



Central Bank of India

Data Protection Cell, Risk Management Department

Request for Proposal (Bid) Document

For

Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025

Bid Number: GEM/2026/B/ 7977310

31/08/2026

Signature of the Bidder with company Seal

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	21
Section-2	22
Scope of Work	23
6 Scope of Work for the BIDDER	24
A. Gap Assessment, Solution Architecture and Implementation Planning:	24
B. Infrastructure and Hardware Supply & Configuration	25
C. Data Privacy and Consent Management Solution	25
D. Implementation of Proposed Solution	25
E. Support Services and Maintenance	26
F. Training and Knowledge Transfer	26
6.1 Project initiation and planning:	33
6.2 Requirements, Design Configuration and Setup:	34
6.3 Functional Scope for Study the Bank System, Prepare PII Data Inventory, GAP Assessment, Prepare a Roadmap / Approach / Implementation Plan and Implement the solution, Policy Review , Framework Design ,Integration and Implementation:	34
6.4. Technical & Functional Scope for Data Privacy and Consent Management Solution and Other privacy Applications/Platforms	51
6.4.1 Consent Management Solution	51
6.4.1.1 Granular Consent Management	51
6.4.1.2 Consent Lifecycle Management & Auditability	52
6.4.1.3 Notice & Transparency Mechanisms	53
6.4.1.4 Version Control	53
6.4.1.5 Integration & Centralized Consent Management	53
6.4.2 Cookies Consent Management	54
6.4.2.1 Cookie Scanning and Categorization	54
6.4.2.2 Cookie Banner	54
6.4.3 Record of Processing Activities (ROPA)	54
6.4.4 Data Discovery, Inventory and Classification and Data flow Mapping	55
6.4.4.1 Data Catalogue	55
6.4.4.2 Data Lineage	55
6.4.4.3 Data Discovery & Classification	56
Signature of the Bidder with company Seal	

6.4.4.4 Endpoint discovery	57
6.4.4.5 Data Inventory & Tagging	57
6.4.4.6 Secure Deployment	58
6.4.4.7 Integration between Data Discovery and Consent Management	58
6.4.4.8 Data Privacy/Security Posture Management.....	58
6.4.4.9 Data Flow Mapping	59
6.4.5 Data Privacy Assessment of Applications	59
6.4.5.1 Core Privacy Assessment Features	59
6.4.5.2 Operational & Strategic Features	60
6.4.6 Data Principal Rights Management/Facilitation	60
6.4.6.1 Rights Management & Request Handling.....	60
6.4.6.2 Workflow Automation & Compliance Adherence.....	61
6.4.6.3 Integration & Multi-Level Workflow Capabilities	61
6.4.6.4 Tracking, Reporting & Auditability	61
6.4.7 Data Protection Impact Assessment (DPIA).....	61
6.4.7.1 Comprehensive DPIA Templates & Workflows.....	61
6.4.8 Privacy Notice Management	62
6.4.8.1 Notice & Transparency Mechanisms	62
6.4.8.2 Version Control.....	63
6.4.8.3 Audit & Reporting	63
6.4.9 Data and Privacy Breach Management	63
6.4.10 Compliance Monitoring, Reporting and Governance Dashboard	64
6.4.11 Third Party Risk Management	64
6.4.12 Integration of System	65
6.4.13 Security and Compliance	65
6.4.14 Privacy by Design	65
6.4.15 Testing and Validation:	66
6.4.16 Reporting and Metrics:.....	66
6.4.17 Security Requirements:	66
6.4.18 Compliance and Governance	66
6.4.18.1 Operational & Strategic Features	66
6.4.19 Implementation Deliverables:	67
6.5. Project Requirements	67
6.6. Onsite Resource Deployment and Governance.....	68
6.7. Additional Scope of Work	71

6.8	Hardware Scope & Sizing for the Platform Infrastructure.....	75
6.8.1	Compliance and Documentation.....	79
6.8.2	Infrastructure Sizing and Design	79
6.8.3	Leverage Bank's existing resources	79
6.8.4	Licensing and Software Requirements	82
6.8.5	High Availability and Disaster Recovery.....	82
6.8.6	Security and Network Requirements.....	82
6.8.7	Performance and Scalability	82
6.8.8	Implementation and Support	83
6.8.9	Additional Requirements	83
6.8.10	Compliance with Future Regulatory and Statutory Requirements	83
6.8.10.1	Regulatory Adaptability & Support	83
6.8.10.2	Timely Updates	83
6.8.10.3	No Additional Cost	84
6.8.10.4	Documentation and Support.....	84
6.8.10.5	Failure to Comply	84
7	Required Artefacts	84
7.1	Platform Architecture.....	84
7.2	Infrastructure Sizing.....	84
7.3	Implementation Approach	84
7.4	Commercials	84
7.5	Team and Resources	84
8.	Project Timelines	85
9.	Maintenance Support	87
Section-3		88
Terms & Conditions.....		89
10.Liquidated Damage.....		90
11.Land Border Sharing Clause.....		91
12.Monitoring & Audit		92
13.Bid Submission		92
14.Integrity Pact.....		94
15.Technical and Commercial Offers.....		94
15.1 Evaluation & Acceptance.....		95
16. Evaluation Process		96
16.1 Stage 1 - Eligibility Criteria		96

