	
17.	Brief Description of after sales service facilities available with the bidder.	
18.	Whether all RFP terms & conditions complied with.	

Signature

Name:

Designation:

Seal of Company

Date:

Annexure 4: Letter for Conformity of Product as per RFP

Date

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: Tender No. **GEM/2026/B/7203650**

We submit our Bid Document herewith. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

We undertake that product and services supplied shall be as per the:-

Compliance	Compliance (Yes/No)	Remarks
Terms & Conditions		
Scope of Work		

(If left blank it will be construed that there is no deviation from the specifications given above)

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 5: GOI Guidelines with Model wise classification (Make in India)

Government has issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 16-9-2020 to encourage 'Make in India' and to promote manufacturing and production of goods, services and works in India with a view to enhancing income and employment.

It is clarified that for all intents and purposes, the latest revised order i.e. the order dated 16-9-2020 shall be applicable being revised Order of the original order i.e. Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 dated 15-6-2017.

The salient features of the aforesaid Order are as under:

- 1) Class-I Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%.
- 2) Class-II Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 20% but less than 50%.
- 3) Non-Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%.
- 4) The margin of purchase preference shall be 20 %, Margin of purchase preference means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference.
- 5) "Minimum Local content" for the purpose of this RFP, the 'local content' requirement to categorize a supplier as 'Class-I local supplier' is minimum 50%. For 'Class-II local supplier', the 'local content' requirement is minimum 20%. If Nodal Ministry/Department has prescribed different percentage of minimum 'local content' requirement to categorize a supplier as 'Class-I local supplier'/'Class-II local supplier', same shall be applicable.

Verification of Local contents:

The local supplier at the time of submission of bid shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content as per **Annexure 31**. Local content certificate shall be issued based upon the procedure for calculating the local content /domestic value addition on the basis of notification bearing no. F. No.33(1) /2017-IPHW dated 14-9-2017 issued by Ministry of Electronics and Information Technology read with Public Procurement (Preference to Make in India) Order 2017 Revised vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 16-09-2020.

False declaration will be in breach of the Code of Integrity under Rule 175(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per rule 151 of the General Financial Rules along with such other actions may be permissible under law.

A supplier who has been debarred by any procuring entity for violation of this order shall not be eligible for preference under this order for procurement by any other procuring entity for the duration of the debarments. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities in the manner prescribed under order No P-45021/2/2017-PP(BE- II) dated 16-092020, para 9(h).

Note:

- a) Bidder has to submit the Make in India Class-I / Class-II local supplier certificate as per attached format.
- b) Bidder has to submit proposal for all line Items.
- c) Any change in classification of Class-I and Class-II, Bidder may submit any change in class level for consideration in subsequent phases.

Purchase Preference:

1) Subject to the provisions of this Order and to any specific instructions issued by the Nodal Ministry or in pursuance of this Order, purchase preference shall be given to 'Class-I local supplier' in procurements undertaken by procuring entities in the manner specified here under,

2) In the procurements of goods or works, which are divisible in nature, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:

- Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract for full quantity will be awarded to L1.
- If L1 bid is not a 'Class-I local supplier', 50% of the order quantity shall be awarded to L1. Thereafter, the lowest bidder among the 'Class-I local supplier' will be invited to match the L1 price for the remaining 50% quantity subject to the Class-I local supplier's quoted price falling within the margin of purchase preference, and contract for that quantity shall be awarded to such 'Class-I local supplier' subject to matching the L1 price. In case such lowest eligible 'Class-I local supplier' fails to match the L1 price or accepts less than the offered quantity, the next higher 'Class-I local supplier' within the margin of purchase preference shall be invited to match the L1 price for remaining quantity and so on, and contract shall be awarded accordingly. In case some quantity is still left uncovered on Class-I local suppliers, then such balance quantity may also be ordered on the L1 bidder.

3) In the procurements of goods or works, which are not divisible in nature, and in procurement of services where the bid is evaluated on price alone, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:

- Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract will be awarded to L1.
- If L1 is not 'Class-I local supplier', the lowest bidder among the 'Class-I local supplier', will be invited to match the L1 price subject to Class-I local supplier's quoted price falling within the margin of purchase preference, and the contract shall be awarded to such 'Class-I local supplier' subject to matching the L1 price.
- In case such lowest eligible 'Class-I local supplier' fails to match the L1 price, the 'Class-I local supplier' with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the 'Class-I local supplier' within the margin of purchase preference matches the L1 price, the contract may be awarded to the L1 bidder.

4) "Class-2 local supplier" will not get purchase preference in any procurement, undertaken by procuring entities.

All others terms and condition are as per order no. No. P-45021/2/2017-PP (BE-II) dated: 16th September 2020.

Annexure 6: Undertaking of Authenticity for Products Supplied

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

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: Tender No. **GEM/2026/B/7203650**

With reference to RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking":

We hereby undertake to produce the certificate from our OEM supplier in support of this undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at any time, we agree to take back the Licenses without demur, if already supplied and return the money if any paid to us by you in this regard.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 7: Undertaking for Acceptance of Terms of RFP

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: Tender No. **GEM/2026/B/7203650**

With reference to RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking"

We understand that Bank shall be placing Order to the Successful Bidder inclusive of taxes only.

1. We confirm that in case of invocation of any Bank Guarantees submitted to the Bank, we will pay applicable GST on Bank Guarantee amount.
2. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.
3. We here by confirm to undertake the ownership of the subject RFP.
4. We hereby undertake to provide latest product/ software with latest version. The charges for the above have been factored in Bill of Material (BOM), otherwise the Bid is liable for rejection. We also confirm that we have not changed the format of BOM.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 8: Manufacturer's Authorization Form

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Dear Sir,

Sub: Tender No. **GEM/2026/B/7203650**

We (Name of the Manufacturer) who are established and reputable manufacturers of having factories at,,, and do hereby authorize M/s (who is the Bidder 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 equipment manufactured by us against the Request for Proposal received from your Bank by the Bidder and we have duly authorized the Bidder for this purpose.

We, hereby, extend warranty for the equipment and support services offered for our products supplied against this RFP by the above-mentioned Bidder.

If Bank desires transfer of the warranty and support services, supposed to be delivered by the successful Bidder, to its preferred Bidder, in such a case, OEM should transfer such warranty and support services without any additional cost to the Bank.

Yours Faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

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

Annexure 9: Integrity Pact

Integrity Pact

Between

Central Bank of India hereinafter referred to as "The Principal",

And

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

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for.....The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

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

Section 1 – Commitments of the Principal

(1.) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

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

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

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal 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 Principal will inform the Chief Vigilance Officer 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. He commits himself to observe the following principles during his participation in the tender 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 Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other

benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

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 cartelisation 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 Principal 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. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" is placed at **Annexure 20**.

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

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

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

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

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". Copy of the "Guidelines on Banning of business dealings". (As given in the **Annexure 21**)

Section 4 – Compensation for Damages

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

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal 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 Bank in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

(1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

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

If the Principal obtains knowledge of 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 Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

- 1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
- 2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.

- 3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality. In case of sub-contracting, the Principal Contractor shall take all responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-contracting, the Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.
- 4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
- 5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.
- 6) The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.
- 7) If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
- 8) The word „Monitor“ would include both singular and plural.

Section 9 – Pact Duration

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

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman & Managing Director of CENTRAL BANK OF INDIA.

Section 10 – Other provisions

- 1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.
- 2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
- 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) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail."

Section 11- FALL CLAUSE

11.1. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying same/exact product/systems or subsystems/services (i.e. same scope, deliverables, timelines, SLAs & pricing terms) at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.

Signed, Sealed and Delivered for the Principal	Signed, Sealed and Delivered for the Bidder
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____
Company Seal	Company Seal
Witness I	Witness II
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____

Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____

Annexure 10: Non-Disclosure Agreement

This **NON-DISCLOSURE AGREEMENT** (hereinafter referred as the "**Agreement**") is made at [.....] on this __ day of _____, 20__ (hereinafter referred as "**Effective Date**")

BETWEEN

_____, a company incorporated under the Companies Act, 1956 having its registered office at _____ (hereinafter referred to as "Company" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the **First PART**;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office, Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as "**Bank**" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the **OTHER PART**.

Company and **Bank** are hereinafter individually referred to as party and collectively referred to as "the Parties."

WHEREAS

Both Parties hereto are in the process of mutual discussions and negotiations regarding a possible business opportunity pursuant to [*] ("Purpose");

AND WHEREAS, in the course of evaluating the Purpose, the Parties hereto shall disclose certain information to each other which the disclosing party considers to be confidential, proprietary, or non-public business information.

NOW, THEREFORE, the Parties have agreed to enter into this Agreement:

1. Definitions:

- 1.1 "Confidential Information" any all information which is marked as confidential in writing by the Disclosing Party at the time it is provided to, obtained or accessed by the Receiving Party in connection with the Purpose and arising out of this Agreement.

If any information is provided in oral or non-written form, then such information shall be reduced in writing at the time of its disclosure or within three (3) days of such disclosure and shall be marked as 'Confidential' by the Disclosing Party or is by its nature manifestly confidential. Confidential Information excludes information referred to in clause 2 below.

- 1.2 "Disclosing Party" means Party disclosing Confidential Information under this Agreement.
- 1.3 "Receiving Party" means Party receiving Confidential Information from the Disclosing Party under this Agreement.
2. The term Confidential Information shall not include any information which:
 - a) is in or comes into the public domain through no fault of the Receiving Party;
 - b) becomes available to the Receiving Party from the third party lawfully without the breach of any confidentiality obligations by such third party;
 - c) is known or developed by the Receiving Party independently of Disclosing Party's disclosure of the Confidential Information to the Receiving Party;
 - d) is disclosed with the written consent of Disclosing Party.
3. The obligations of confidentiality under this Agreement shall not apply to the extent Confidential Information is required to be disclosed by Receiving Party so as to comply with applicable law, regulatory body, or to a valid order of a court, administrative agency or governmental body having authority over the Receiving Party or where disclosure is made in connection with any claim by Receiving Party in connection with any judicial or other proceeding involving the Receiving Party and Disclosing Party relating to this Agreement or the Purpose, provided that the Receiving Party has notified Disclosing Party in writing as soon as reasonably, legally and practicable permissible upon receiving such order and the obligations of non-disclosure under this Agreement is waived off only to the limited extent that Disclosing Party has not been able to obtain waiver or restraining order from disclosure within the timeline by which the Receiving Party is required to comply with such an order.
4. **Non-disclosure:** The Receiving Party shall not commercially use or disclose any Confidential Information or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to consultants only if the consultant has executed a Non-disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in

violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefore.

Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

5. **Term:** This Agreement shall be valid for a period of [] months from the date of signing this Agreement ("Term"). Either Party may terminate this Agreement at any time by giving [] days written notice to the other Party. Unless terminated sooner in accordance with the foregoing sentence, this Agreement shall terminate upon the earlier of:
- (i) expiry of the Term;
 - (ii) on completion of the Purpose, or
 - (iii) on the signing of a definitive agreement between the Parties relating to the Purpose.

The confidentiality obligations shall survive for a period of one (1) year from the date of expiry or termination of this Agreement.

6. **Ownership and Protection of Confidential Information and Intellectual Property:**

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall maintain ownership and all intellectual property and proprietary rights over the Confidential Information. All Confidential Information disclosed under this Agreement remains the exclusive property of the Disclosing Party. Nothing in this Agreement grants the Receiving Party any rights, title, or interest in or to any intellectual property rights, patents, copyrights, trademarks, or other proprietary rights of the Disclosing Party. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface, or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the

Receiving Party shall not add or emboss its own or any other any mark, symbol, or logo on such Confidential Information.

7. **Remedies:** The Receiving Party recognizes that Confidential Information is valuable property of the Disclosing Party and in the event of breach of this Agreement monetary damages may not be a sufficient remedy. Therefore, without prejudice to other rights or remedies that Disclosing Party may have, it would be entitled to equitable relief, including by way of injunction, as a remedy for any breach or anticipated breach of this Agreement.
8. **Return of confidential information:** Upon written demand of the Disclosing Party, the Receiving Party shall:
 - i. Cease using the Confidential Information;
 - ii. Return the Confidential Information and all copies, abstract, extracts, samples, notes, or modules thereof to the Disclosing Party within seven [X] days after receipt of notice, and
 - iii. Upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.
 - iv. Failure to comply with these obligations may result in legal action, including but not limited to claims for breach of contract and any associated damages. The Receiving Party's obligations under this agreement regarding the confidentiality of the Confidential Information shall survive the return or destruction of the Confidential Information.
9. This Agreement contains the entire understanding between the Parties with respect to non-disclosure of Confidential Information and supersedes all prior agreements and understanding with respect to this subject. This Agreement may be amended only by written agreement executed by both parties. This Agreement shall be binding on successors and permitted assigns of the parties.
10. **Notification:** Receiving Party shall notify Disclosing Party within [X] days/ hours of discovering any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.
11. **Governing Law and Judication:** This Agreement shall be governed by and construed in accordance with the laws of India without giving effect to the choice of law

principles thereof and the parties hereto irrevocably submit to the exclusive jurisdiction of the courts in Mumbai, India.

12. The provisions of this Agreement shall be severable in the event that any of the provisions hereof are held by a court of competent jurisdiction to be invalid, void or otherwise unenforceable, and the remaining provisions shall remain enforceable to the fullest extent permitted by law.
13. In no event shall either Party, its affiliates, or related entities be liable for consequential, special, indirect, incidental, punitive or exemplary loss, damage, or expense relating to this Agreement (whether in contract, statute, tort (such as negligence), or otherwise).
14. **Indemnity:** The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party or its officers, employees, agents or consultants. etc.

IN WITNESS WHEREOF, the Parties hereto have executed these presents the day, month and year first hereinabove written.

For and on behalf of

Name of Authorized signatory:

Designation:

For and on behalf of

CENTRAL BANK OF INDIA

Name of Authorized signatory:

Designation:

Annexure 11: Performance Bank Guarantee

To,

Central Bank of India, Mumbai

In consideration of Central Bank of India having Registered Office at Chandermukhi Building, Nariman Point, Mumbai 400 021 (hereinafter referred to as "Purchaser") having agreed to purchase of software, hardware & other components & services (hereinafter referred to as "Goods") from M/s ----- (hereinafter referred to as "Contractor") on the terms and conditions contained in their agreement/purchase order No----- dt.----- (hereinafter referred to as the "Contract") subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the complete Data and Gen AI Platform and solution as per the terms and conditions of the said contract, to be supplied by the contractor and also guaranteeing the maintenance, by the contractor, of the computer hardware and systems as per the terms and conditions of the said contract;

1) We, ----- (Bank) (hereinafter called "the Bank"), in consideration of the premises and at the request of the contractor, do hereby guarantee and undertake to pay to the purchaser, forthwith on mere demand and without any demur, at any time up to ----- any money or moneys not exceeding a total sum of Rs----- (Rupees-----only) as may be claimed by the purchaser to be due from the contractor by way of loss or damage caused to or that would be caused to or suffered by the purchaser by reason of failure of computer hardware to perform as per the said contract, and also failure of the contractor to maintain the computer hardware and systems as per the terms and conditions of the said contract.

2) Notwithstanding anything to the contrary, the decision of the purchaser as to whether computer hardware has failed to perform as per the said contract, and also as to whether the contractor has failed to maintain of the complete Data and Gen AI Platform and solution as per the terms and conditions of the said contract will be final and binding on the Bank and the Bank shall not be entitled to ask the purchaser to establish its claim or claims under this Guarantee but shall pay the same to the purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the contractor. Any such demand made by the purchaser on the Bank shall be conclusive and binding notwithstanding any difference between the purchaser and the contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3) This Guarantee shall expire on -----; without prejudice to the purchaser's claim or claims demanded from or otherwise notified to the Bank in writing on or before the said date i.e. ----- (this date should be date of expiry of Guarantee).

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the purchaser under or by virtue of the said contract have been duly paid and its claims satisfied or discharged

or the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the purchaser that the purchaser shall have the fullest liberty without affecting in any manner the Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the purchaser against the contractor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and the Bank shall not be released from its liability for the reasons of any such extensions being granted to the contractor for any forbearance, act or omission on the part of the purchaser or any other indulgence shown by the purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the contractor or the Bank nor shall it be affected by any change in the constitution of the purchaser by any amalgamation or absorption or with the contractor, Bank or the purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by us (whether singly or jointly with other Banks) on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing un-cancelled and we further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by us on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to our local address as mentioned in this guarantee.

10) Notwithstanding anything contained herein above: -

i) Our liability under this Bank Guarantee shall not exceed Rs------(Rupees----- only);

ii) This Bank Guarantee shall be valid up to -----;(date of expiry) and

iii) We are liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before--
- ----- (date of expiry of Guarantee plus claim period, if any)

11) The Bank has power to issue this Guarantee under the statute/constitution and the undersigned has full power to sign this Guarantee on behalf of the Bank.

Date this ----- day of ----- 2025 at -----

For and on behalf of ----- Bank.

sd/- -----

Annexure 12: Minimum Technical Specifications

Functional Requirement:

SI will size, design and implement the platform for approx. 150 use cases. However, SI will deliver 20–25 use cases under this contract. SI may refer to the list of **indicative use cases** below, for estimation and planning purposes. The detailed scope for the Use Cases will be finalized with the successful bidder. Bidder to ensure the system performance and SLA are met throughout the contract period.

The Bank reserves the right to change/modify the indicative use-case list and adjust implementation priorities based on prevailing business or regulatory requirements at the time of implementation, without incurring any additional cost to the Bank.

Each quarter, the Bank will share a list of use cases that are to be implemented as part of this initiative. These use cases will include a combination of Reporting, Business Intelligence (BI), Analytics, and GenAI applications across various business domains.

Key Performance Indicators (KPIs) will be defined for all use cases; however, adherence to the KPIs for 11 of these use cases will be linked to payment milestones.

Domain	Theme	Use case Group /Components
Growth of CASA	NTB acquisition	Driving CA acquisitions through digital marketing campaigns
		Driving SA acquisitions through digital marketing campaigns
	ETB Deepen engagement through cross sell	Cross-sell for CA customers to drive additional transaction products (e.g., salary, POS, QR, tax , bill payments) including leveraging marketing campaigns for cross-sell
		Cross-sell for SA customers to drive additional payments products (e.g., UPI, bill and tax payments, subscriptions and transfers) including leveraging marketing campaigns for cross-sell
	Churn	Identify customers likely to churn and launch interventions to reduce attrition for CA base
		Identify customers likely to churn and launch interventions to reduce attrition for SA base
	Reactivation	Reactivate dormant /inoperative CA accounts
		Reactivate dormant /inoperative SA accounts
Growth of fee income	Increase cross-sell	Cross-sell products to CA base to drive corporate fee income growth through LC (letter of credit), BG

		Cross-sell products to CA base to drive corporate/SME fee income growth through POS, Digi FMS, CMS, Insurances, virtual accounts, locker facility, CIB platform, etc.
		Cross-sell products to SA base to drive retail fee income growth through mutual funds, insurance, fastags, bill payment (BBPS), Debit cards
Growth of RAM advances	RAM NTB acquisition	Drive new acquisitions for Retail advances (incl. DLP, lead conversions and underwriting)
		Drive new acquisitions for MSME advances (incl. new acquisitions and underwriting)
		Drive new acquisitions for Agri advances (incl. DLP, lead conversions and underwriting)
	RAM ETB cross-sell	Cross-Sell Products to Retail advances customers
		Cross-Sell Products to MSME advances customers
		Cross-Sell Products to Agri advances customers
Improving collections	Collections efficiency	Driving recoveries for Agri through targeted campaigns leveraging risk segmentation, settlements (late-stage delinquencies) etc.
Reduction in fraud	Early warning systems and mule hunting	Develop anomaly detection models to flag irregularities in customer transaction behaviour using AI-driven models including using Graph Databases for connected insights
		Develop AI-driven mule hunting models to detect and flag suspicious accounts
Driving operations efficiency	GenAI led productivity	Enhancing productivity of call-centers using GenAI based call summarization
		GenAI led virtual assistant for internal employees
		Enable self-service data exploration and analysis through 'Ask your data' based insight generation
Customer analytics	Customer 360 & Lifetime value	Develop 360-degree view of the customer (e.g. portfolio of products, account history) to enable RM interventions
		Develop customer lifetime value scorecards for relationship management
Additional potential use Cases	Gen AI	GenAI-led copy and creative creation for marketing campaigns (i.e., for outbound channels generate end to end copies for SMS, Email, Whatsapp)
		Personalize landing pages for products
		Personalized humanoid bot calling for droppers

		GenAI led alert generation (e.g., tracking of key metrics for Retail app Centeez)
		Profile and tag NTB Centeez customers leveraging lookalike models
		Design interventions to improve adoption of Centeez App for Retail customers

SR #	Category	Requirement Description	Compliance (Yes/No)
FR-1	Reporting and Visualization	The solution must enable reporting dashboards and visualizations to provide actionable insights aligned with the Bank's use cases.	
FR-2	Reporting and Visualization	Reporting tools must support self-service analysis capabilities for business users.	
FR-3	Reporting and Visualization	The system must provide real-time or near-real-time data visualization based on use case needs.	
FR-4	Machine Learning (ML) and AI Use Cases	The bidder must support the design, development, training, and validation of machine learning models aligned with identified use cases.	
FR-5	Machine Learning (ML) and AI Use Cases	ML models must be integrated into operational workflows and support seamless deployment and execution.	
FR-6	Machine Learning (ML) and AI Use Cases	The solution must implement monitoring of model performance covering accuracy, latency, and resource usage.	
FR-7	Machine Learning (ML) and AI Use Cases	The bidder must establish automated model retraining workflows to address model drift and performance degradation.	
FR-8	Generative AI Capabilities	The solution must include Generative AI models configured for use cases such as content generation or summarization.	
FR-9	Generative AI Capabilities	Generative AI models must operate within the Bank's compliance and ethical guidelines.	
FR-10	Generative AI Capabilities	The solution must ensure safe and responsible AI use, with safeguards to prevent misuse or unintended consequences of outputs.	
FR-11	Generative AI Capabilities	Generative AI capabilities must be integrated into existing Bank systems and workflows.	
FR-12	Agentic AI Implementation	Agentic AI systems must support autonomous decision-making and execution for designated use cases.	
FR-13	Agentic AI Implementation	Human oversight mechanisms	
FR-14	Agentic AI Implementation	The system must include mechanisms to monitor and evaluate Agentic AI performance and reliability.	

FR-15	Agentic AI Implementation	Agentic AI must be seamlessly integrated into the Bank's decision-making and operational frameworks.	
FR-16	Use Case Impact Monitoring	The bidder must implement an automated tracking system for each use case, including:	
FR-17	Use Case Impact Monitoring	Data collection and impact metric calculation	
FR-18	Use Case Impact Monitoring	Visualization through dashboards and reports	
FR-19	Use Case Impact Monitoring	Alerts for deviations from defined thresholds	
FR-20	Use Case Impact Monitoring	The monitoring framework must be extensible to support future use cases without requiring significant architectural changes.	
FR-21	Requirement Analysis and Technical Support	The bidder must assist the Bank's Data team in:	
FR-22	Requirement Analysis and Technical Support	Analyzing and validating technical and business requirements	
FR-23	Requirement Analysis and Technical Support	Designing scalable, compliant solutions aligned with existing architecture	
FR-24	Requirement Analysis and Technical Support	The bidder must provide ongoing technical guidance, including: Data pipeline design Data quality checks Governance implementation	
FR-25	Requirement Analysis and Technical Support	Support must be provided for workflow development, model configuration, and performance optimization.	
FR-26	Platform Integration and Enablement	The solution must support seamless integration with the Bank's existing systems, tools, and data platforms.	
FR-27	Platform Integration and Enablement	The bidder must implement: Secure access controls Encryption mechanisms Audit trails to maintain data confidentiality and integrity	
FR-28	Platform Integration and Enablement	The solution must support identification and implementation of automation opportunities.	

FR-29	Platform Integration and Enablement	The bidder must provide recommendations for optimal use of compute, storage, and memory resources.	
FR-30	Deployment and Post-Deployment Support	The bidder must provide full technical support during deployment, including: Configuration Issue resolution Production transition	
FR-31	Deployment and Post-Deployment Support	Post-deployment support must include: Dashboard configuration Performance monitoring tools Documentation and knowledge transfer	
FR-32	Compliance, Ethics, and Security	The solution must enforce: Access controls, Data encryption (in transit and at rest), Audit logging for all data and AI workflows	
FR-33	Compliance, Ethics, and Security	The solution must conform to all applicable regulations including GDPR, ISO 27001, and relevant financial industry standards.	
FR-34	Compliance, Ethics, and Security	Ethical AI principles must be embedded in all ML and Generative AI components, ensuring fairness, explainability, and accountability.	
FR-35	Reporting Requirements	Typical reports to be delivered by the Bidder are given below: Top Management, H/O & Z/O Dashboards MIS Dashboards Scheduled Reports Ad hoc reports Analytical Dashboards Alert Management Regulatory Reports System Reports SLR Reports Security Reports IT Operations Reports CBS/Finacle Reports Business Verticals Reports, etc	

Non-Functional Requirement:

SR#	Category	Requirement Description	Compliance (Yes/No)
Non-FR#1	Data Source	Support for structured, semi-structured, and unstructured data from internal/external sources	
Non-FR#2	Data Source	Support ingestion of files: flat files, PDFs, Excel, logs, audio, video, images, streams, etc.	
Non-FR#3	Data Source	No limitation on type, format, or size of ingested data	
Non-FR#4	Data Source	Provide connectors to enable seamless integration with multiple data sources such as APIs, relational and non-relational databases, file-based systems, IoT devices, APIs, files, CDC, ETL, Kafka, SFTP/MFT, Message Brokers and	
Non-FR#5	Data Source	Enable both real-time (streaming), incremental and batch ingestion modes to accommodate dynamic and high-volume data workloads	
Non-FR#6	Data Source	The system must include robust pre-processing functionality to clean, validate, and normalize raw data into standardized formats suitable for analytics, machine learning, or storage.	
Non-FR#7	Data Source	The solution should support automatic extraction of metadata and the application of semantic tags to improve data discoverability, cataloguing, and contextual understanding.	
Non-FR#8	Data Source	The architecture must enable seamless integration with scalable, high-performance storage solutions optimized for different data types (e.g., object stores for unstructured data, vector databases for embeddings)	
Non-FR#9	Data Source	Solution should be able to preprocess and normalize data into consistent formats for downstream use	
Non-FR#10	Data Source	The system shall include capabilities to monitor ingestion performance, log operational metrics, and handle ingestion errors gracefully with retry and alerting mechanisms.	

Non-FR#11	Data Source	All data pipelines must enforce end-to-end encryption (in transit and at rest) and include fine-grained access controls to ensure data confidentiality, integrity, and availability	
Non-FR#12	Data Source	The solution must comply with relevant data governance policies and regulatory frameworks, such as GDPR, HIPAA, or industry-specific standards, ensuring auditability and data subject rights enforcement.	
Non-FR#13	Data Source	Secured end to end data journey for data pipeline with encryption and access controls	
Non-FR#14	Data Integration	Newly ingested data available for querying within 15 minutes (real-time) or 1 hour (batch) in Curated Zone	
Non-FR#15	Data Integration	Design and implement ETL/ELT pipelines to handle large-scale batch data ingestion and processing	
Non-FR#16	Data Integration	Automate ingestion of structured, semi-structured, and unstructured data from vendor platforms without manual intervention	
Non-FR#17	Data Integration	Parallel processing for data ingestion and replication	
Non-FR#18	Data Integration	Support joining multiple sources/tables during data ingestion	
Non-FR#19	Data Integration	Orchestration and triggering of jobs via easy-to-use interface with job status reports (success/failure/retrigger)	
Non-FR#20	Data Integration	Support data ingestion from ODBC sources, DB links, messaging queues with high throughput and low latency	
Non-FR#21	Data Integration	Provide an easy-to-use GUI for configuring data sources and selecting tables/columns for ingestion	
Non-FR#22	Data Integration	CDC solution capable of loading data into the target store(s), single or multiple, with real-time or near-real-time ingestion of incremental changes (inserts, updates, deletes) via CDC.	
Non-FR#23	Data Integration	Ensure data consistency, integrity, minimize latency, and reduce need for full reloads.	

Non-FR#24	Data Integration	CDC connector integration and pipeline orchestration	
Non-FR#25	Data Integration	Develop CDC pipelines to replicate transactional data into the Data Lakehouse	
Non-FR#26	Data Integration	Optimization CDC processes to minimize impact on source systems	
Non-FR#27	Data Integration	Mechanisms to handle schema evolution and data versioning in the target store	
Non-FR#28	Data Integration	Monitor CDC pipelines for performance and troubleshoot issues as needed	
Non-FR#29	Data Integration	Develop pipelines to process and store message-based data in the Data Lakehouse	
Non-FR#30	Data Integration	Message serialization and deserialization for efficient processing	
Non-FR#31	Data Integration	Ensure reliable message delivery using acknowledgment and retry mechanisms	
Non-FR#32	Data Integration	Buffering, processing, and streaming CDC events to Lakehouse	
Non-FR#33	Data Integration	Workflows for Automated scheduled data processing tasks should be configurable in the solution	
Non-FR#34	Data Integration	Ensure that all data acquisition methods and systems generate audit and diagnostic logs for each data load	
Non-FR#35	Data Integration	Provide a centralized metadata repository for data sourcing, sharing, and reconciliation	
Non-FR#36	Data Integration	Ensure master data integrity, standardization, and alignment across systems.	
Non-FR#37	Data Integration	Ensure low-latency processing, data consistency, scalability, fault tolerant irrespective of changes in source and to reduce the need for full/Partial data reloads	
Non-FR#38	Data Integration	Implement mechanisms ensuring low-latency data ingestion and processing	
Non-FR#39	Data Integration	Ensure fault tolerance and high availability in all streaming workflows	
Non-FR#40	Data Integration	Provide capabilities to monitor and fine-tune streaming pipelines for optimal performance	

Non-FR#41	Data Integration	Platform should ingest encrypted data from the source system. Ensure that it is compatible with the encryption and decryption mechanisms implemented at the source system	
Non-FR#42	Data Integration	The proposed tool must support data masking as stipulated by the Bank during data transformation	
Non-FR#43	Data Integration	Provide an alerting, reporting, and monitoring utility as part of the solution, including email notifications and SMS alerts to all relevant stakeholders in case of failure	
Non-FR#44	Data Integration	Incorporate automated business-defined sanity checks, validations, and data reconciliations in the data acquisition solution to ensure data integrity	
Non-FR#45	Data Integration	Implement re-runability checkpoints in data pipelines to allow scheduled executions and automatic reruns in case of failures	
Non-FR#46	Data Integration	Design data pipelines to support parallel data reading and writing into the platform	
Non-FR#47	Data Integration	Log detailed job metadata for every run, including job duration, start time, end time, user details, job status (success/failure), error messages, and other relevant information. Implement authentication and authorization controls on the metadata repository to ensure secure access	
Non-FR#48	Data Integration	Enable metadata exchange between internal and external systems. The solution should provide a common repository with facilities that are capable of sourcing, sharing, storing and reconciling a comprehensive spectrum of metadata including business, technical and operational metadata	
Non-FR#49	Data Integration	Automatic Metadata management and lineage tracking of master data	
Non-FR#50	Data Storage & Processing	Layered storage for data in-line with Access and store to optimize performance and capacity	

Non-FR#51	Data Storage & Processing	Define the architecture and directory structure of the Landing Zone to accommodate various data sources and formats	
Non-FR#52	Data Storage & Processing	Define and implement systemic data validation and quality checks to ensure data integrity before moving data into the Landing Zone	
Non-FR#53	Data Storage & Processing	Design and implement data models optimized for columnar, graph, document, Key-value, raw, File based storage formats	
Non-FR#54	Data Storage & Processing	Design the logical and physical architecture of the data lake, including folder structures and naming conventions	
Non-FR#55	Data Storage & Processing	Implement ETL pipelines to ingest, validate, and transform data into storage layer	
Non-FR#56	Data Storage & Processing	Ingestion and storage of clean, deduplicated master data	
Non-FR#57	Data Storage & Processing	Stateful stream processing and real-time analytics	
Non-FR#58	Data Storage & Processing	Batch ingestion from relational sources	
Non-FR#59	Data Storage & Processing	Low-latency access to reference data for downstream systems. Monitor AI actions and enforce policies for ethical AI usage	
Non-FR#60	Data Storage & Processing	Distributed, immutable, scalable, and fault-tolerant raw data storage	
Non-FR#61	Data Storage & Processing	Support staging areas for validation and transformation	
Non-FR#62	Data Storage & Processing	Serve as single source of truth for analytics and downstream consumption	
Non-FR#63	Data Storage & Processing	Store large volumes of structured, semi-structured, and unstructured data (CSV, images, videos, binary, etc.)	
Non-FR#64	Data Storage & Processing	Implement Data Lake to store structured, semi-structured, unstructured data, and data streams	
Non-FR#65	Data Storage & Processing	Support seamless acquisition and processing of data into the data lake with no manual intervention	
Non-FR#66	Data Storage & Processing	Ensure real-time and batch data ingestion, with streaming capabilities	

Non-FR#67	Data Storage & Processing	Provide a scalable, unified Data Lake capable of supporting all data types and formats	
Non-FR#68	Data Storage & Processing	Alert when schema/structure changes in source systems cause a mismatch with Data Lake schema	
Non-FR#69	Data Storage & Processing	Support data compression for both fast and severe compression based on processing needs	
Non-FR#70	Storage & Processing	Provide structured and optimized environment for analytical queries and reporting on curated data	
Non-FR#71	Data Storage & Processing	Provide logical separation of staging, landing, and storage layers in Data Lakehouse architecture	
Non-FR#72	Data Storage & Processing	Design solution to handle different types of workloads (CPU-intensive, storage-intensive, GPU/Performance-intensive)	
Non-FR#73	Data Storage & Processing	Support ACID transactions, indexing, and optimizations like partitioning and bucketing for large-scale analytics	
Non-FR#74	Data Storage & Processing	Support OLAP-style queries on structured data, including SQL-based querying and metadata management	
Non-FR#75	Data Storage & Processing	Support the storage, indexing, and querying of high-dimensional vector data for ML, similarity search, and recommendations	
Non-FR#76	Data Storage & Processing	Validation of vector search accuracy and integration with downstream machine learning or analytics workflows	
Non-FR#77	Data Storage & Processing	Enable efficient nearest-neighbour, hybrid, time-weighted, metadata-aware, and vector-based analytics on large datasets	
Non-FR#78	Data Storage & Processing	Secure role-based access with integration to Bank's Active Directory for AuthN and multifactor authentication to vector data	
Non-FR#79	Data Storage & Processing	Enable efficient nearest neighbour searches and vector-based analytics on large datasets	
Non-FR#80	Data Storage & Processing	Optimize Data Lake for analytical workloads, using columnar storage formats to enhance query performance	

Non-FR#81	Data Storage & Processing	Enable storage and processing of graph-structured data for advanced use cases (e.g., network analysis, recommendation systems)	
Non-FR#82	Data Storage & Processing	Support in-memory processing and real-time analytics on ingested data	
Non-FR#83	Data Storage & Processing	High performance regardless of data volume or user concurrency	
Non-FR#84	Data Storage & Processing	Key-value store for managing graph data with adjacency lists	
Non-FR#85	Data Storage & Processing	Graph database for scalable and transactional graph queries	
Non-FR#86	Data Storage & Processing	Support schema-on-read for flexible data exploration and analytics on document-based data	
Non-FR#87	Data Storage & Processing	Provide full-text search and indexing for document data	
Non-FR#88	Data Storage & Processing	Support low-latency storage and retrieval for key-value pairs enabling fast lookups and updates	
Non-FR#89	Data Storage & Processing	Support use cases like session management, caching, and real-time applications requiring high throughput	
Non-FR#90	Data Storage & Processing	Provide SQL layer on top of key-value store for querying key-value data	
Non-FR#91	Data Storage & Processing	Enable schema-on-read capabilities for flexible data exploration and support downstream transformations and processing	
Non-FR#92	Data Storage & Processing	Support schema-on-read, compression, and efficient querying for file-based datasets	
Non-FR#93	Data Storage & Processing	Seamlessly integrate with downstream/upstream applications for data push/pull	
Non-FR#94	Operations	Support for ingesting data from the Data Lakehouse to proprietary models	
Non-FR#95	Data Storage & Processing	Provide a core distributed storage layer for scalability and fault tolerance	
Non-FR#96	Data Storage & Processing	The solution should support bulk data and targeted data extracts via statistical tools and APIs	
Non-FR#97	Data Storage & Processing	Design vector database schema and indexing; generate, store, index embeddings; configure similarity search; optimize performance; validate ML integration.	