16.2 Stage 2 -Technical Evaluation	96
16.3 Stage 3– Commercial Evaluation Criteria.....	96
16.4 Normalization of Bids.....	97
16.5 FINAL EVALUATION – WEIGHTED TECHNO-COMMERCIAL EVALUATION	98
17 General Terms.....	100
17.1 Important Terms & Conditions:	100
17.2 Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)	101
18 Payment Terms	101
19 Service Level Agreement.....	107
20 Reporting of Material Adverse Events and Incident Management.....	117
21 Insurance.....	118
22 Order Cancellation.....	118
23 Indemnity	119
24 Confidentiality & Non-Disclosure.....	122
25 Force Majeure.....	123
26 Resolution of Disputes.....	123
27 Format of the Letter of undertaking of Authenticity to be submitted by the Bidder.	124
28 Sub-Contractor/ Independent Contractor	125
29 Assignment	125
30 Execution of Contract, SLA & NDA	125
31 Bidder’s Liability.....	126
32 Information Ownership.....	126
33 Inspection, Audit, Review, Monitoring & Visitations	126
34 Monitoring	127
35 Visitations	128
36 Information Security	128
37 Intellectual Property Rights	128
38 Enterprise License:	131
39 Termination.....	132
39.1 Termination for Default	132
39.2 Termination for Insolvency.....	133
39.3 Termination- Key Terms & Conditions	133
39.4 Right to Transfer IT Outsourcing Arrangements	134
39.5 Exit Option & Contract Re-Negotiation.....	134
40 Privacy & Security Safeguards	134

Signature of the Bidder with company Seal

41 Governing Law and Jurisdiction.....	135
42 Compliance	135
42.1 Adherence to IT/Cyber Security Policy	139
42.2 Compliance with Laws.....	139
43 Violation of Terms.....	140
44 Corrupt & Fraudulent Practices	140
45 Publicity	140
46 Entire Agreement; Amendments.....	140
47 Survival and Severability.....	140
48 Bidding Document.....	141
48.1 Amendments to Bidding Documents	141
48.2 Period of Validity.....	141
48.3 Last Date and Time for Submission of Bids	141
48.4 Late Bids	141
48.5 Modifications and/or Withdrawal of Bids.....	141
48.6 Clarification of Bids.....	141
49 Signing of Contract.....	142
50 Sustainable Sourcing.....	142
51 Remote Access.....	142
52 Business Continuity and Disaster Recovery	142
52.1 Business Continuity Plan (BCP)	142
52.2 Disaster Recovery Plan (DRP).....	142
53 Obligation to Co-operate with relevant authorities in case of Insolvency/Resolution.....	143
53.1 Insolvency	143
53.2 Cooperation.....	143
53.3 Continued Service During Resolution.....	143
53.4 Notification	143
54 Data Localization.....	143
55 Authorized Signatory	143
56 Escrow Arrangements.....	144
Section-4	145
Annexures	146
Checklist for Submission	147
Annexure 1: Conformity Letter.....	149
Annexure 2: Masked Commercial Bid.....	150

Annexure 3: Bidder's Information.....	160
Annexure 4: Letter for Conformity of Product as per RFP.....	161
Annexure 5: GOI Guidelines with Model wise classification (Make in India)	162
Annexure 6: Undertaking of Authenticity for Products Supplied.....	165
Annexure 7: Undertaking for Acceptance of Terms of RFP.....	166
Annexure 8: Manufacturer's Authorization Form	167
Annexure 9: Integrity Pact	168
Annexure 10: Non-Disclosure Agreement.....	173
Annexure 11: Performance Bank Guarantee	178
Annexure 12: Technical Evaluation Sheet.....	181
Annexure 13: Bid Security (BG Format- for Earnest Money Deposit)	188
Annexure 14: Bidder's Particulars	190
Annexure 15: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"	191
Annexure 16: NPA UNDERTAKING	192
Annexure 17: Land Border Sharing Undertaking Letter.....	193
Annexure 18: Cover Letter	195
Annexure 19: Escalation Matrix	196
Annexure 20: Query Format	197
Annexure 21: Guidelines on Banning of Business Dealing	198
Annexure 22: Undertaking of Information Security from Bidder	207
Annexure 23: [Software, Hardware, Cryptographic Bill of Material Format].....	209
Annexure 24- Template for Third Party Due Diligence Questionnaire	216
Annexure 25: Bidder's Particulars on Company Letter Head:	220
Annexure 26: List of Hardware and Software Components:	221
Annexure 27: Letter for Refund of EMD.....	225
Annexure 29: Undertaking for Data Privacy:	228
Annexure 30: Undertaking for 5 Years Roadmap:	229
Annexure 31: Format for Local Content:.....	230
Annexure 32: Proposed Team Profile:	231
Annexure 33: Volumetrics	232
Annexure 34 Declaration of Source Code Audit	233
Annexure 35: Technical/functional Specifications	234
Annexure 36 Format for Credential Letter (For Bidder)	253
Annexure 37 Format for Credential Letter (For OEM)	254
Annexure 38 Undertaking for Infrastructure Sizing and Capacity Planning	255
Signature of the Bidder with company Seal	