Non-FR#98	Data Storage & Processing	Design agent lifecycle management; build multi-agent workflows; integrate real-time and batch data; develop AI/ML reasoning and event triggers; optimize performance and error handling; connect knowledge graphs; ensure scalability, security, monitoring, compliance.	
Non-FR#99	Data Storage & Processing	Configure agentic long-term memory embedding generation; implement similarity search; design memory schemas; enable memory updates; integrate retrieval with agent workflows; optimize and secure memory; monitor usage; ensure governance compliance.	
Non-FR#100	Data Storage & Processing	Design and version AI workflow prompts; build and optimize RAG pipelines with vector DB; standardize prompts/retrieval; integrate AI models and external knowledge; monitor/improve pipeline; secure data; ensure compliance.	
Non-FR#101	Data Storage & Processing	Ensure tools are compatible with data quality, privacy, and security policies during data transformation	
Non-FR#102	Access	Support search for object space, tagged data sets, specific fields, or raw text	
Non-FR#103	Access	Configure tools for indexing and searching data stored in the lake house	
Non-FR#104	Access	Integrate tools to enable metadata-driven search and discovery	
Non-FR#105	Access	Design and implement data pipelines to pre-process and index data for search	
Non-FR#106	Access	Define and enforce access control policies for search operations	
Non-FR#107	Access	Support querying of both structured and unstructured data in the Data Lakehouse. Test and optimize search performance, ensuring scalability and relevance of search results	
Non-FR#108	Access	Enable SQL-like queries for data exploration and analysis	
Non-FR#109	Access	Support drill-down to individual data sources and data profiling analysis	

Non-FR#110	Access	Provide programmatic access to data in the Lakehouse through RESTful APIs, enabling integration with external systems	
Non-FR#111	Access	Provide secure API access to platform services through an API gateway	
Non-FR#112	Access	Provide Metadata and lineage APIs for data discovery, governance and tracing	
Non-FR#113	Access	Provide APIs for orchestrating and accessing data pipelines	
Non-FR#114	Access	Enable SQL-based programmatic access to structured data	
Non-FR#115	Access	Provide direct file-based access to raw and processed data	
Non-FR#116	Access	Enable seamless and secure access to data by integrating with enterprise identity management systems	
Non-FR#117	Access	Provide centralized authentication and authorization, reducing the need for multiple credentials	
Non-FR#118	Access	Implement SSO integration with platform services for better security and user experience	
Non-FR#119	Access	The solution must provide role-based access to reports and dashboards, ensuring granular data access based on user roles	
Non-FR#120	Access	Facilitate secure and scalable access to machine learning models and data via APIs	
Non-FR#121	Access	Provide open REST APIs for automated provisioning, reporting, and integration with DevOps and MLOps tools	
Non-FR#122	Access	Develop a centralized registry for managing agent APIs and tool integrations	
Non-FR#123	Access	Ensure API versioning and backward compatibility for smooth updates	
Non-FR#124	Access	Dynamic discovery of APIs and tools for agents	
Non-FR#125	Access	Monitor API usage and performance with observability tools	
Non-FR#126	Access	Automate API documentation generation	
Non-FR#127	Access	Manage data pipelines that prepare data for search indexing	

Non-FR#128	Access	Support search for values within columns/tables of reports and full-text search capabilities	
Non-FR#129	Access	Support fast and scalable search across structured, semi-structured, and unstructured data for analytics and discovery	
Non-FR#130	Access	The solution must integrate with a distributed search engine for indexing file-based data	
Non-FR#131	Access	Enable bank branch users to access reports via the Bank's portal, with responsibility for required network configurations	
Non-FR#132	Access	The Platform shall provide a standardized and secure Tool Interface with a centralized Agent API Registry to enable governed, versioned, discoverable, and monitored interactions between agents, tools, and external systems using Standard API communication protocol.	
Non-FR#133	Consumption	Test APIs for reliability, scalability, and fault tolerance	
Non-FR#134	Consumption	Set up tools to deploy models as APIs	
Non-FR#135	Consumption	Implement version control and monitoring for deployed models in the Model Hub	
Non-FR#136	Consumption	Implement end-to-end visualization solution for existing and new reports	
Non-FR#137	Consumption	The proposed solution must support visualization for all types of structured, semi-structured, and unstructured data, including clickstream, audit logs, documents, multimedia data (images, videos, audios), XBRL format	
Non-FR#138	Consumption	The solution must be able to connect to various data sources, such as delimited files, Excel, XML, SQL/NoSQL databases, and more	
Non-FR#139	Consumption	The solution must have data blending capabilities, allowing users to blend data from multiple sources (e.g., mapping or creating relationships across data sources)	

Non-FR#140	Consumption	The proposed consumption solution should be integrated seamlessly with Data Lakehouse, Data Marts, Feature Mart, etc.	
Non-FR#141	Consumption	The solution should allow BI users to save queries, data filters, and drill-down paths used in decision-making processes for future reuse	
Non-FR#142	Consumption	Enable generation of interactive and static reports from data stored in the Lakehouse	
Non-FR#143	Consumption	Dashboard should support advanced data filtering with visual and static filters to slice and dice data by selecting chart sections or conditions	
Non-FR#144	Consumption	Validate report accuracy, scalability, and usability to meet business requirements	
Non-FR#145	Consumption	The solution must support an easy-to-create and maintain reporting framework/model containing business concepts and measures	
Non-FR#146	Consumption	The solution should support features such as alerts (threshold-based), collaboration, white-labelling, open integration, and more	
Non-FR#147	Consumption	The solution should allow users to create customizable ad-hoc reports via a report writer with drag-and-drop functionality	
Non-FR#148	Consumption	Integrate BI tools with the lake house for dashboard creation and configure tools to support dashboard queries	
Non-FR#149	Consumption	Optimize data pipelines and queries for real-time dashboard performance	
Non-FR#150	Consumption	The system must enable seamless consumption of data by downstream applications in required formats and frequencies	
Non-FR#151	Consumption	The solution must integrate with BI Tools like Tableau, Power BI, or Qlik for report generation and visualization	
Non-FR#152	Consumption	Enable real-time and interactive visualizations of data stored in the Lakehouse for monitoring, trend analysis, and decision-making	
Non-FR#153	Consumption	Enable custom web and mobile applications to consume and visualize	

		data from the Lakehouse via APIs or direct queries	
Non-FR#154	Consumption	Support real-time and batch data pipelines with tailored interfaces for specific business use cases	
Non-FR#155	Consumption	Provide real-time and batch data delivery to mobile apps, enabling interactive visualizations, notifications, and decision-making on the go	
Non-FR#156	Consumption	Data exploration tools shall support SQL-based querying, data profiling, and visualization for analysts and data scientists to derive insights quickly	
Non-FR#157	Consumption	The machine-learning platform should either support multiple models out of the box or allow custom coding for ML models	
Non-FR#158	Consumption	Data exploration tools shall support both real-time and batch reporting, querying large datasets effectively	
Non-FR#159	Consumption	Automate reporting processes with minimal manual intervention from the bank side	
Non-FR#160	Consumption	Support automated scheduling of reports and provide delivery status to users	
Non-FR#161	Consumption	Provide drag-and-drop, slice-and-dice, and other runtime customization features for reports and dashboards	
Non-FR#162	Consumption	Ensure reports and dashboards are accessible via mobile devices with support for multiple screen resolutions	
Non-FR#163	Consumption	Design output pipelines for delivering multi-modal content (text, images, audio, video, etc.).	
Non-FR#164	Consumption	Personalization and contextual adaptation of outputs for end-users.	
Non-FR#165	Consumption	The reporting solution should be high performing, scalable, resilient, and reliable to handle all demands without a single point of failure	

Non-FR#166	Consumption	Provide tools to migrate reports from the existing solution to the new solution in coordination with the bank's MIS team	
Non-FR#167	Consumption	Proposed solution should support account-specific reports based on discussions with the bank during implementation	
Non-FR#168	Consumption	Integrate with tools for advanced data exploration and analysis workflows	
Non-FR#169	Consumption	Configure tools to support interactive data exploration	
Non-FR#170	Consumption	Reporting and Dashboard solution shall provide drill-down features such as transaction level, sequential, cyclical, and visual drill downs	
Non-FR#171	Consumption	The reporting solution must support all required formats, including but not limited to: Excel, PDF, delimited files, XBRL, XML, and others	
Non-FR#172	Consumption	Data Platform Solution shall Integrate seamlessly with BI tools for enterprise reporting and dashboards	
Non-FR#173	Consumption	Ability to deploy models as standard APIs or services	
Non-FR#174	Sandbox/ Workbench	Model Development and Experimentation: Supports multiple machine learning models out-of-the-box and allows for custom coding of additional algorithms. Provides a secure, isolated sandbox environment for experimentation, model training, and analytics workflow development. Facilitates interactive data exploration and model development in a collaborative setting. Enables seamless building, training, tuning, and deployment of machine learning models. Supports deep learning and advanced machine learning model training with scalable compute resources. Offers tools for statistical computing, data visualization, and advanced data	

		analysis using popular programming languages such as Python, R, and Scala.	
Non-FR#175		Integration with Lakehouse Architecture Fully integrates with the Lakehouse for: Seamless access to raw and processed datasets. Running distributed computations. Training, deploying, and inferencing ML and LLM models. Enables interactive and batch analysis workflows leveraging the Lakehouse's storage and compute capabilities.	
Non-FR#176		Data and Artefact Management: Provides high-performance, scalable storage for: Intermediate datasets, Experiment outputs and results, Model artefacts, Large training and validation datasets. Enables experiment-specific artefact tracking and storage. Supports metadata management and lineage tracking of models and datasets.	
Non-FR#177		Compute Infrastructure and Resource Management: Delivers robust, scalable infrastructure to support isolated, resource-intensive data science workloads. Provides distributed processing environments to support: Advanced analytics, Machine learning workflows, Data transformations. Supports interactive and batch job execution in isolated containers or environments. Infrastructure provisioning, monitoring, and resource management. Container orchestration and resource isolation. Distributed workload scheduling and compute resource allocation. Monitoring of resource utilization and performance for cost optimization.	

Non-FR#178		Language and Framework Support: Supports multiple programming languages (like Python, R, Scala, etc). Compatible with leading data science libraries and frameworks (e.g. TensorFlow, PyTorch, scikit-learn). Enables integration with popular data science IDEs and notebook environments (e.g., Jupyter, Zeppelin).	
Non-FR#179		Collaboration and Version Control: Facilitates seamless collaboration among data scientists, analysts, and engineers via shared environment Supports Real-time collaborative editing of notebooks and code. Experiment tracking and result sharing. Version control for code, models, and notebooks (e.g., via Git). Metadata and lineage tracking for datasets and experiments. Shared visualization and communication tools for insight dissemination.	
Non-FR-180		SLM / LLM : Tools configured for SLM / LLM experimentation and fine-tuning GPU-enabled infrastructure nodes set up ML/DL frameworks integrated for model development and fine-tuning Distributed processing for SLM / LLM workflows enabled SLM / LLM workflows validated for performance, scalability, security, governance compliance	
Non-FR#181	Sandbox - Prompting	The Platform shall provide a governed environment for interactive prompt engineering, enabling iterative prompt experimentation and evaluation using notebooks and on premise fine-tuned models, with support for distributed processing and validation of performance, scalability, and compliance with data governance policies.	

Non-FR#182	Sandbox - Collaboration	The Platform shall provide collaboration tools with shared workspaces, version-controlled code repositories, and shared notebooks to enable team-based development and analysis, along with metadata and lineage tracking to ensure seamless sharing, traceability, and governed collaboration.	
Non-FR#183	Operations	Orchestration, scheduling (based on resource awareness) and monitoring of real-time pipelines and workflows	
Non-FR#184	Operations	Define Task dependencies, Check pointing and re-run ability	
Non-FR#185	Operations	Parallel read/write to repository and AI/ML platforms	
Non-FR#186	Operations	Pipeline failure handling and resume from last checkpoint	
Non-FR#187	Operations	Logging of job metadata (start/end time, status, errors, user)	
Non-FR#188	Operations	Solution should be able to collect and manage logs from Platform components and services and then Integrate them centralized log aggregation, search, and visualization.	
Non-FR#189	Operations	Define log retention, archiving, and access policies to comply with governance and audit requirements	
Non-FR#190	Operations	Platform should Provide Observability Tools for: Monitoring and alerting across all layers — infrastructure, network, storage, and computing resources Data Observability for Movement of data between various layers including AI models.	
Non-FR#191	Operations	Platform should collect and visualize real-time data including GPU usage, memory throughput, network performance, data pipeline latency, streaming jobs and job execution details, with configurable alerts for anomalies	

Non-FR#192	Operations	Reusability of tagged datasets and operators across ML pipelines	
Non-FR#193	Operations	Platform should support the integration with analytical tools, statistical tools, and AI/ML tools for reporting and analysis	
Non-FR#194	Operations	User-friendly tools for model evaluation, deployment, and visualization	
Non-FR#195	Operations	Integration with open-source, proprietary, or supported tools (e.g., Python, R, SAS, TensorFlow, etc.)	
Non-FR#196	Consumption	Platform should support the adhoc, canned, and automated distributed reports to downstream systems (like CRM, OFSAA, etc.)	
Non-FR#197	Operations	Platform should support the analytics types: benchmarking, predictive, web, social, geo, trend, profit, etc.	
Non-FR#198	Operations	Platform should support the model creation using languages like Python, R, etc. & platform like Keras, TensorFlow, SAS, etc.	
Non-FR#199	Operations	Platform should build automated pipelines for ML lifecycle (prep → train → deploy)	
Non-FR#200	Operations	Platform should support the collaborative notebooks (Jupyter-style)	
Non-FR#201	Operations	Platform should be capable with tools for model deployment, monitoring, retraining, and versioning	
Non-FR#202	Operations	Platform should have Real-time or near-real-time analytics capabilities	
Non-FR#203	Operations	Analytics platform should allow seamless integration with the Lakehouse for data access, distributed computations, and model deployment	
Non-FR#204	Operations	The streaming analytics platform must process thousands of events per second, with end-to-end latency kept sub one second for real-time insights. It should support complex event processing and windowing, capable of	

		handling 10 or more simultaneous use cases efficiently	
Non-FR#205	Operations	Platform should be tightly coupled with underlying data Lakehouse storage to manage raw streaming data and processed outputs, supporting batch and micro-batch analytics	
Non-FR#206	Operations	Enable collaborative development of machine learning models, with version control and metadata lineage tracking	
Non-FR#207	Operations	Containerize models and orchestrate deployments, Integrate with tools for real-time data streaming and inference workflows	
Non-FR#208	Operations	Provide scalable storage for data scientists to store intermediate datasets, experiment outputs, and model artefacts	
Non-FR#209	Operations	Support distributed data processing and machine learning workflows, including support for multiple programming languages (e.g., Python, R, Scala)	
Non-FR#210	Operations	Provide tools and infrastructure to experiment with, fine-tune, and deploy small & large language models for NLP tasks	
Non-FR#211	Operations	Facilitate collaborative data analysis with shared environments, version control, and real-time collaboration for code, notebooks, and experiment tracking	
Non-FR#212	Operations	Support version control, CI/CD pipelines, and automated testing for code, scripts, and configuration files	
Non-FR#213	Operations	Validate version control and CI/CD workflows to ensure traceability, security, and automation	
Non-FR#214	Operations	Provide a centralized hub for managing, deploying, and monitoring machine learning models with version control	

Non-FR#215	Operations	AutoML features for generating optimal models from candidates	
Non-FR#216	Operations	Provide insights into model behaviour, predictions, and decision-making processes to ensure transparency and compliance	
Non-FR#217	Operations	Create realistic simulation environments to rigorously test AI agent behaviours and workflows, Enable scenario-based testing for edge cases and failure conditions	
Non-FR#218	Operations	Establish and enforce safety, compliance, and operational boundaries within AI systems	
Non-FR#219	Operations	Enable testing of AI systems under various scenarios, including edge cases and failure conditions.	
Non-FR#220	Operations	Monitor AI actions and enforce policies for ethical AI usage	
Non-FR#221	Operations	Integrate feedback loops to refine guardrails and improve system reliability	
Non-FR#222	Operations	Ensure the system is scalable, secure, and adheres to governance standards	
Non-FR#223	Operations	Implement centralized logging for aggregating and analysing logs from platform components to ensure system efficiency and fault detection	
Non-FR#224	Operations	Ensure the logging solution supports audit logs, enabling efficient troubleshooting, auditability, and error detection	
Non-FR#225	Operations	Provide logging controls, allowing the user to specify which events to log (e.g., log failures only) to reduce overhead	
Non-FR#226	Operations	Ensure logging of all user activities related to operational activities without impacting system performance	
Non-FR#227	Operations	The system must generate audit and diagnostic logs for every data load or acquisition process	

Non-FR#228	Operations	A complete report of all executed jobs should be sent via email to stakeholders, highlighting failed or delayed jobs	
Non-FR#229	Operations	Observability tools should integrate smoothly with standard monitoring platforms used in enterprises	
Non-FR#230	Operations	The observability system should scale with workload growth (supporting approx. 150 use cases) and provide sufficient long-term storage for logs and metrics to support audit and compliance requirements	
Non-FR#231	Operations	Monitor reporting jobs daily, with automated alerts (email/SMS) on job success/failure status	
Non-FR#232	Operations	Enable threshold-based and event-based alerts for report job status to individual/group mailboxes	
Non-FR#233	Operations	The bidder must implement a logging & monitoring solution for audit control, real-time health monitoring, and performance alerts	
Non-FR#234	Operations	Provide real-time infrastructure monitoring, including metrics collection, visualization, and alerting for performance and availability	
Non-FR#235	Operations	An alerting report and monitoring utility should be implemented. In case of failure, email alerts and mobile SMS should be sent to stakeholders	
Non-FR#236	Operations	Enable automated integration of code changes into a shared repository, ensuring continuous testing, validation, and build processes	
Non-FR#237	Operations	Automate builds, tests, and integration workflows to detect integration issues early, improving code quality and accelerating development	
Non-FR#238	Operations	Provide integrated version control, continuous integration pipelines, build dependency management, and static code analysis	
Non-FR#239	Operations	Automate the deployment of validated code, configurations, and artifacts into production or staging, ensuring repeatable and error-free deployments	

Non-FR#240	Operations	Ensure rollback mechanisms for deployments to ensure stability and consistency during releases	
Non-FR#241	Operations	Enable tracking, managing, and versioning of ML models and associated metadata throughout their lifecycle	
Non-FR#242	Operations	Support deployment of ML models into production environments for real-time or batch inference with scalability and monitoring	
Non-FR#243	Operations	Monitor model performance, resource usage and ensure governance of deployed models to support business-critical analytics operations	
Non-FR#244	Operations	Manage and automate complex workflows and dependencies across data pipelines, analytics processes, and ML operations	
Non-FR#245	Operations	Enable tracking and versioning of data pipelines, ensuring reproducibility, traceability, and rollback capabilities	
Non-FR#246	Operations	Deploy explainability workflows, Visualize explainability metrics via dashboards, Validate explainability workflows against regulations	
Non-FR#247	Operations	Implement safety and compliance guardrails	
Non-FR#248	Operations	Detect and mitigate real-time anomalies	
Non-FR#249	Operations	Monitor agent actions and enforce ethical AI policies	
Non-FR#250	Operations	Integrate feedback loops to improve reliability, Ensure scalability, security, and governance alignment	
Non-FR#251	Operations	Central monitoring Dashboard/console for Platform components, container environment, cluster health, analytics performance and resource usage	
Non-FR#252	Operations	Integrate with centralized log aggregation and analysis system of the Bank	
Non-FR#253	Operations	Monitoring and governance of ingestion pipelines	
Non-FR#254	Operations	Define and configure alerting thresholds for critical metrics and events	

Non-FR#255	Operations	Validate monitoring workflows to ensure comprehensive coverage, real-time alerts, and actionable insights	
Non-FR#256	Operations	Provide real-time telemetry-based information for data lakehouse solutions (e.g., CPU, memory, temperature, etc.)	
Non-FR#257	Operations	Automated notifications for data transmission loss (connectivity/system/hardware failures)	
Non-FR#258	Security	Implement mechanisms to detect and address errors or anomalies in real-time	
Non-FR#259	Security	Ensure sensitive data protection by applying dynamic or static data masking techniques to maintain privacy while supporting analytics	
Non-FR#260	Security	Define and enforce data masking policies at the query level and during data ingestion/transformation for compliance	
Non-FR#261	Security	Implement anonymization techniques for sensitive data, ensuring compliance with data privacy regulations (e.g., PII)	
Non-FR#262	Security	Ensure data encryption both at rest and in transit, using appropriate key management practices to protect against unauthorized access	
Non-FR#263	Security	Enable TLS 1.2+ version with Forward Secrecy encryption for securing data in transit between Platform services and clients. SSL 2.0, 3.0, TLS1.0, TLS1.1 to be disabled to avoid latest Vulnerabilities	
Non-FR#264	Security	Ingest encrypted data and support source-side encryption/decryption mechanisms	
Non-FR#265	Security	Must enforce the use of Strong Cipher Suites to ensure secure communication over the network	
Non-FR#266	Security	Verify the identity of users, applications, and services, via integration with the Bank's IDP systems	
Non-FR#267	Security	Implement fine-grained access control using RBAC (Role-Based	

		Access Control) or ABAC (Attribute-Based Access Control)	
Non-FR#268	Security	Enforce anonymization policies on sensitive data fields at query level to ensure consistent anonymization across the data lakehouse	
Non-FR#269	Security	Maintain audit trails for all data access and user activities across the system, ensuring compliance and traceability	
Non-FR#270	Security	Encrypt sensitive data at rest in the platform distributed storage and during data transfer between services	
Non-FR#271	Security	Provide centralized auditing of all user activities, data transformations, and access to ensure compliance and security	
Non-FR#272	Security	The solution must provide application-level security, data-level security, single sign-on, and audit capabilities	
Non-FR#273	Security	Secure the individual hosts in the data lakehouse cluster with, malware protection, and system hardening	
Non-FR#274	Security	Monitor and secure cluster-level activities to prevent unauthorized access, vulnerabilities, and security breaches	
Non-FR#275	Security	Implement intrusion detection and malware protection for hosts within the data lakehouse cluster to ensure security	
Non-FR#276	Security	Centralized log aggregation for security events	
Non-FR#277	Security	Real-time analytics for anomaly and threat detection	
Non-FR#278	Security	External feeds for vulnerabilities and threat intelligence	
Non-FR#279	Security	Unified security policies integrated across systems	
Non-FR#280	Security	Track data origin, transformations, and usage	
Non-FR#281	Security	Intuitive visual tools to explore data lineage	
Non-FR#282	Security	Implement role-based access control (RBAC) to ensure security and privacy	

Non-FR#283	Security	Support ingestion of encrypted data from source systems and handling the encryption/decryption mechanisms	
Non-FR#284	Security	Ensure the ability to propagate changes to the data dictionary and business glossary in real-time	
Non-FR#285	Security	Review and implement conformance to governance policies and processes periodically (monthly/quarterly)	
Non-FR#286	Security	Enforce security and privacy controls, ensuring data inside the Data Lake is accessible only by authorized users	
Non-FR#287	Security	Support data encryption (at rest and in transit)	
Non-FR#288	Security	Integrate with Active Directory for authentication	
Non-FR#289	Security	Implement additional security features such as multi-factor authentication and data encryption	
Non-FR#290	Security	Provide password protection for accessing reports from mobile devices via web-based mobile configuration interface	
Non-FR#291	Security	Provide proactive security and software advisory alerts, with fixes to address potential issues	
Non-FR#292	Security	The infrastructure must comply with Bank's IT/Information Security/Cyber Security policies, IT Act 2000, and other statutory and regulatory requirements	
Non-FR#293	Security	The solution should be compliant with RBI guidelines for data reporting and analytics	
Non-FR#294	Security	Masked data must remain analytically usable	
Non-FR#295	Security	Mask specific columns/tables on demand	
Non-FR#296	Security	Substitution, Nullifying, Spacing, FPE, Number/date variance	
Non-FR#297	Security	Tools to identify weak passwords and ransomware patterns	
Non-FR#298	Security	Protection and detection capabilities against ransomware	
Non-FR#299	Security	Data Lake must meet Basel Committee's BCBS 239 standards	
Non-FR#300	Security	AES 256, FIPS certified, minimal impact	

Non-FR#301	Security	SLA-compliant encryption with minimal latency	
Non-FR#302	Security	Based on discussions with data owners	
Non-FR#303	Security	Expose APIs for integration with encryption tools	
Non-FR#304	Security	Restrict admin overrides for encryption rules	
Non-FR#305	Security	Identify gaps in current DLP - Data Loss Prevention solution	
Non-FR#306	Security	Assess firewall setup and recommend improvements	
Non-FR#307	Security	Review and improve integration with IPS tools	
Non-FR#308	Security	Evaluate Web Application Firewall for compatibility	
Non-FR#309	Security	Ingest logs, identify threats, and ensure visibility in SIEM	
Non-FR#310	Security	Integrate with Privileged Access Management solutions	
Non-FR#311	Security	Analyze logs as per bank's policies	
Non-FR#312	Security	Log ingestion and monitoring in real-time	
Non-FR#313	Security	Predefined workflows for detection, response, and recovery	
Non-FR#314	Security	Conduct internal penetration tests and resolve findings	
Non-FR#315	Security	Solution should ensure that masked data is usable. Also, propose tools should have selective masking of columns functionality in user specified tables	
Non-FR#316	Security	Perform and resolve external assessments	
Non-FR#317	Security	Implement patch updates and manage them regularly	
Non-FR#318	Security	Provide a secure, isolated environment for data scientists to experiment, build, and test machine learning models and analytics workflows	
Non-FR#319	Security	Implement data masking as required during data transformation	
Non-FR#320	Data Governance	Support secure access and enforcement of data governance policies	
Non-FR#321	Data Governance	Implement data quality solution from origin to consumption, with	

		connectivity to wide range of data sources	
Non-FR#322	Data Governance	Metadata governance and version control	
Non-FR#323	Data Governance	Implement data cleansing, including record deduplication logic and data correction files	
Non-FR#324	Data Governance	Implement automated sanity checks, validations, and reconciliation of data to ensure integrity	
Non-FR#325	Data Governance	Build data quality dashboards with alerts to notify administrators of data quality issues	
Non-FR#326	Data Governance	Ensure the system identifies and flags data issues in source systems related to integrity constraints and domain rules	
Non-FR#327	Data Governance	Implement remediation plan for identified data quality gaps, performing root-cause analysis	
Non-FR#328	Data Governance	Provide traceability of data transformations and rules from source to downstream systems	
Non-FR#329	Data Governance	Associate glossary with technical metadata	
Non-FR#330	Data Governance	Discover, classify, and trace lineage of metadata	
Non-FR#331	Data Governance	Centralized repository for managing metadata, enabling data discovery, classification, and lineage tracking	
Non-FR#332	Data Governance	Facilitate collaboration by allowing users to search, understand, and govern data assets effectively within the data lake house	
Non-FR#333	Data Governance	User-friendly glossary interface with external tool integration	
Non-FR#334	Data Governance	Ensure data accuracy, completeness, consistency, and reliability across the data lake house	
Non-FR#335	Data Governance	Tools for monitoring, profiling, and validating data	
Non-FR#336	Data Governance	Metadata-driven policy creation and governance	
Non-FR#337	Data Governance	Centralised Policy-based enforcement of quality metrics	
Non-FR#338	Data Governance	Notifications for data quality issues	
Non-FR#339	Data Governance	Policy enforcement for access, usage, and compliance	

Non-FR#340	Data Governance	Track policy compliance and user activity	
Non-FR#341	Data Governance	Analyse and understand data patterns and anomalies	
Non-FR#342	Data Governance	Evaluate and classify data across the Lakehouse	
Non-FR#343	Data Governance	Integrate the catalogue with external tools and workflows	
Non-FR#344	Data Governance	Implement end-to-end data governance solution including metadata management	
Non-FR#345	Data Governance	Support parallel processing for data governance tasks, including handling concurrent users	
Non-FR#346	Data Governance	Provide change management features for tracking versioning and migration of code	
Non-FR#347	Data Governance	Provide data lineage views, tracking data flow and transformations from source to downstream systems	
Non-FR#348	Data Governance	Implement a reconciliation methodology for each source system, with real-time reporting and alerts for discrepancies	
Non-FR#349	Data Governance	Provide error drill-down for reconciliation failures, identifying errors on a near real-time basis	
Non-FR#350	Data Governance	Implement data masking for sensitive fields as required by the bank	
Non-FR#351	Data Governance	Ensure unmasking of data is restricted as per user requirements	
Non-FR#352	Data Governance	Provide data reconciliation status for each data load and movement	
Non-FR#353	Infrastructure	Entire Data Lakehouse platform i.e. Hardware, System Software and associated software tools should be able to design and deploy as per given Service Level Agreement throughout the Contract Period	
Non-FR#354	Infrastructure	Design and deploy GPU-enabled clusters within the Platform ecosystem to support ML/DL workloads, dedicated servers, Virtual machines, container environment considering CPU, memory, storage, and network requirements	
Non-FR#355	Infrastructure	Integration of analytics engine with GPU libraries for accelerated data processing	

Non-FR#356	Infrastructure	Design and deploy dedicated servers, considering CPU, memory, storage, and network requirements	
Non-FR#357	Infrastructure	Blade Server/Rack server with latest Generation processors, GPU/on-chip AI accelerator	
Non-FR#358	Infrastructure	- Servers must be rack-mounted and equipped with dual 32-core Intel Xeon Platinum CPUs (2.7 GHz or better) or equivalent CPU that support the latest computational and graphics accelerators. - High density servers with in-built liquid cooling should be available to support current and future demands - The servers must support real-time. hardware performance monitoring and alerting, agent-free monitoring, driver updates, and configuration. - The solution must include features for power monitoring and capping, RAID management, external storage management, and monitoring of Fiber Channel, Host Bus Adapters (HBAs), I/O ports, and overall system health. - The servers must support at least six PCI-Express 3.0 slots, including at least two x16 PCIe slots	
Non-FR#359	Infrastructure	Server Minimum Specification: - Server should be compact but equipped with redundancy to avoid any single point of failure. 512 GB DDR5 5600 MHz RAM (using 64GB DIMMs), scalable to 4 TB. Capable of identifying and reporting whether genuine OEM memory is installed. - Must support min 32 DDR5 DIMM slots (RDIMMs/LRDIMMs) with speeds of 5600 MT/s or higher and having advanced memory protection features, including ECC with multi-bit error protection, online spare, mirrored memory, and fast fault tolerance - Server shall be Controller Embedded / PCIe based or connected over the Fiber Channel via FCP to support RAID controller supporting RAID,1, 5, 6, 10, 50, 60.	

		Server should support Operating Systems and Virtualization Software proposed as part of solution	
Non-FR#360	Infrastructure	GPU minimum specification: Each GPU card should have a memory capacity of 141 GB or more to handle large and complex AI models. Any model of the GPU from the OEM should be in use in any Bank in India. The memory type must be HBM3e with a memory bandwidth of up to 4.8 TB/s or higher to support demanding tasks. GPU slicing with minimal performance overhead should be available. SI/Bidder must ensure that all GPUs are supplied with the appropriate interface and power connections required for their type and form factor. It should offer seamless interconnectivity options to enable the formation of powerful GPU clusters and support high-speed interconnect technologies (NVLink, NVSwitch) with a bi-directional bandwidth of approximately 900 GB/s. Additionally, it must be compatible with PCIe Gen5 X 16 (128 GB/s) interconnects and deliver performance metrics of FP64 equivalent to or exceeding 30-34 TeraFLOPs and FP32 equivalent to or exceeding 60-67 TeraFLOPs. SI to ensure GPUs are supplied with all the required specific proprietary software stack including but not limited to LLMs, Tool kit, drivers, control panel, etc. Each server must include a minimum of 512 GB DDR5 5600 MHz RAM (using minimum 64GB DIMMs), scalable to minimum 4 TB in a fully populated configuration. The servers must be capable of identifying and reporting whether	

		genuine OEM memory is installed to ensure system reliability. • The servers must support minimum 32 DDR5 DIMM slots (RDIMMs/LRDIMMs) with speeds of 5600 MT/s or higher and provide advanced memory protection features, including ECC with multi-bit error protection, online spare, mirrored memory, and fast fault tolerance. • Server shall be Controller Embedded / PCIe based or connected over the Fiber Channel via FCP to support RAID controller supporting RAID,1, 5, 6, 10, 50, 60. • Server should support Operating Systems and Virtualization Software proposed as part of solution. All kind of software licenses should be provided by the bidders.	
Non-FR#361	Infrastructure	•The servers must support a minimum of 12 x 2.5" SSD/NVMe drives and include a RAID controller with 12GB NV Cache, supporting RAID levels 1, 5, 6, 10, 50, 60. •The storage controller must support secure encryption/data-at-rest encryption and hardware RAID for NVMe disks •NVMe drives intended for hot-tier workloads shall be directly connected and not bottlenecked by shared controllers. •NVMe drives (with min. IOPS-5000) should be provided for Hot Tier & Production workloads, which should be directly connected and not bottle necked by shared controllers. However, to meet SLA SI/Bidder to provide NVMe drives in Warm/Cold Tier as well as UAT, Dev, Sandbox wherever required	

		•Throughput to be assessed by the Storage size, data transformation window, etc •Storage performance testing aligned to expected workloads shall be included as part of acceptance testing •Storage performance figures shall be validated during acceptance testing under representative workloads	
Non-FR#362	Infrastructure	• User and application traffic: at least 2 dual-port 25 Gb Base-SFP+ network interface cards (NICs) and transceivers. • Management: Dedicated management port with 1× 1GbE for BMC and 10 GbE for OS Management • Storage Network: 2× 200 Gb Ethernet ○ Support for RoCE v2, Jumbo Frames, NVMe-oF (wherever applicable) • GPU/ AI Network: ○ 2× 200 Gb or higher NICs per GPU server ○ GPUDirect RDMA ○ InfiniBand or RoCE Ethernet • Intra-Node GPU Connectivity: ○ NVlink Switch 900 Gb/s per GPU pair • Minimum of 12 PCIe Gen5 slots or more for upgrades (SmartNIC, additional GPU, DPU, or accelerator card). SI to ensure CPU and GPU clusters connectivity to meet the SLA.	

		- The servers must include a minimum of 1 VGA/video port, 2 x USB 2.0/USB 3.0 ports, dedicated management ports, and support for serial, MicroSD, and USB 3.0 interfaces. - The servers should support and be certified for the operating system proposed to be installed and must integrate with leading server management software.	
Non-FR#363	Infrastructure	NV Link Switch Specification: - High Bandwidth Interconnect: The NVLink switch should provide a minimum bandwidth of 900 GB/s per GPU pair, ensuring fast communication between GPUs to handle heavy AI and analytics workloads effectively. - Scalability: It must support scaling up to at least 16 GPUs per cluster, delivering low latency and high throughput to enable efficient parallel processing across multiple GPUs. - Compatibility: The switch should be compatible with common enterprise-grade GPUs (such as NVIDIA H200) widely used in AI and analytics solutions. - Reliability and Redundancy: Features like failover support and error correction are necessary to maintain uninterrupted data flow and high availability. - The bidder/SI shall submit indicative rack-level and cluster-level GPU interconnect layouts.	

Non-FR#364	Infrastructure	• SAN-based storage facilities must be provisioned for all environments. • The proposed solution should ensure high-speed and low-latency storage networking. • The SAN fabric shall be dual-fabric with multipathing, lossless, NVMe-oF capable, and fully redundant, providing line-rate performance, zero packet loss, and microsecond end-to-end latency to meet enterprise Lakehouse and GenAI SLAs, which will be validated during acceptance testing. • There should not be any oversubscription for storage paths. Automatic path failover without I/O interruption. • The SAN and network switches must be designed to accommodate port-level redundancy, path level redundancy, etc ensuring high availability and fault tolerance for critical operations. • All critical hardware components, including but not limited to Switch, Link, Optics, Power Supply, Control Plane, Hard disks, PCI cards, fans, etc. shall not possess any single point of failure and must be hot-swappable to ensure zero downtime. • Software & Control Plane capabilities like Non-disruptive upgrades (ISSU), stateful failover, Fast convergence (< 1s) shall be available.	
Non-FR#365	Infrastructure	server racks must conform to industry standards (e.g., 42U racks) and include redundant Power Distribution Units (PDUs), cable management arms, perforated doors, mounted wheels, exhaust fans, and lock-and-key mechanisms	

Non-FR#366	Infrastructure	Power Requirement Platinum-rated dual-redundant power supplies System ID, health, and predictive failure monitoring Real-time power & temperature monitoring with alerts Intelligent PDUs with telemetry & Indian standards compliance Compatibility with Data Centre UPS and full-load runtime estimation Rack power density up to 12 kVA Dual independent A/B power feeds Surge protectors & voltage regulation Modular scalability for power expansion Cooling Requirement Support for high-density compute/storage cooling Maintain required temperature/humidity ranges Provide thermal output (BTU/hr) and wattage per unit Direct-to-chip liquid cooling with certified components Chilled-water system compatibility 24×7×365 GPU thermal reliability N+1 cooling redundancy Backup cooling provision (CRAH/chilled-water redundancy) Hot-swappable fans, controllers, PSUs Environmental sensors for temperature, humidity, airflow Telemetry for temperature, airflow, water flow, leak detection Monitoring protocol support: SNMP, Modbus TCP, Redfish Leak detection, drip trays, condensation (dew-point) control Front-to-back airflow & optimized chassis Automated fan-speed control with sensors Compatibility with BMS/DCIM platforms Modular cooling design for future expansion	
------------	----------------	--	--

		Alignment with planned power/cooling infra CE, RoHS, BIS certification CRAC/AC delta-load impact in tons/kW	
Non-FR#367	Infrastructure	Connectivity and Expansion: • The SI must ensure that all hardware provisioned is sufficient to support the Bank's current and future requirements, including any additional infrastructure necessary for migration, testing, and operational continuity • Should the infrastructure fail to meet SLRs during the contract period, the SI shall deploy additional hardware, software, or other components at its own cost to meet the required performance levels and storage requirements	
Non-FR#368	Infrastructure	• Environment-wise sizing guidance: Data Centre (DC): 100% of production capacity Disaster Recovery Centre (DRC): 100% of production capacity User Acceptance Testing (UAT): minimum 30% of production capacity Development (Dev): minimum 10% of production capacity Sandbox: minimum 10% of production capacity	
Non-FR#369	Infrastructure	All Servers should be hardened as per security standards and VAPT complied before moving into Production. Also, complied with Bank's ongoing security standards and VAPT requirements	

Non-FR#370	Infrastructure	The servers must comply with industry standards such as ACPI 6.1, PCIe 5.0, Energy Star, and UEFI and include security features like: • Secure default passwords • Persistent event logging, including user activity • Secure alerting mechanisms • Automatic BIOS recovery • Rapid OS recovery • System erase functionality • Cryptographically signed firmware • System lockdown capabilities	
Non-FR#371	Operations & Maintenance	Uptime of Platform (including underlying Infrastructure, System, Software, Software tools, ingestion tool, processing, access, consumption capabilities) shall be $\geq 99.95\%$ (Monthly)	
Non-FR#372	Operations & Maintenance	Provide BCP for critical business continuity	
Non-FR#373	Operations & Maintenance	Archived data must remain available to all end users	
Non-FR#374	Operations & Maintenance	Archival process should be automated as per bank policy	
Non-FR#375	Operations & Maintenance	Reconciliation report to be provided to bank after each archival cycle	
Non-FR#376	Operations & Maintenance	Support standard configurable routines for data archiving or purging	
Non-FR#377	Operations & Maintenance	Hybrid, cost-effective, fast-recovery backups	
Non-FR#378	Operations & Maintenance	Users can query DB while backup runs	
Non-FR#379	Operations & Maintenance	Implement framework to monitor and handle hardware failures or corruption at the file system level	
Non-FR#380	Operations & Maintenance	Enable point-in-time recovery of files/directories from accidental deletions or corruption	
Non-FR#381	Operations & Maintenance	Restore data/services in case of a breach with minimal disruption	
Non-FR#382	Operations & Maintenance	Minimal/no manual intervention for DR	

Non-FR#383	Operations & Maintenance	Continuous sync of jobs, policies, and deployments	
Non-FR#384	Operations & Maintenance	RPO - Recovery Point Objective - Up to 10 mins RTO - Recovery Time Objective - Up to 120 mins	
Non-FR#385	Operations & Maintenance	Support mock DR as well as planned DR drill failover scenarios by bank	
Non-FR#386	Operations & Maintenance	Archive data older than bank-defined retention in low-cost cold storage	
Non-FR#387	Operations & Maintenance	Enable audit and error logs for auditing and troubleshooting	
Non-FR#388	Operations & Maintenance	Implement data replication from production setup to DR setup with the same configuration	
Non-FR#389	Operations & Maintenance	Provide complete visibility into the network with centralized management, dynamic load balancing, and multi-tenant support	
Non-FR#390	Operations & Maintenance	Monitor production and trigger DR	
Non-FR#391	Operations & Maintenance	Store historical data and support alarms and events for root cause analysis	
Non-FR#392	Operations & Maintenance	Collect telemetry data (e.g., server serial numbers, IP addresses, software installed) for proactive system reviews	
Non-FR#393	Operations & Maintenance	Provide a dashboard to monitor node health and system-level alarms (CPU, memory, etc.) across multiple locations	
Non-FR#394	Operations & Maintenance	Provide customizable dashboards for users, allowing flexibility in selecting widgets (e.g., health, utilization, etc.)	
Non-FR#395	Operations & Maintenance	Support profile-based deployment and management of multiple servers from a single console	
Non-FR#396	Operations & Maintenance	The solution should be certified for data Lakehouse deployment by the OEM, with published references for smooth deployment	
Non-FR#397	Operations & Maintenance	Warrant that all hardware, software, and associated components proposed shall be of the latest version and free from end-of-life (EOL) or end-of-support (EOS) status at the time of submission of the bid, throughout the	

		contract period and 2 years post completion of contract period; product replacement must be at no extra cost if declared EOL/EOS by OEM	
Non-FR#398	Operations & Maintenance	The infrastructure must be the latest, best-of-breed, and must meet the Bank's current and projected growth volumes throughout the contract.	
Non-FR#399	Operations & Maintenance	The solution must support secure communication over both IPv4 and IPv6 networks	
Non-FR#400	Operations & Maintenance	Propose solution in High-availability mode in both DC and DR, with no single point of failure	
Non-FR#401	Operations & Maintenance	supplied hardware with load balancers to ensure optimal performance	
Non-FR#402	Operations & Maintenance	Propose same CPU type, generation, family, and architecture for all servers	
Non-FR#403	Operations & Maintenance	The production and non-production environments must be physically separate	
Non-FR#404	Operations & Maintenance	GPU-supported clusters for ML and parallel processing	
Non-FR#405	Operations & Maintenance	Dedicated, isolated clusters for critical workloads	
Non-FR#406	Operations & Maintenance	Redundancy and performance-enhancing storage setup	
Non-FR#407	Operations & Maintenance	The SAN and network switches must be designed to accommodate redundancy, ensuring high availability and fault tolerance for critical operations	
Non-FR#408	Operations & Maintenance	Containerize applications and services in the lake house	
Non-FR#409	Operations & Maintenance	VM creation/management with workload isolation	
Non-FR#410	Operations & Maintenance	Integrate with Bank's Privileged Identity Management system and maintain the same.	
Non-FR#411	Operations & Maintenance	Monitor VM performance/resource consumption	
Non-FR#412	Operations & Maintenance	If virtualization is implemented, ensure no single point of failure	
Non-FR#413	Operations & Maintenance	Ensure components like Hard disk, PCI cards, Fans, and Power supply are hot swappable for no downtime/disruption	

Non-FR#414	Operations & Maintenance	Provide and implement racks and other required components for all environments	
Non-FR#415	Operations & Maintenance	Assess and propose required bandwidth for the entire contract duration, adhering to the Bank's SLRs	
Non-FR#416	Operations & Maintenance	Capability to perform system upgrades with minimum impact on Data Lake uptime	
Non-FR#417	Operations & Maintenance	Provide performance benchmarks for all components of the data solution	
Non-FR#418	Operations & Maintenance	Should accommodate growth in sources, systems, IOT, unstructured data, and use cases	
Non-FR#419	Operations & Maintenance	Solution must scale horizontally without downtime or major architecture changes	
Non-FR#420	Operations & Maintenance	Platform should support integration with future tools/technologies	
Non-FR#421	Operations & Maintenance	Must maintain performance with rising concurrent user activity	
Non-FR#422	Operations & Maintenance	Performance must not degrade due to increased data/system volumes	
Non-FR#423	Operations & Maintenance	Design should plan for increased storage (web/mobile ingestion, CDP analytics, etc.)	
Non-FR#424	Unit Testing Requirements	Develop and document unit test cases.	
		Prepare test data and execute unit test cases to validate individual components, including: AI models, Algorithms and Analytics modules	
Non-FR#425	System Integration Testing (SIT) Requirements	Design SIT strategy, test scenarios, and test cases for all integrated systems, including AI and analytics components.	
		Prepare SIT test data, execute test cases, log and resolve defects, and provide root cause analysis.	
		Ensure AI models, cognitive systems, and analytics workflows are fully functional and tested during SIT.	
		Provide SIT sign-off upon successful completion.	
Non-FR#426	Functional Validation Requirements	Validate that each application feature, including AI-driven functionalities, works as per defined requirements.	

		Ensure AI models produce accurate, reliable, and explainable results aligned with business objectives.	
Non-FR#427	User Acceptance Testing (UAT) Support Requirements	Support the Bank in preparing and executing acceptance testing, including: Defect logging, Resolution, Root cause analysis	
		Support UAT at the Bank's specified premises, including AI and analytics use cases.	
		Provide daily updates on UAT status to the Bank's IT Head or designated representative, including AI/analytics progress.	
		Assist the Bank in obtaining acceptance testing sign-off for AI, analytics, and reporting modules.	
		Ensure acceptance testing includes validation of: AI model performance, Accuracy, Compliance with ethical AI guidelines	
Non-FR#428	Regression & Re-testing Requirements	Re-run functional and non-functional tests to ensure that modifications or updates to: AI models, Analytics workflows, Reporting systems Do not impact overall functionality	
Non-FR#429	Performance Testing Requirements	Perform performance testing for: AI models, Analytics pipelines, Reporting systems before go-live and annually post-go-live.	
		Log and resolve performance issues and provide root cause analysis.	
		Share performance and stress test reports with the Bank ensuring: Model latency, Scalability, Throughput, meet agreed performance criteria.	
Non-FR#430	Quality Assurance & Compliance Requirements	Implement a QA framework to monitor and maintain data quality for AI and analytics use cases.	
		Conduct regular audits and reviews for compliance with: Data governance policies, Ethical AI standards, Regulatory requirements	
		Ensure rigorous testing of AI models, analytics workflows, and reporting systems for: security, privacy, compliance	

Non-FR#431	Test Environment & Tooling Requirements	Configure a test environment that reflects real-world scenarios, including AI and analytics use cases.	
		Generate anonymized test data suitable for AI model training and testing.	
		Provide and configure tools for: User interface testing, Functional testing, API testing, AI-specific testing (e.g., model validation, bias detection, explainability testing)	
Non-FR#432	CI/CD and Automation Requirements	Ensure automated unit, functional, and non-functional testing (e.g., performance, security) are integrated into the CI/CD pipeline.	
		Include execution reports as part of release artefacts, with a specific focus on AI and analytics components.	
Non-FR#433	Compliance with Data Protection Regulations	The solution, including its architecture, deployment, and maintenance, shall comply with the Data Protection Act and all other applicable statutory and regulatory frameworks.	
		Adherence to the Bank's internal Data Protection Policy is mandatory. Sensitive data, including Personally Identifiable Information (PII), must remain within the Bank's controlled environment (i.e., Data Centre (DC) and Disaster Recovery Centre (DRC)) at all times. Such data must not be transferred or exposed to any public or private cloud environment during any phase of its lifecycle.	
		The solution must comply with the Digital Personal Data Protection Act, 2023 and any future data protection regulations issued by competent authorities or regulators.	
Non-FR#434	Deployment of Data Protection Components	Encryption and hashing of sensitive information using industry-standard cryptographic algorithms such as AES, RSA, ECC, and SHA-2.	
		All cryptographic operations must comply with:	
		The Bank's internal Data Protection Guidelines.	

		Prevailing legal, regulatory, and statutory frameworks.	
Non-FR#435	Cryptographic Key Management	The proposed solution shall integrate seamlessly with the Bank's existing Key Management System (KMS) for:	
		Secure generation, storage, rotation, and usage of cryptographic keys involved in encryption, decryption, processes.	
		It must also leverage the Bank's existing Hardware Security Module (HSM) for secure storage and management of:	
		Cryptographic keys, digital certificates, passwords, and security tokens.	
		All cryptographic designs and mechanisms shall be subject to review and approval by the Bank's designated teams, including the Chief Information Security Officer (CISO).	
Non-FR#436	Data Protection Functionalities	The solution must provide comprehensive data protection mechanisms, including:	
		Encryption, tokenization, and masking of sensitive and PII data.	
		It should support Real-time and batch-mode processing of sensitive data via secure APIs or other mechanisms	
		Retrieval of tokenized data must be restricted to on-premises environments using secure APIs or authenticated access protocols.	
		The solution must also support Digital signing and signature verification for ensuring data authenticity and integrity.	
Non-FR#437	Historical Data Management	The system shall support secure retention of historical data in accordance with the Bank's archival policies.	
		It must incorporate a data purging and archiving mechanism for historical records, compliant with data lifecycle management standards.	
		The solution must offer encrypted backup and restoration capabilities to guarantee both data availability and	

		data security during disaster recovery or routine operational needs.	
Non-FR#438	Data Storage and Management	Data Availability - 99.9% (monthly) availability of data storage services	
Non-FR#439	Data Storage and Management	Adherence to Bank's data retention policy	
Non-FR#440	Query Performance	Simple Query-1 < 10s Simple Query-2 < 30s Moderate Query-1 < 48s Complex Query-1 < 2.5 mins Complex Query-2 < 10mins Complex Query-2 < 30 mins	
Non-FR#441	Data Access Vs Query performance	Ensure transparent data access across tiers without requiring application-level changes or impacting query performance.	
Non-FR#442	BI Dashboard Refresh	Target BI Refresh rate of less than 2 seconds for standard dashboards	
Non-FR#443	Reporting	Target Report Generation time of less than 5 seconds for Standard Reports	
Non-FR#444	Reporting	Target Report Generation time of less than 30 seconds for Complex Reports	
Non-FR#445	Reporting	Adhoc Reports (beyond period of 3 years) generation time could be maximum 24 hours	
Non-FR#446	Analytics	Target Model Training jobs (except GenAI) to be completed in less than 12 hrs	
Non-FR#447	Analytics	Target Model Inference in less than 100 milliseconds	
Non-FR#448	Backup Frequency	As per Bank's backup policy	
Non-FR#449	Backup Job Success Rate	99.95% success rate for all backup jobs (daily, weekly, fortnightly, monthly etc) measured and enforced monthly, for applicable penalty.	
Non-FR#450	Restore Job Success Rate	99.95% success rate for all restore jobs.	

Non-FR#451	Backup Retention Period	As per Bank's backup retention policy	
Non-FR#452	System Monitoring SLA	99.95% uptime for monitoring tools	
Non-FR#453	Alerting SLA	Alerts for critical issues triggered within less than 10s detection	
Non-FR#454	Testing & Quality Assurance	Develop and document unit test cases. Prepare test data and execute unit test cases to validate individual components, including: AI models, Algorithms, Analytics modules	
Non-FR#455	Testing & Quality Assurance	Design SIT strategy, test scenarios, and test cases for all integrated systems, including AI and analytics components.	
		Prepare SIT test data, execute test cases, log and resolve defects, and provide root cause analysis.	
		Ensure AI models, cognitive systems, and analytics workflows are fully functional and tested during SIT.	
		Provide SIT sign-off upon successful completion.	
Non-FR#456	Testing & Quality Assurance	Validate that each application feature, including AI-driven functionalities, works as per defined requirements.	
		Ensure AI models produce accurate, reliable, and explainable results aligned with business objectives.	
Non-FR#457	Testing & Quality Assurance	Support the Bank in preparing and executing acceptance testing, including: Defect logging, Resolution, Root cause analysis	
		Assign dedicated resources to support UAT at the Bank's specified premises, including AI and analytics use cases.	
		Provide daily updates on UAT status to the Bank's IT Head or designated representative, including AI/analytics progress.	
		Assist the Bank in obtaining acceptance testing sign-off for AI, analytics, and reporting modules.	
		Ensure acceptance testing includes validation of: AI model performance, Accuracy, Compliance with ethical AI guidelines	

Non-FR#458	Testing & Quality Assurance	Re-run functional and non-functional tests to ensure that modifications or updates to: AI models, Analytics workflows, or Reporting systems do not impact overall functionality	
Non-FR#459	Testing & Quality Assurance	Perform performance testing for: AI models, Analytics pipelines, Reporting systems before go-live and annually post go-live	
		Log and resolve performance issues and provide root cause analysis.	
		Share performance and stress test reports with the Bank ensuring they meet agreed performance criteria: Model latency, Scalability and throughput	
Non-FR#460	Testing & Quality Assurance	Implement a QA framework to monitor and maintain data quality for AI and analytics use cases.	
		Conduct regular audits and reviews for compliance with: Data governance policies, Ethical AI standards, Regulatory requirements	
		Ensure rigorous testing of AI models, analytics workflows, and reporting systems for: security, privacy, compliance	
Non-FR#461	Testing & Quality Assurance	Configure a test environment that reflects real-world scenarios, including AI and analytics use cases.	
		Generate anonymized test data suitable for AI model training and testing.	
		Provide and configure tools for: User interface testing, Functional testing, API testing, AI-specific testing (e.g., model validation, bias detection, explainability testing)	
Non-FR#462	Testing & Quality Assurance	Ensure automated unit, functional, and non-functional testing (e.g., performance, security) are integrated into the CI/CD pipeline.	
		Include execution reports as part of release artifacts, with a specific focus on AI and analytics components.	
Non-FR#463	Regulatory Compliance SLA	100% compliance with applicable regulations	

Non-FR#464	Audit SLA	Audit logs retained for a minimum of 1 year and accessible within 5 minutes of request	
	Audit SLA beyond period of 1 year	To be retained and made available within Maximum 24 hours	
Non-FR#465	Compliance with Data Protection Regulations	The solution, including its architecture, deployment, and maintenance, shall comply with the Data Protection Act and all other applicable statutory and regulatory frameworks.	
		Adherence to the Bank's internal Data Protection Policy is mandatory. Sensitive data, including Personally Identifiable Information (PII), must remain within the Bank's controlled environment (i.e., Data Center (DC) and Disaster Recovery Center (DRC)) at all times. Such data must not be transferred or exposed to any public or private cloud environment during any phase of its lifecycle.	
		The solution must comply with the Digital Personal Data Protection Act, 2023 and any future data protection regulations issued by competent authorities or regulators.	
Non-FR#466	Deployment of Data Protection Components	A dedicated data protection component/solution shall be deployed and hosted within the Bank's DC and DRC to execute all data protection-related functions.	
		This component shall handle Tokenization of any data transmitted to external/cloud services. Encryption and hashing of sensitive information using industry-standard cryptographic algorithms such as AES, RSA, ECC, and SHA-2.	
		All cryptographic operations must comply with Bank's internal Data Protection Guidelines Prevailing legal, regulatory, and statutory frameworks.	
Non-FR#467	Cryptographic Key Management	The proposed solution shall integrate seamlessly with the Bank's existing Key Management System (KMS) for: Secure generation, storage, rotation, and usage of cryptographic keys	

		involved in encryption, decryption, tokenization, and de-tokenization processes.	
		It must also leverage the Bank's existing Hardware Security Module (HSM) for secure storage and management of Cryptographic keys, digital certificates, passwords, and security tokens.	
		All cryptographic designs and mechanisms shall be subject to review and approval by the Bank's designated teams, including the Chief Information Security Officer (CISO).	
Non-FR#468	Data Protection Functionalities	The solution must provide comprehensive data protection mechanisms, including: Encryption, tokenization, and masking of sensitive and PII data for both on-premises and cloud-related scenarios.	
		It should support Real-time and batch-mode processing of sensitive data via secure APIs or other mechanisms.	
		Retrieval of tokenized data must be restricted to on-premises environments using secure APIs or authenticated access protocols.	
		The solution must also support Digital signing and signature verification for ensuring data authenticity and integrity.	
Non-FR#469	Historical Data Management	The system shall support secure retention of historical data in accordance with the Bank's archival policies.	
		It must incorporate a data purging and archiving mechanism for historical records, compliant with data lifecycle management standards.	
		The solution must offer encrypted backup and restoration capabilities to guarantee both data availability and data security during disaster recovery or routine operational needs.	
Non-FR#470	Regulatory Compliance	Adherence to the Regulatory compliance as mentioned in Section-6 #6.12 Regulatory Compliance	

Non-FR#471	Certifications	Attain the certifications as mentioned in Section-6 # 6.19 Certifications section	
Non-FR#472	Migration	New platform shall support existing operational requirements, applications, reporting, dashboard, analytics, and ML model execution	
Non-FR#473	Migration	Ensure that all data transformations and mappings are aligned with the new platform's data model and architecture	
Non-FR#474	Migration	Perform data reconciliation and generate reports to confirm the successful migration of all data	
Non-FR#475	Migration	Bank's critical existing Assets TM1, ADF, Planning & Analytics, Integration of CIMS, FIS ALM Data, Reporting Solution, ML models etc are compatible on proposed platform.	
Non-FR#476	Migration	Pre-migration end-to-end Testing, validation and Post Migration reconciliation mechanism is available	

Annexure 13: Bid Security (BG Format- for Earnest Money Deposit)

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

Dear Sir,

In response to your invitation to respond to your RFP for _____, M/s ____ having their registered office at _____ (hereinafter called the Bidder") wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

Whereas the „Bidder“ has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantee an amount of **Rs _____ (RupeesOnly)** as bid security as required to be submitted by the, Bidder“ as a condition for participation in the said process of RFQ.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

1. If the Bidder withdraws his proposal during the period of the proposal validity; or
2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently. We undertake to pay immediately on demand to Central Bank of India the said amount of Rupees ----- without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by Central Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein above:

1. Our liability under this Bank guarantee shall not exceed **Rs. _____ (RupeesOnly)**
2. This Bank guarantee will be valid up to _____; and
3. We are liable to pay the guarantee amount or any part thereof under this Bank Guarantee only upon service of a written claim or demand by you on or before _____ (date of expiry of BG plus claim period, if any)

In witness whereof the Bank, through the authorized officer has sets its hand and stamp on this ____ day of ____ at.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 14: Bidder's Particulars

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Tender No. GEM/2026/B/7203650

#	Particulars	
1.	Name of the Bidder	
2.	Address with E mail id, Mobile no. and Pincode	
3.	GST Number	
4.	Bank Details	
5.	PAN Number	
6.	Name of Authorised Person Mobile No: Landline No:	
7.	i. Email ID ii. Alternative Email ID	
8.	Details of Document cost / Tender fee	UTR/Reference No. date & Amount
9.	Details of EMD	BG/UTR/Reference No. date & Amount
10.	Exemption Certificate details (if applicable). Eg: MSME/Udyog Aadhar certificate etc.	Please upload copy of the same along with details

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"

(This letter should be on the letterhead of the bidder)

Date:-----

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking"
Tender No. GEM/2026/B/7203650.

Sir,

With reference to above, we <<<<Name of the Company>>>> hereby furnish and confirm the details as given below: -

1. Date of Agreement-
2. Expiry Date of Agreement
3. Type of Entity: Group Company/Not a group Company
4. Name of Directors of Company
5. Is any of the Director(s), Key Managerial Personnel and their relatives are stated above related to Central Bank of India: YES/NO

Note: - The terms 'control', 'director', 'key managerial personnel', and 'relative' have the same meaning as assigned under the Companies Act, 2013 and the Rules framed thereunder from time to time.

Authorized Signatory Name:

Designation:

Email and Phone

Annexure 16: NPA Undertaking

Performance letter to be given by all the bidders participating in RFP for Augmentation, Refresh of System Supporting Application at Bank on their official letterhead

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking" No. GEM/2026/B/7203650

Sir,

We _____(bidder name), hereby undertake that-

- We have not been declared NPA by any Bank in India.
- Further, we do not have any pending case with any organization across the globe which affects our credibility to service the Bank.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 17: Land Border Sharing Undertaking Letter

(This undertaking should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking" Tender No. GEM/2026/B/7203650

Dear Sir/Madam,

We, M/s_____ are a private/ public limited company/ LLP/ firm <strike off whichever is not applicable> incorporated under the provisions of the Companies Act, 1956/2013, Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having our registered office at _____ (referred to as the "Bidder") are desirous of participating in the Tender Process in response to our captioned RFP and in this connection we hereby declare, confirm and agree as follows:

We, the Bidder have read and understood the contents of the RFP and Office Memorandum & the Order (Public Procurement No.1) both bearing no.F.No.6/18/2019/PPD of 23rd July 2020 issued by Ministry of Finance, Government of India on insertion of Rule 144 (xi) in the General Financial Rules (GFRs) 2017 and the amendments & clarifications thereto, regarding restrictions on availing/ procurement of goods and services, of any Bidder from a country which shares a land border with India and/ or sub-contracting to contractors from such countries.

In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), we, the Bidder hereby declare and confirm that:

Strike off whichever is not applicable

1. "I/we have read the clause regarding restrictions on procurement from a bidder of the country which shares a land border with India; I/ we certify that _____ is not from such a country.
2. "I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that _____ is from such a country. I hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority is attached]"

Further, in case the work awarded to us, I/we undertake that I/we shall not subcontract any of assigned work under this engagement without the prior permission of Bank.

Further, we undertake that I/we have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that our subcontractor is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that our sub-contractor fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority]"

We, hereby confirm that we fulfil all the eligibility criteria as per the office memorandum/ order mentioned above and RFP and we are eligible to participate in the Tender process. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the contract, Bank shall be within its rights to forthwith terminate the contract/ bid without notice to us and initiate such action including legal action in accordance with law. Bank shall also be within its right to forfeit the security deposits/ earnest money provided by us and also recover from us the loss and damages sustained by the Bank on account of the above.

This declaration cum Undertaking is executed by us through our Authorized signatory/ ies after having read and understood the Office Memorandum and Order including the words defined in the said order.

Dated this _____ by _____ 20__

Yours faithfully,

Authorized Signatory

Name:

Designation:

Bidder's Corporate Name:

Address:

Email & Phone No.:

List of documents enclosed:

1. Copy of Certificate of valid registration with the Competent Authority (strike off if not applicable)
2. _____
3. _____
4. _____

Annexure 18: Cover Letter

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sub: Tender No. GEM/2026/B/7203650

Dear Sir/Madam,

1. Having examined the Scope Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, install and maintain 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 Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.
3. We agree to abide by this bid Offer for 180 days from date of bid (Commercial Bid) opening and our Offer shall remain binding on us which 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 certify that we have provided all the information requested by the Bank in the format prescribed 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.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

(Name: Contact Person, Phone No., Fax, E-mail)

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

Annexure 19: Escalation Matrix

Ref: Tender No - **GEM/2026/B/7203650**

Date: -

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Reg: RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking"

Escalation Matrix.

Name of the Company

Delivery Related Issues:

Sr .	Name	Designation	Full Office Address	Phone No.	Mobile	Email address
A		First Level Contact				
B		Second level Contact				
C		Third level Contact				
D		Country Head				

Service-Related Issues:

Sr .	Name	Designation	Full Office Address	Phone No.	Mobile	Email address
a		First Level Contact				
b		Second level Contact				
c		Third level Contact				
d		Country Head				

Any change in designation, substitution will be informed by us immediately.

(Signature of the Bidder with Seal)

Full name and Designation of authorized signatory

Date:

Phone No.:

E-mail:

Annexure 20: Query Format

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

Queries:

Sr. No.	Page #	Point / Section #	Query	Banks Response (Bidder Should not fill in this column)
1				
2				
3				
4				
5				
6				
7				
8				
9				

Date:

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)

Annexure 21: Guidelines on Banning of Business Dealing

Ref.: **Tender No. GEM/2026/B/7203650**

1.0 GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

1.0 There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with CENTRAL BANK OF INDIA shall apply for registration in the prescribed Application –Form.

1.1 Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by CENTRAL BANK OF INDIA.

1.2 Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order

2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA, IF ANY.

2.1 Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Bank, it shall be confirmed whether it is real substantial Bank and details of the same shall be furnished.

2.1.2 The amount of commission/remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3 Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by CENTRAL BANK OF INDIA in Indian Rupees only.

2.2 Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e. whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2 The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items .

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by CENTRAL BANK OF INDIA. Besides this there would be a penalty of banning business dealings with CENTRAL BANK OF INDIA or damage or payment of a named sum.

- 1) Introduction
- 2) Scope
- 3) Definitions
- 4) Initiation of banning / suspension
- 5) Suspension of business dealing
- 6) Ground on which banning of business dealings can be initiated
- 7) Banning of business dealings
- 8) Removal from list of approved agencies –suppliers/contractors
- 9) Show-cause notice
- 10) Appeal against the competent authority
- 11) Review of the decision by the competent authority
- 12) Circulation of names of agencies with whom business dealings have been banned

1. Introduction

1.1 Central Bank of India, being a Public Sector Enterprise and 'State', within the meaning of Article 12 of Constitution of India, has to ensure preservation of rights enshrined in Chapter III of the Constitution. CENTRAL BANK OF INDIA has also to safeguard its commercial interests. CENTRAL BANK OF INDIA deals with Agencies, who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of CENTRAL BANK OF INDIA to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure compliance with the constitutional mandate, it is incumbent on CENTRAL BANK OF INDIA to observe principles of natural justice before banning the business dealings with any Agency.

1.2 Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if tendered, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2. Scope

2.1 The General Conditions of Contract (GCC) of CENTRAL BANK OF INDIA generally provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2. Similarly, in case of sale of material there is a clause to deal with the Agencies / customers/ Buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Bank (CENTRAL BANK OF INDIA) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to all the Units and subsidiaries of CENTRAL BANK OF INDIA.

2.6 It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3.Definitions

In these Guidelines, unless the context otherwise requires:

- 1) 'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer' shall mean and include a public limited Bank or a private limited Bank, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor / Supplier / Purchaser / Customer/ Bidder / Tenderer' in the context of these guidelines is indicated as 'Agency'.
- 2) 'Inter-connected Agency' shall mean two or more companies having any of the following features:
 - i. If one is a subsidiary of the other;
 - ii. If the Director(s), Partner(s), Manager(s) or Representative(s) are common;
 - iii. If management is common;
 - iv. If one owns or controls the other in any manner.
- 3) 'Competent Authority' and 'Appellate Authority' shall mean the following:
 - i. For Bank (entire CENTRAL BANK OF INDIA) wide Banning Executive Director (BSD) shall be the "Competent Authority" for the purpose of these guidelines. Chairman & Managing Director, CENTRAL BANK OF INDIA shall be the "Appellate Authority" in respect of such cases except banning of business dealings with Foreign Suppliers of imported coal/coke.
 - ii. For banning of business dealings with Foreign Suppliers of imported goods, CENTRAL BANK OF INDIA Executive Directors" Committee (EDC) shall be the

- "Competent Authority". The Appeal against the Order passed by EDC, shall lie with Chairman & Managing Director, as First Appellate Authority.
- iii. In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach CENTRAL BANK OF INDIA Board as Second Appellate Authority.
 - iv. For Zonal Offices Only: Any officer not below the rank of Deputy General Manager appointed or nominated by the Head of Zonal Office shall be the "Competent Authority" for the purpose of these guidelines. The Head of the concerned Zonal Office shall be the "Appellate Authority" in all such cases.
 - v. For Corporate Office only: For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of BSD shall be the "Competent Authority" and concerned Executive Director (BSD) shall be the "Appellate Authority".
 - vi. Chairman & Managing Director, CENTRAL BANK OF INDIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.
- 4) 'Investigating Department' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.
 - 5) 'List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Unit /Corporate Vigilance may also be competent to advise such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with CENTRAL BANK OF INDIA is under investigation by any department (except Foreign Suppliers of imported goods), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all Departmental Heads within the Plants / Units. During the period of suspension, no business dealing may be held with the Agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (BSD), CENTRAL BANK OF INDIA Corporate Office along with the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

5.5 For suspension of business dealings with Foreign Suppliers of imported goods, following shall be the procedure:-

- i) Suspension of the foreign suppliers shall apply throughout the Bank including Subsidiaries.
- ii) Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors Committee (EDC) with ED (BSD) as Convener of the Committee. The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.
- iii) If EDC opines that it is a fit case for suspension, EDC may pass necessary orders which shall be communicated to the foreign supplier by ED, BSD.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrant;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or CENTRAL BANK OF INDIA, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc.;

6.4 If the Agency continuously refuses to return / refund the dues of CENTRAL BANK OF INDIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and / or fudging /forging /tampering of documents;

6.8 If the Agency uses intimidation / threatening or brings undue outside pressure on the Bank (CENTRAL BANK OF INDIA) or its official in acceptance / performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Bank (CENTRAL BANK OF INDIA) or not;

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Bank

(CENTRAL BANK OF INDIA) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Bank (CENTRAL BANK OF INDIA), forcefully occupies, tampers or damages the Bank's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent

Authority may decide to ban business dealing for any good and sufficient reason).

7 Banning of Business Dealings

7.1 A decision to ban business dealings with any Agency should apply throughout the Bank including Subsidiaries.

7.2 There will be a Standing Committee in each Zone to be appointed by Head of Zonal Office for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers of goods. However, for procurement of items / award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager / Dy. General Manager each from Operations, Law & BSD. Member from BSD shall be the convener of the committee. The functions of the committee shall, inter-alia include:

- 1) To study the report of the Investigating Agency and decide if a prima-facie case for Bank- wide / Local unit wise banning exists, if not, send back the case to the Competent Authority.
- 2) To recommend for issue of show-cause notice to the Agency by the concerned department.
- 3) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.
- 4) To submit final recommendation to the Competent Authority for banning or otherwise.

7.3 If Bank wide banning is contemplated by the banning Committee of any Zone, the proposal should be sent by the committee to ED (BSD) through the Head of the Zonal Office setting out the facts of the case and the justification of the action proposed along with all the relevant papers and documents. BSD shall get feedback about that agency from all other Zones and based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority. At this stage if it is felt by the Competent Authority that there is no sufficient ground for Bank wide banning, then the case shall be sent back to the Head of Zonal Office for further action at the Zone level. If the prima-facie decision for Bank-wide banning has been taken, ED (BSD) shall issue a show-cause notice to the agency conveying why it should not be banned throughout CENTRAL BANK OF INDIA.

After considering the reply of the Agency and other circumstances and facts of the case, ED (BSD) will submit the case to the Competent Authority to take a final decision for Bank-wide banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported goods.

- 1) Banning of the agencies shall apply throughout the Bank including Subsidiaries.
- 2) Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director,

BSD to place it before Executive Directors' Committee (EDC) with ED (BSD) as Convener of the Committee.

- 3) The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.
- 4) If EDC opines that it is a fit case for initiating banning action, it will direct ED (BSD) to issue show-cause notice to the agency for replying within a reasonable period.
- 5) On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED (BSD) to EDC for consideration & decision.
- 6) The decision of the EDC shall be communicated to the agency by ED (BSD).

8 Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from Competing in Open Tender Enquiries, but Limited Tender Enquiry (LTE) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9 Show Cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defense.

9.2 If the Agency requests for inspection of any relevant document in possession of CENTRAL BANK OF INDIA, necessary facility for inspection of documents may be provided.

9.3 The Competent Authority may consider and pass an appropriate speaking order:

- i. For exonerating the Agency if the charges are not established;
- ii. For removing the Agency from the list of approved Suppliers / Contractors, etc.
- iii. For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10 Appeal against the Decision of the Competent Authority

10.1 The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11 Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee/EDC as the case may be for examination and recommendation.

12 Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency has been banned by the Central or State Government or any other Public Sector Enterprise, CENTRAL BANK OF INDIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter-connected Agencies.

12.4 Based on the above, Zonal Offices may formulate their own procedure for implementation of the Guidelines and same be made a part of the tender documents.

Annexure 22: Undertaking of Information Security from Bidder

Ref: **Tender No. GEM/2026/B/7203650**

Date: -

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Reg:- RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking"

We hereby undertake that the proposed product 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 software being delivered as well as any subsequent versions/modifications done) which may lead to any data leakage/compromise of the server/solution or any cyber security incident in future.

We also undertake that :-

- 1) The product offered, as part of the contract, does not contain Embedded Malicious Code that would activate procedures to:
 - i) Inhibit the desires and designed function of the equipment.
 - ii) Cause physical damage to the user or equipment during the exploitation.
 - iii) Tap information resident or transient in the equipment/network
- 2) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software and any loss occurring due to the above may be recovered from the existing contracts.
- 3) To ensure that the setup / link provided for updation / downloading / authorisation of licenses either on Banks network or through Internet should be

free of any malware / viruses etc. Any damages / losses caused to Bank due to aforesaid shall be passed on to the bidder account.

Also, undertake that the proposed solution / software to be supplied will be complying to Bank's Information Security Policy (of the version of the application being delivered as well as any subsequent versions/modifications done). And new Information Security requirement will be compiled within the timeline set by Bank / Regulatory agencies.

Yours faithfully,

(Signature of the Bidder with Seal)

Full name and Designation of authorized signatory

Date:

Phone No.:

E-mail:

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory on Information security as per regulatory requirement)

Annexure 23: Software Bill of Material (SBOM) Format

Ref.: Tender No. GEM/2026/B/7203650

SBOM FORMAT								
S N	Applic ation Name	Softw are Pack ages	Type of Software (App/Web/D B/Middlewa re)	Installed Version/ Installed Date	Late st Vers ion	License Type (Perpet ual/ Subscri ption)	No. of Licenses /AMC validity	OEM/ AMC Vendo r
1								
2								
3								
4								

The bidder must submit only such document as assurance regarding the accuracy, completeness and timelines of SBOM.

Yours faithfully,

(Signature of the Bidder with Seal)
Full name and Designation of authorized signatory
Date:

Annexure 24: Template for Third Party Due Diligence Questionnaire

Ref.: Tender No. GEM/2026/B/7203650

Third Party Name					
Third Party Location					
Service Description					
S.N	Domain	Sub-domain	Control question	Response	Comments (If any)
				(To be filled by Third Party)	
1	Governance	Strategy & Operating Model	Do you have a dedicated information / cyber security team, responsible for information security governance across the organization?		
2	Governance	Policies, Standards & Architecture	Do you have information / cyber security policy?		
3	Governance	Policies, Standards & Architecture	Are all your policies and procedures reviewed periodically?		
4	Governance	Cyber Risk Culture & Behaviour	Do you perform periodic risk assessments? If Yes, please define the frequency		
5	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment ISO 27001: 2013 certified for the scope of the service being offered to Central Bank of India? If Yes, please provide the latest copy of the certification and specify the scope of implementation.		
6	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment SOC 2 Type II attested or certified for the scope of the service being offered to Central Bank of India?		
7	Governance	Cyber Risk Management, Metrics & Reporting	Is your environment PCI - DSS certified for the scope of the service being offered to Central Bank of India?		
8	Governance	Cyber Risk Management, Metrics & Reporting	Are appropriate procedures & controls implemented to ensure compliance with the usage of proprietary software products?		
9	Resilient	Incident & Crisis Readiness	Do you have a formal document for incident management?		
10	Resilient	Incident & Crisis Readiness	Is awareness training given to your employees to identify information security events?		

11	Resilient	Incident & Crisis Readiness	Do you have a formal cyber crisis management plan?		
12	Resilient	Incident Response	a. Have you ever experienced a cybersecurity incident or data breach in last 3 years? This includes network, systems, software, etc. b. Will you notify Central Bank of India about any security, privacy incident, and event of disaster affecting Central bank of India services within 2 hrs. of incident being identified? c. Are the root cause analysis is performed for the security incidents.		
13	Resilient	Incident Response	Please provide details if you have ever been subject to any enforcement actions, investigations or litigation related to privacy or information security?		
14	Resilient	BCP / DR	Do you have a Business Continuity / Disaster Recovery Plan in place at an organization level?		
15	Resilient	BCP / DR	Have you identified the events that could cause interruptions to business process?		
16	Resilient	BCP / DR	Do you have a failover site? Please describe if that is Hot, Warm or Cold site.		
17	Resilient	BCP / DR	Is there sufficient redundant capacity to ensure services are not impacted in multi-tenant environments during peak usage?		
18	Resilient	BCP / DR	If You store Central Bank of India data - is backed up data tested on a regular basis? - is data backup encrypted?		
19	Information Security	Penetration Testing & Vulnerability Scanning	Do you periodically perform External IS Audit/ VAPA		
20	Information Security	Security Event Monitoring	1. Do you have mechanism to preserve Audit trail logs?		
21	Information Security	Network Security	Have you implemented Advance cyber security controls/ tools (eg. WAF, DDoS, Firewall , SIEM etc)		
22	Information Security	Customer Data Protection	Do you have the technical capabilities to identify & segregate Central Bank of India's data [including Bank's customer data] from other entities data and maintain confidentiality & integrity? Please describe and share the evidence.		

23	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	Has the third-party or has any of the third-party's owners directors/ shareholders/employees been the subject of any allegations, investigation, conviction and/or other relevant criminal practices relating to bribery or corruption in the last three years?		
24	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	Has the third-party complied with all applicable provisions of HR-related Acts, including, but not limited to Contract Labour (Regulation & Abolition) Act, Minimum Wages Act, Payment of Wages Act, Maternity Benefits Act, Payment of Gratuity Act, Equal Remuneration Act, Employee's Compensation Act, etc.?		
25	Ethics, Regulatory & Compliance	Ethics, Regulatory & Compliance	In the last three years has the third-party received any local/governmental citations or fines relating to labour issues?		
26	Data Privacy	Monitoring & Enforcement	Do you have Adequate data privacy and security controls in place to protect data integrity and confidentiality.		
27	Data Privacy	Monitoring & Enforcement	Do you have and regular data privacy training and awareness module for your employees?		
28	Operational	HR/Personnel Security	Do you perform a background screening or check prior to allowing constituent access to systems and data ?		
29	Operational	Operation Management	Does the third-party have a defined process for tracking and ensuring compliance to SLAs / KPIs agreed with Central Bank of India?		
30	Operational	Operation Management	Are there adequate controls in place to monitor the activities undertaken through sub-contracting, including tracking of errors, etc.?		
31	Operational	Supply Chain Risk Management	Do you have documented & approved Organization level outsourcing risk management policy/framework to govern your third parties you are dependent upon?		
32	Operational	Supply Chain Risk Management	i. Have you obtained the prior consent from Central Bank of India for subcontracting complete or partial activities to third party[ies]		

33	Operational	Supply Chain Risk Management	Does your Agreement /Contract with your third parties who will be involved in provisioning/rendering services to Central Bank of India include a. Information/Data security/Regulatory requirements and applicable data security standards, privacy laws & data localization requirements b. Confidentiality c. Business Continuity d. Right to audit & seek information from the service provider.		
34	Strategic and Geographical	Country risk assessment	Do the third party provides service from India.		
35	Strategic and Geographical	Adverse Media	Has there been any adverse media published against the third party in past 2 years (relating to Financial Reporting, AML, Human Rights, Environmental Laws, Others etc.)). If Yes, please describe		
36	Financial Risk	Revenue Trend	Does the third party have a positive Net Worth/ Revenue Trend for last 3 financial years?		
37	Regulatory and Supervisory requirements		whether the service provider is located in India or abroad, the Service provide shall ensure that the outsourcing should neither impede nor interfere with the ability of the Bank to effectively oversee and manage the outsourcing activities. Further, the Service provide shall ensure that the outsourcing does not impede the RBI/ Auditor in carrying out its supervisory functions and objectives.		
38	Physical security	Physical & Environmental Security	a. Does vendor have physical and environmental security measures in place like CCTV, Fire extinguisher, fire alarm, Smoke detector, biometric, UPS, AC, etc. b. Is there regular fire drills performed?		

I /We hereby certified that the above information/data provided is correct and true. Bank can call for Evidence/ Documentary proof/ data in support of the above information for Audit / internal purpose anytime and the same will be provided and submitted to Bank as and when required

Authorised Signatory

Name & Designation of Authorised Signatory

Subject: Tender No. GEM/2026/B/7203650

Sl. No	Particulars	Details
1	Name of the Bidder	
2	Address with E mail id, Mobile no. and Pin code	
3	GST Number	
4	Bank Details	
5	PAN Number	
6	Name of Authorized Person	
	Mobile No:	
	Landline No:	
7	i. Email ID	
	ii. Alternative Email ID	
8	Details of Document cost / Tender fee	UTR/Reference No. date & Amount
9	Details of EMD	BG/UTR/Reference No. date & Amount
10	Exemption Certificate details (if applicable). E.g.: MSME/Udyog Aadhar certificate etc.	Please upload copy of the same along with details

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 25: List of Hardware and Software Components:

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

The below software is proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below licenses (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr No.	Software / Tool or Component Required	OEM Name	Justification (Why Software is needed)	Licensing Metric for software (Customer based/ Processor Based/ any other)

The below Hardware items are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below items (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr No.	Hardware Item or Component Required	Quantity	OEM Name	Size of Hardware for provisioning Racks space	Number of Power Inputs and Power consumption for device

Yours faithfully,

Signature of Authorized Signatory:

Date:

Name of Signatory:

Place:

Designation:

Seal of Company:

Annexure 26: Letter for Refund of EMD

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

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

We (Company Name) had participated in the Request for Proposal (RFP) bearing reference no. **Tender No. GEM/2026/B/7203650** for RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking". and we are an unsuccessful bidder.

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

Sr. No.	Bidder Name	DD/BG Number	Drawn on Bank Name	Amount (₹)

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

Name of the Bank with Branch:

Account Type:

Account Title:

Account Number:

IFSC Code:

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 27: Format for Submission of Client References by Bidder

To,

**Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Subject: Tender No. GEM/2026/B/7203650

Bidder to fill the below details of the Projects implemented by them within last 5 years as on date of submission of the Bid i.e. The start date of the referenced Project must be no earlier than five (5) years from the Bid Submission Date

SL No	Name of the Client	PO dated	Project Implementation Period	Work Completion date	On-prem / Cloud / Hybrid	Work Domains *	Word details**	Contact Person	Designation	Alternative Contact	Mail ID	Contact number	Remarks

*Lakehouse Platform Implementation / Platform Setup for Analytics/ Data Transformation/ Migration/ FM/ Use case etc

**Delivery/ Installation/ Implementation/ Designing/ Development/ Maintenance / use case development/ maintenance etc

The documentary proof of the client reference is enclosed.

Yours faithfully,

Signature of Authorized Signatory: Name of Signatory: Designation: Seal of Company:	Date: Place:
--	-------------------------------

Annexure 28: Undertaking for Data Privacy

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory on Data Privacy requirement)

To,

**Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Subject: Tender No. GEM/2026/B/7203650

We hereby undertake to comply with the regulations of Digital Personal Data Protection Bill (DPDPA 2023) and any future amendment/addition to the Bill in future as part of the engagement during entire period of contract.

Further, we ensure that the Data privacy, security and confidentiality of the Bank shall not be compromised.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 29: Undertaking for 7 Years Roadmap

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

To,

Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

We, _____ hereby confirm that as a bidder and the product provider, would Design, Supply, Install, Manage and Maintenance of Data and Gen AI Platform and solution. We also commit to support the proposed Data and Gen AI Platform and solution for a minimum period of 5 years and further period of another 2 years if extended.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 30: Format for Local Content

(This certificate for local content should be on the letterhead of the bidder as well as the OEM/ Manufacturer duly signed by an authorized signatory)

CERTIFICATION FOR LOCAL CONTENT

To,

**Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Subject: Tender No. GEM/2026/B/7203650

Bidder Name:

This is to certify that the RFP bearing reference no. Tender No. GEM/2026/B/7203650 for RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking" is having the local content of ____% as defined in the above-mentioned RFP and amendment thereto.

This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 – Revision vide Order No. P-45021/2/2017-PP (BE-II) dated 04th June 2020.

Yours faithfully,

Signature of Statutory Auditor/Cost Auditor

Registration Number:

Seal:

Countersigned by the bidder:

Bidder – (Authorized Signatory)

Date:

Place:

Annexure 31: Proposed Team Profile

To,
Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Subject: Tender No. GEM/2026/B/7203650

Sl N O.	Name of the Role (Product Owner/ Solution Architect etc)	Name of the Resour ce	Experie nce in Years	Education Qualificat ion (Btech/ Mtech etc)	Certificati ons	Experti se / Skill set	Remark s/ Comme nts

We hereby acknowledge that the information provided by us is true and to the Best of our Knowledge

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place

Annexure 32: Volumetrics

Existing Source Systems

S.No.	Data Source	Description	Data Type	Current Data Ingestion	Ingestion Frequency	Daily Incremental Volume (in GB)	Total Volume (in TB)
1	CBS	Core Banking Solution	Database	CDC	Daily	253.0	148.2
2	INTERNET BANKING	Internet Banking Database	Database	ETL	Daily	14.5	9.9
3	UPI	UPI transaction database	Flat File	ETL	Daily	12.7	8.4
4	MOBILE BANKING	Mobile Banking Database	Database	ETL	Daily	8.0	7.0
5	HRMS	HRMS Database	Database	ETL	Daily	8.6	5.3
6	TREASURY	Database for Treasury operation of bank	Database/ Flat File	ETL	Daily	5.9	4.4
7	TRADE FINANCE	Database for Trade Finance products	Database/ Flat File	ETL	Daily	5.7	4.4
8	ASBA	IPO Database	Database	ETL	Daily	4.1	3.3
9	GL	Used for financial statement preparation	Database/Flat File	ETL	Daily	3.3	2.2
10	ATM SWITCH	Switch Data for Central bank and other banks customers transactions	Database	ETL	Daily	1.5	2.2
11	INTERNAL PORTAL	Database of Inhouse developed portals	Database	ETL	Daily	0.2	1.3
12	PENSION	Pension database	Database	ETL	Monthly	1.5	1.3
13	CALL CENTER	Database of Call center of our bank like inbound, outbound calls etc	Flat File	ETL	Discontinued	1.5	1.2
14	LLMS	Loan Management System		ETL	Daily	0.0	0.0

Potential Source Systems (Internal)

S.No.	Source Systems (Potential)	Description	Data Type	Ingestion Frequency	Daily Incremental (In GB)	Total Volume (In TB)
1	Omni Channel Platform	Replace existing Internet Banking and Mobile Banking	Database/File	Daily	70.00	2.23
2	Digital Lending Platform(DLP)	Replace existing LLMS	Database/File	Daily	2.00	0.08
3	Integrated Customer Care(ICC)	Replace existing CALL center	Database/File	Daily		
3.a	Audio			Daily	4.33	1.95
3.b	Database			Daily	0.05	0.06
4	Wealth Management	Wealth Management Database	Database/File	Daily		0.00
5	Martech	Marketing Platform Database	Database/File	Daily	Not yet live	0.00
6	Collections	SMA customers allocation and disposition Database	Database/File	Daily		
6.a	Audio			Daily	3	1.32
6.b	RDBMS			Daily	1.5	0.90
7	Video KYC, Digital KYC & Electronic KYC	Database of Customer on boarded through Video KYC, Digital KYC & Electronic KYC	Database/File	Daily		
7.a	Video		External	Daily	15.00	3.70
7.b	Database		External	Daily	0.07	0.45
8	Payment Hub	Payment Hub used by our bank Database	Database/File	Daily		0.00
9	POS solution	Point of Sale customer Database	Database/File	Daily		0.00
10	Fastag	Fastag customers database	Database/File	Daily		0.00

11	EFRMS	Electronic Fraud management System Database	Database/File	Daily		0.00
12	Financial Inclusion Application	Database of Bank's Business Correspondent (BC) transactions	Database/File	Daily	13.33	4.10
13	e TDS	Electronic TDS Database	Database/File	Daily		0.00
14	CDSL	Source system for Bank's DEMAT accounts	Database/File	Daily		0.00
15	Cent Digipay	Bank issued QR Code customers transaction database	Database/File	Daily		0.00

Potential Source Systems (External) but not limited to:

S.No.	Data Source	Description
1	Central and State Government Portals	Government portals at the central and state levels provide access to leads and data related to agribusiness and rural banking
2	CFR	Central Fraud Registry: RBI's portal.
3	Jeevan Praman Portal	Jeevan Pramaan is a biometric-enabled digital service for pensioners. Pensioners of the Central Government, State Government, or any other Government organization can benefit from this facility.
4	RAM	CRISIL RAM is part of the package.
5	NPS/NSDL portal	NPS Accounts Details
6	CRILC for Fraud /Red flag account	Central Repository of Information on Large Credits for fraud-related transactions.
7	Capitaline	Market data and financial information are available on securities, derivatives, and commodities traded on Indian stock markets.

S.No.	Data Source	Description
8	CDSL/NSDL	National Securities Depositories Ltd (NSDL) and Central Securities Depositories Ltd (CDSL) are depositories that hold your financial securities, such as shares and bonds, in dematerialized form and facilitate trading on stock exchanges.
9	Central and State Government Portals	Government portals at the central and state levels provide access to leads and data related to agribusiness and rural banking.
10	CGTMSE Portal	Credit Guarantee Fund Trust for Micro and Small Enterprises (CGTMSE) provides access to MSME-related information.
11	Credit bureau data	Data from credit bureau
12	CARE	CARE subscription/website for credit ratings
13	CRISIL/ SAVERISK	SAVERISK is a data aggregator that helps measure risk against your counterparty by providing detailed risk assessment services.
14	External Commercial Borrowing (ECB)	Commercial loans raised by eligible resident entities solely for commercial purposes from recognized non-resident entities
15	EDPMS	Export Data Processing and Monitoring System (EDPMS)
16	Bloomberg	Bloomberg is an application used by the treasury team and client-facing teams for tracking market movements, receiving alerts, and facilitating chats.
17	Files stored in FTP	Miscellaneous files, such as creative files, videos, audio, and other materials related to corporate communication.
18	Goldmine	An external vendor is engaged for managing social media activities and engagement.
19	Google Analytics and Ads related data	Google Analytics provides insights into website usage, traffic, and other related metrics.
20	Indian Readership Survey	The Indian Readership Survey is an ongoing research study on readership patterns.
21	IDPMS	The Import Data Processing and Monitoring System (IDPMS) is a system designed to process and monitor import-related data.
22	Integra	AEPS transactions are managed here. This includes financial inclusion, business correspondents' data, performance management, and transaction tracking. Monitoring of transactions below ₹2 lakh is performed by CMCC.
23	Internal Records	The information stored includes the Minutes Preparation Checklist, Government Notifications received via email, Feedback Reports from Directors, Performance Evaluations of Directors,

S.No.	Data Source	Description
		Nominations of Directors to Committees of the Board, and details of Directors' Sitting Fees.
24	CIBIL	Credit bureau data
25	CRIF	Credit bureau data
26	KVIC Portal	The Khadi and Village Industries Commission (KVIC) portal serves as a platform for MSME industries to access resources, schemes, and information related to the promotion and development of khadi and village industries.
27	CICs	Credit rating information centers, similar to CIBIL, provide credit-related data and ratings to assess the creditworthiness of individuals and businesses.
28	Manual Payments and TDS Data	Local files containing payment and tax-related data are stored.
29	NABARD Ensure Portal	Subsidies are released through the government portal. The government shares leads, and subsidy claims are processed further for the benefit of farmers.
30	National Portal	National Credit Guarantee Trustee Company
31	NCGTC Website	National Credit Guarantee Trustee Company
32	NCLT	National Company Law Tribunal
33	Cogenecis	Leading data, news and market intelligence provider to financial market professionals
34	TReDS	The three platform files—M1 Exchange, TReDS, and InvoiceMart—are part of a scheme designed to establish and operate an institutional mechanism for facilitating the financing of trade receivables for MSMEs. This mechanism enables MSMEs to receive payments from corporate entities, government departments, and public sector undertakings (PSUs) through multiple financiers.
35	Udyami Mitra portal	A credit delivery platform enabling ease of access to MSMEs financial and non- financial service needs
36	CORDEX	Collects data related to frauds and security risk.
37	VISA, NPCI, and MasterCard networks.	Data files containing information around card-based transactions from providers such as VISA, Mastercard, etc.
38	Corpository	A web-based platform for corporate information provides details such as information about directors, financials, auditors, credit ratings, and more.

S.No.	Data Source	Description
39	CRILIC	For exposures exceeding INR 5 crore, the information is reported to the RBI. Data from eight verticals is consolidated and submitted to the RBI in a predefined format, consisting of approximately 120 fields.
40	CRISIL	Credit Rating Information Services of India Limited CRISIL models are used by the bank, vendor-based module
41	External Credit Rating Agencies (ECRAs).	Various websites and applications, including CRISIL, are accessed to obtain credit-related information, credit scores, and other relevant details for clients.
42	Informist	Real-time financial wire agencies, such as NewsWire18 and CRISIL MarketWire, provide up-to-date financial news and market-related information.
43	Macro-indicators	An external data source containing information related to macroeconomic indicators.
44	RBI	Various pieces of information are obtained from the RBI website.
45	NeSL Portal	The portal is designed to compare borrower information with data from previous months. Borrower information is uploaded onto the portal and can be downloaded at a later date for comparison purposes.

Projected Volumetric

	Current State	Growth	Target State
Technology State	Integrated hardware and software solution (DB2 as database) IIAS 1.18.0 Ingestion using IBM Infosphere® Change Data Capture/ IBM Infosphere® Data Replication for Core Banking System BI Tool - Cognos, Tableau		To be proposed by the SI
Source Systems	14		Up to 40
Storage	1.2 PB	*_Expected Data Growth over the 5 years contract period is given in subsequent Table	Expected Data size by end of 5th year would be: 4 PB (Raw-Source Data size) in DC Production. Out of this Bank expects Data of minimum 3 years would be there in Hot Tier for Reporting purpose. For Analytics Inferencing Bank would require 5 years of Data in Hot Tier for approx. 150 Use cases. Hot Tier Storage & Compute to be sized based on SLA adherence, Solution requirement. (Additional considerations for UAT, Dev, Sandbox, Analytics & Models, Backup, Archival, Tiered Storage Layer, Compute, etc will have to be provisioned by the SI). SI to meet the solution requirements and SLA.

	Current State	Growth	Target State
			Same Sizing to be considered for DR Production excluding UAT, Dev and Sandbox. At later point, if Bank wants to increase the storage, then provision should be there to increase the storage without increasing the compute.
Data Growth	~ 350 GB/daily ~ 500 GB/daily during month end		
Data Retention Requirements	10 Years		10 Years
Data Volume at various temperatures - Hot, Cold, Archive % split	None		To be estimated by the SI based on the following: a. Industry best practices for data tiering. b. Experience in implementing and managing a Data Lakehouse and next-generation AI platform for similarly sized Indian banking clients.
Count of Work loads	5000 jobs+ 750 On demand + 400 Regulatory		All the jobs, reports to be optimized and migrated to the new Data platform. However, Regulatory reports to be migrated as per Bank's requirement.
Average Execution Time of Jobs	End to end Data Pipeline - 10 minutes to up to 5 hrs.		As per the Non-Functional Requirement
Frequency of Jobs	On-demand, Scheduled (Daily, Monthly, Quarterly, Half yearly and yearly)		On-demand, Scheduled (Daily, Monthly, Quarterly, Half yearly and yearly)
Count of Source Systems where CDC is used	1 (Core Banking System - BANCS@24)		Core Banking System - BANCS@24. Rest to be estimated / determined by the SI
Compute of Source Systems where CDC is used	CBS - 96 Physical Cores i.e. 768 vCores in a 3node cluster Processor Type is Oracle M8		CBS - 96 Physical Cores i.e. 768 vCores in 3node cluster Processor Type is Oracle M8

	Current State	Growth	Target State
			Omni Channel – IBM Linux One S390x IFL 4 in 2 node cluster UPI – 2 Node cluster Per Node - 64 core with 2 sockets i.e.128 core Processor Type - Intel Xeon Gen 5 Platinum
Count of named end users, accessing the BI Solution			~ 550 Users Super Admin - 05 Developer Users – 50 Viewer - 495
Count of Reports (excel based) - Scheduled, Ad-Hoc etc	500		~ 1000
Count of BI Dashboards in 6 years	85		150
Count of named Application users:	# Planning & Analytics (CPM/TM1) - Total users 191 # Daily users access DB for multiple activities - 90 # ADF Iris Application - 20+ Users # ETL - 45+ Users		

***Expected Data Growth over the 5 years contract period**

	Y1	Y2	Y3	Y4	Y5	Total Size in GB	Total Size in PB
Incremental daily in GB	350	525	788	1181	1772		
Structured Data	126000	189000	283500	425250	637875	1661625	1.66
Incremental daily in GB	105	158	236	354	532		

Un-structured Data	37800	56700	85050	127575	191363	498488	0.50
Existing Data size Day zero onwzrds							1.70
<u>Total Structured + Un-structured + Existing Data</u>							~ 4.00

Expected Data size by end of 5th year would be:

4 PB (Raw-Source Data size) in DC Production.

Out of this Bank expects Data of minimum 3 years would be there in Hot Tier for Reporting purpose. For Analytics Inferencing Bank would require 5 years of Data in Hot Tier for approx. 150 Use cases.

Hot Tier Storage & Compute to be sized based on SLA adherence, Solution requirement.

(Additional considerations for UAT, Dev, Sandbox, Analytics & Models, Backup, Archival, Tiered Storage Layer, Compute, etc will have to be provisioned by the SI). SI to meet the solution requirements and SLA.

We expect the SI to provide a full detailed calculation (in the Technical Bid) for the Storage, Compute etc. which they propose for the Data Lakehouse for a period of 5 years.

Same Sizing to be considered for DR Production excluding UAT, Dev and Sandbox.

At later point, if Bank wants to increase the storage, then provision should be there to increase the storage without increasing the compute.

Annexure 33: Declaration of Source Code Audit

(To be submitted by Bidders on their letter head)

To,

**Deputy General Manager -IT (Digital)
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Subject: Tender No. GEM/2026/B/7203650

Dear Sir,

We declare that source code of our application has been audited by professionally competent personnel/ Information Security (IS) Auditors.

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

Yours faithfully,

Authorized Signatory

Seal of the company

Name: Designation:

Bidder's Corporate Name

Address

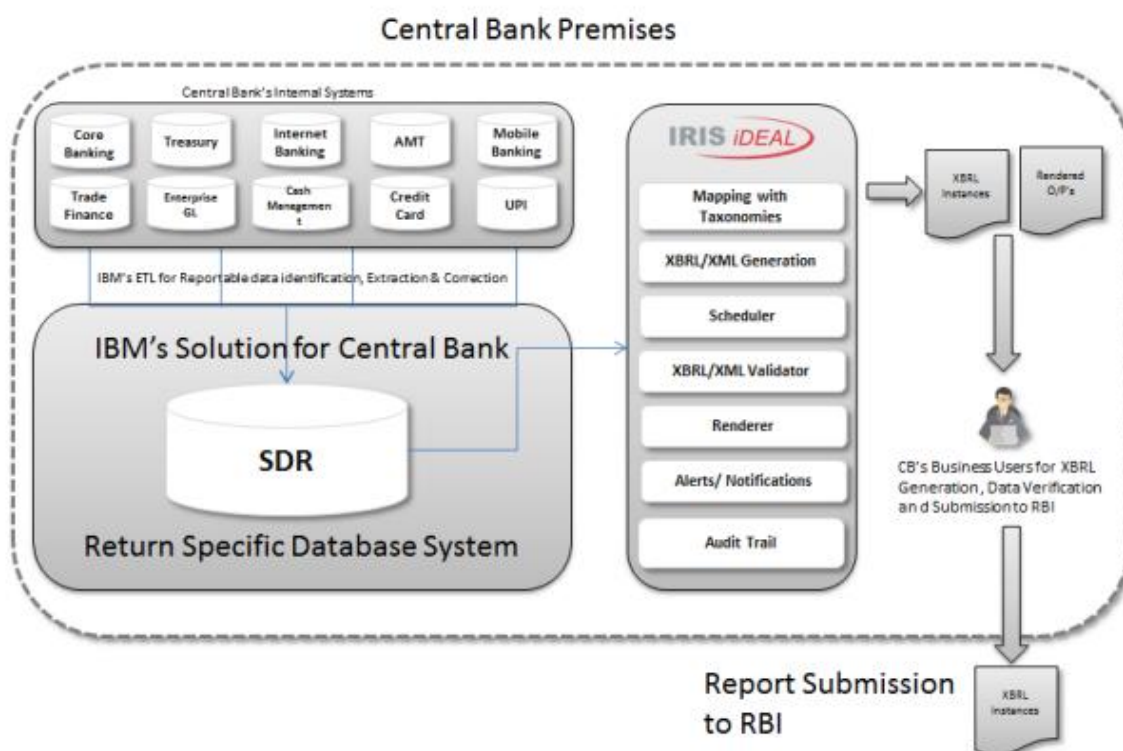
Email and Phone

Date:

Annexure 34: Existing Application Details

34.1 ADF Application

CENTRAL BANK OF INDIA generates automatic statutory ADF Reports in the format required by RBI. This IRIS's iDEAL Solution, a bridge between the bank's SDR and RBI reporting requirements in XBRL and SDMX formats, it can also significantly reduce the time and effort required by Bank to automate and submit reportable data in required format to RBI. IRIS iDEAL solution is available to handle complete XBRL and SDMX reporting to RBI for banks. The consolidated and reportable data from bank's multiple data sources will be ingested into the SDR. This data will be consumed by the IRIS iDEAL Solution to generate the XBRL instance documents and SDMX formats.

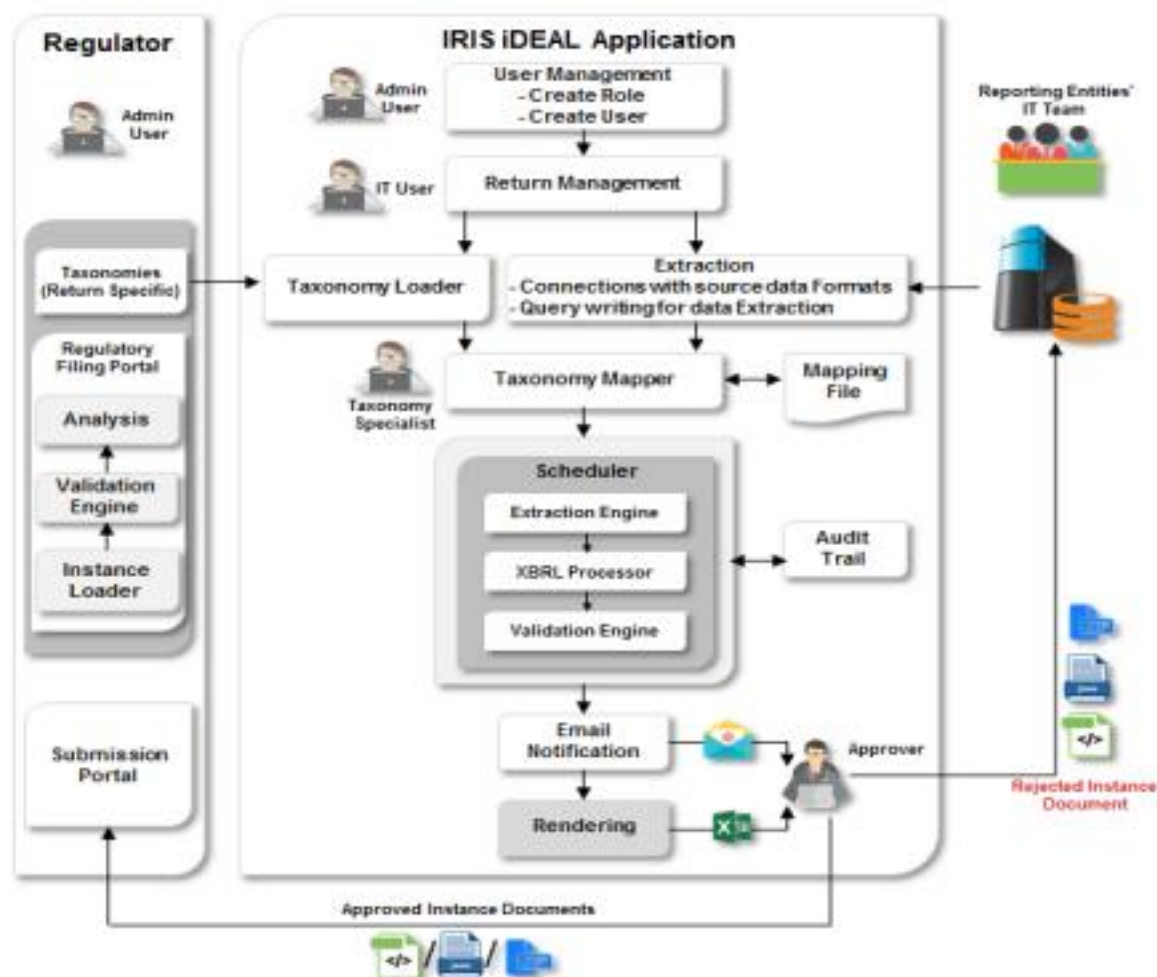


Some of the key benefits that IRIS iDEAL offers are:

- Can consume data directly from the pre-defined database/ Excel®/ xml files
- Generates XBRL instance, SDMX and rendering output directly from application
- Can automate XBRL and SDMX instance generation process
- Eliminates all the worries of customizing the internal bank applications

- Ensures ultimate reliability and accuracy of the data in XBRL & SDMX formats
- Help banks in meeting the strict RBI deadlines for filing data into XBRL & SDMX format
- Can be enhanced to incorporate any future changes in taxonomy, Schema and RBI rules The complete solution is packaged into following main components:
- Taxonomy Mapper
- XBRL & SDMX processor
- Scheduler
- Validator
- Renderer
- Audit Trail
- User Management
- Log Viewer

IRIS iDEAL Solution Work Flow



Taxonomy Mapper:

The application enables user to upload new taxonomy in 'Regulatory Returns' module and in this module enable users to map the source data elements (data

sets extracted from input sources via extraction module) with the taxonomy elements.

This iDEAL Solution demands only a one-time mapping to be defined as a part of the application configuration. Henceforth, the data can be directly extracted and generated using the previous mappings.

XBRL & SDMX Processor:

iDEAL processor reads input data and converts it into XBRL instance or SDMX format. The generated XBRL/ SDMX instance will comply with XBRL 2.1 specification and all RBI guidelines both in presentation and validation pertaining to XBRL and SDMX.

Scheduler and Notifications: Allows users to schedule and automate XBRL/ SDMX generation process based on the reporting frequency. Notification engine notifies associated users about the status of the scheduled activity.

Validator:

Validator module of this application validates the XBRL instance document or SDMX reports generated from the processor with predefined XBRL 2.1 specification and RBI specific business rules.

Renderer:

Renderer is a process of converting generated XBRL instance document/ SDMX files into human readable formats. This can also be downloaded in html or Excel® formats.

Audit Trail:

Applications audit trail allows admin users to track the operations of business users who have access to the iDEAL® Solution for various functionalities. It tracks all the changes made in different modules of the application. Admin user will be able to monitor all the user activities and reports can be generated on the same.

Authorized users can verify the data converted XBRL/ SDMX formats and can provide approval through this module.

User Management:

iDEAL® user management feature allows administrators to assign granular roles and permissions to users, thus strictly controlling/ managing access to different modules of the application such as Log viewer, Mapping, Taxonomy and Returns

34.2 Financial Planning & Budgeting Application

Overview of budgeting exercise in Bank

Financial Planning & Budgeting process of Central Bank of India. And Bank is responsible for –

- (a) Conducting planning & budgeting exercise and setting up performance targets for various business units within the Bank.
- (b) Track budget vs actuals performance, report shortfalls

Annual budgeting exercise is initiated in January every year to set business targets and budgets for the next financial year. Bank considers inputs from various macro-economic factors, SCB performance as well as historical trends to arrive at the business forecast and targets followed by P&L estimates.

Once the budget is finalized at Central Office level, the numbers are allocated to the lower administrative layers i.e. zones, regions and branches. Bank considers branch specific parameters as well as industry trends to assess potential of the branch while allocating the CO budget.

Bank uploads the branch budget allocation in the existing planning & budgeting solution developed in IBM Planning Analytics. Regional users review and make updates to the branch wise numbers. Bank budget is finalized once the updated numbers are approved at different administrative hierarchy levels i.e. Region, Zone and Central Office with the help of workflow.

Finalized budget is then tracked against actual data. Daily actual data is sourced from GL balances.

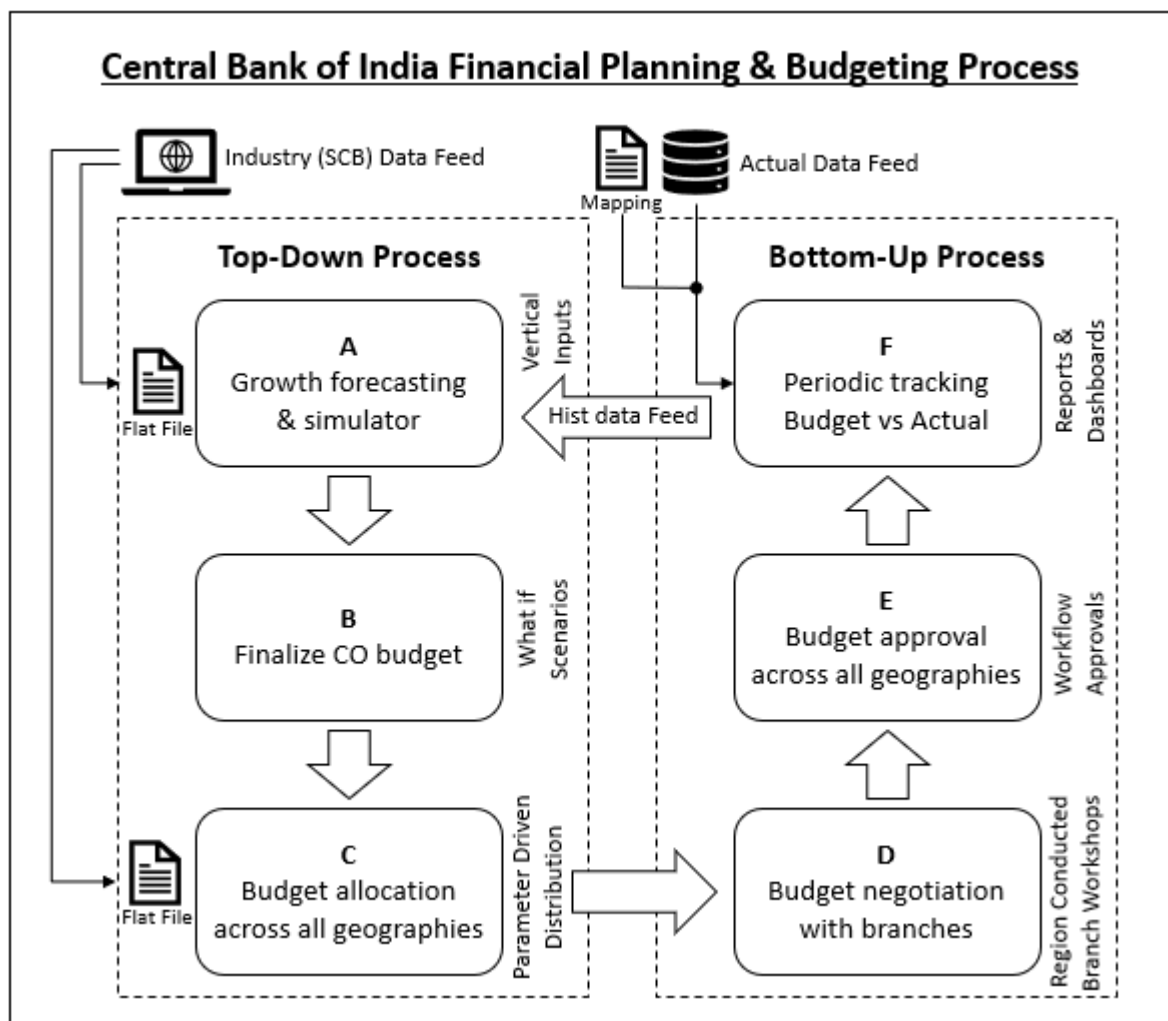
Scope of Applicability

Following key stages have been identified to requirements of the proposed solution.

- A. Growth forecasting and simulator
- B. Finalize CO budget
- C. Budget allocation across all geographies (up-to branch level)
- D. Budget settlement with branches
- E. Budget approval across all geographies
- F. Periodic tracking – budget vs actual

Overall budgeting process is a hybrid approach that combines top down as well as bottom-up approach of forecasting. At present bank is carrying out activities as a part of stage A, B and C with significant manual intervention. Stage D, E and F are broadly part of earlier planning & budgeting solution.

Industry data i.e. Schedule Commercial Banks (SCB) data need to be considered at two stages. Firstly, at "Stage A. Growth forecasting and simulator" as a reference while deciding budget year target. Secondly at "Stage C. Budget allocation across all geographies" to understand district wise branch potential while distributing the targets decided at Central Office level.



User friendly web interface for budget planning and forecasting

- End to end automation in budget planning and forecasting, target setting and tracking for 400+ business KPIs
- Scientific process inclusion by using SCB data (district potential) and Bank 2 years growth comparison & projection
- Business user input facility for budget target & adjustment
- Self-Service capabilities for Reports/Dashboard & trends, Ratio Simulation
- Used by CO/ZOs/ROs for budget preparation, forecasting, tracking and daily reporting
- 400+ Business KPIs figure daily data with last 2 years and current fiscal data availability
- Periodic Tracking Daily, Monthly, quarterly at any time and extensive 10+ reports
- Gap Between Actual vs Budgeted (reports/dashboard)
- Reduction of Manpower involved in Manual Budget preparation/tracking

Budget Scenarios & Adjustments

Bank intends what-if analysis for below financial ratios.

- NIM (%)
- ROA
- Yield on Advances (%)
- Cost of Deposits (%)
- Cost to Income Ratio
- Provision Coverage Ratio
- Credit Deposit Ratio
- Other income to Total income
- Yield on Funds
- Cost of Funds
- Credit Cost
- Slippage Ratio

Expectations from Ratio what-if analysis is as below to make decisions about the budget and targets of underlying components

- a) Observe the impact on underlying components i.e. numerator or denominator by entering desired value of the Ratio
- b) Observe the impact on other ratios by changing one of the ratios at a time which may impact common components of other ratios.
- c) Once the desired results are achieved, Business user will transfer the outcomes i.e. derived underlying components to the CO Budget sheet as a projection for business KPIs

Periodic Tracking – budget vs actual

Primary focus of the reports in the solution is to track plan and budget. The KPIs are considered where budget or targets are being set by the Business department.

KPIs will be divided based on update frequency i.e. Daily, Monthly and Quarterly.

1. Monthly Performance Monthly RO-ZO
2. Monthly Performance Population size-wise
3. Quarterly Performance
4. Daily Business Figures
5. Daily Variation (without account)
6. Actual-Budget-Gap-YTD & YoY Growth - Zone-wise Monthly Report
7. Actual-Budget-Gap-YTD & YoY Growth - KPI-wise Monthly Report
8. Cumulative Up-gradation, Cash Recovery, TWO & Terminal NPA as on (month-end)

Data Refresh Frequency

1. Actual Data

Actual data for KPIs will be updated at a daily, monthly or quarterly frequency subject to availability of data in the identified source systems.

2. Budget Data

- a) Budget data is prepared as a part of annual budgeting exercise.
- b) There will a provision to make updates to the budget during the year as desired by the department.
- c) The Budget is expected to be available for Year, Quarter and Month levels.

Annexure 35: Self-Declaration Regarding Non-Suspension by GeM in the Last Six Months

Date

To,

General Manager IT
Central Bank of India
DIT, CBD Belapur

Ref: Tender No. GEM/2026/B/7203650

Dated:

Dear Sir/Madam,

In response to the [Insert Tender/Request for Proposal Name and Number], I/We, the undersigned, hereby declare the following:

1. I/We, M/s _____, having our registered office at [Insert Address], confirm that we have not been suspended by the Government e-Marketplace (GeM) platform for any reason whatsoever in the last six (6) months prior to the date of submission of this bid.
2. I/We further affirm that this declaration is made after conducting necessary due diligence to ensure its accuracy and completeness.
3. I/We understand and accept that any false declaration or misrepresentation in this regard may result in immediate disqualification from the bidding process, termination of the contract (if awarded), and any other actions deemed appropriate by Central Bank of India.

Thank you for your consideration.

Yours faithfully,

[Authorized				Signatory]
[Name	of	the	Authorized	Signatory]
[Designation]				
[Contact				Details]
[Seal/Stamp of the Bidding Entity]				

Annexure 36: Declaration / undertaking from bidder to comply with the Information and cyber security controls

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

To,

General Manager IT
Central Bank of India
DIT, CBD Belapur

Re: : RFP for RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking" Tender No. GEM/2026/B/7203650.

Sir,

Further to our proposal dated _____, in response to the Request for Proposal _____ (Bank's tender No. hereinafter referred to as "RFP") issued by Central Bank of India ("Bank") we hereby covenant, warrant and confirm as follows:
We hereby agree to comply with the Information and cyber security controls as per Bank's and Regulatory Authorities IT Security Guidelines on an ongoing basis and regulatory / legal guidelines and directives related to SP / outsourcing issued by regulators / legal entities from time to time. The SP shall provide access to the regulators, legal authorities, Bank and Bank appointed auditors for on-site/off-site supervision.

We ensure that outsourced critical IT services are subjected to the annual IT audit / Technology risk assessment process by an independent professional agency as approved by the local government or regulator at no extra cost to the Bank.
We abide with all clauses of Bank's Cyber Security Controls which will be part of the NDA/SLA signed with the Bank at the time of award of contract.

Dated this _____ by _____ 20____ Yours faithfully,

Authorized Signatory

Name: _____

Designation: _____

OEM's Corporate Name: _____

Address: _____

Email ID: _____

Phone Number: _____

Annexure 37: Information/Cyber-Security Measures/Controls for selected Service Provider

To,

General Manager IT
Central Bank of India
DIT, CBD Belapur

Re: : RFP for Design, Supply, Implementation & Maintenance of Data Lakehouse and AI/ Gen AI Platform for "Data Transformation and AI Banking" Tender No. GEM/2026/B/7203650.

1. Incident Response and Management

Service Provider must have a mechanism/resources to take appropriate action in case of any cybersecurity incident. They must have written incident response procedures including the roles of staff/outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and coordination with stakeholders, including specifically the bank, during response. Service provider shall report all cyber incidents to the Bank immediately upon detection (if applicable).

Service Provider's BCP/DR capabilities shall adequately and effectively support the Service Provider's cyber resilience objectives and should be so designed to enable the Service Provider to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

Service Provider is responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers. Service Provider shall have necessary arrangements, including a documented procedure for such purpose. This shall include, among other things, informing the bank about any cybersecurity incident occurring in respect of the bank within 30 minutes of detection to early mitigate the risk as well as to meet extant regulatory requirements.

2. IT Risk Management

The Service Provider shall assist the Bank in adhering to compliance guidelines of the regulatory authorities and facilitate Bank from time to time. The Service Provider shall conform to the security practices and procedures laid down in the Information Technology Act 2000 as amended by the information Technology (Amendment) Act 2008 (IT Act and IT Amendment Act) and the information Technology (Reasonable

Security Practices and Procedures and Sensitive Personal Data or information) Rules 2011 (Privacy Rules).

The Service Provider shall carry out Information security / cyber security risk assessment and apply risk treatment measures on regular intervals. The Service Provider shall put in appropriate cyber security measures in place and comply with the legal and regulatory guidelines and directives.

The SP shall be subjected to the annual IT audit / Technology risk assessment process by an independent professional agency as approved by the local government or regulator.

Dated this _____ by _____ 20____ Yours faithfully,

Authorized Signatory

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

*****End of Document*****