List of Abbreviations

AD	Active Directory
AIBOM	Artificial Intelligence Bill of Material
AMC	Annual Maintenance Contract`
API	Application Programming Interface
APM	Application Performance Management
ATS	Annual Technical Support
Bank	Central Bank of India
BCMS	Business Continuity Management System
BCP	Business Continuity Process
BFSI	Banking, Financial Services, and Insurance.
BOM	Bill of Material
BYOK	Bring Your Own Key
CA	Chartered Accountant
CBOM	Cryptographic Bill of Materials
CMK	Customer Managed Key
CMPT	Consent Management and Privacy Tool
CPRA	California Privacy Rights Act.
CRM	Customer Relationship Management
DB	Database
DC	Data Centre
DC/DR	Data Centre / Disaster Recovery
DPBI	Data Protection Board of India
DPDPA	Digital Personal Data Protection Act 2023
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRC/ DRS	Disaster Recovery Centre/ Site
DSCI	Data Security Council of India
EMD	Earnest Money Deposit
EMS	Enterprise Management System/Solution
EOL	End-of-Life
EOS	End-of-Support
EPP	End Point Protection
ERP	Enterprise Resource Planning
FY	Financial Year
GSI	Global System Integrator
GST	Goods & Service Tax
GSTIN	Goods and Services Tax Identification Number
HBOM	Hardware Bill of Materials

Signature of the Bidder with company Seal

HLD	High Level Design Document
HTML, CSS	Hyper Text Markup Language / Cascading Style Sheets
IAPP	International Association of Privacy Professionals
IBA	Indian Bankers Association
IRDAI	Insurance Regulatory & Development Authority of India
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
IT	Information Technology
IT/BCP policy	Information Technology / Business Continuity Planning Policy
ITAM	IT Asset Management
JSON/XML	JavaScript Object Notation / Extensible Markup Language
KPIs	Key Performance Indicators
LLD	Low Level Design Document
LLP	Limited Liability Partnership
MAF	Manufacturer Authorization Form
MEITY	Ministry of Electronics and Information Technology, GOI
MSEs	Micro & Small Enterprises
MSME	Micro, Small & Medium Enterprise
NEFT	National Electronic Funds Transfer
NEGD	National e-Governance Division
NS	Near Site
OEM	Original Equipment Manufacturer
ORA	Online Reverse Auction
PAN	Permanent Account Number
PbD	Privacy by Design
PBG	Performance Bank Guarantee
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PO	Purchase Order
PoC	Proof of Concept
PSB	Public Sector Bank
PSE	Public Sector Enterprise
PSU	Public Sector Undertaking
PwD	Persons with Disability
RBAC	Role-Based Access Control
RBI	Reserve Bank of India
ReST APIs	Representational State Transfer Application Programming Interfaces
RFP	Request for Proposal
RTGS	Real Time Gross Settlement

Signature of the Bidder with company Seal

SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAS	Serial attached SCSI
SBOM	Software Bill of Materials
SDR	Single Data Repository
SI	System Integrator
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Centre
SPI	Sensitive Personal Information
SPOC	Single Point of Contact
SSD	Solid State Drive
TCO	Total Cost of Ownership
UAM	Udyog Aadhaar Memorandum
UAT	User Acceptance Testing
UCIC	Unique Customer Identification Code
UIDAI	Unique Identification Authority of India
VA	Vulnerability Assessment
VAPT	Vulnerability Assessment and Penetration Testing
WCAG	Web Content Accessibility Guidelines

Section-1

Signature of the Bidder with company Seal

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 4585 plus Branches, 13 Zonal Offices, 90 Regional Offices spread across the Country as on 31.03.2026. 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 for **Implementation of Data Privacy & Consent Management Solution /Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025.**

Bank through this Request for Proposal (RFP) is interested in identifying a Bidder/Solution Provider/System Integrator **for Implementation of Data Privacy & Consent Management Solution /Tool as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025.**

The Bank proposes to implement a Data Privacy and Consent Management Solution/Tools and the Bank invites online tender offers (Technical offer and Commercial offer) from eligible, reputed SIs/Bidders to **Design, Supply Implementation of Data Privacy & Consent Management Solution /Tool as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025.**

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/ 7977310
Date of RFP Issue	31/08/2026
Bid Security (EMD)	₹90,00,000.00 /- (Rupees Ninety Lakh 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

Signature of the Bidder with company Seal

	narration Tender ref no GEM/2026/B/7977310 dated 31/08/2026 in Favour of "Central Bank Of India" and payable at Mumbai.
e-mail IDs for sending queries and Last Date for submission of queries	cmitdpcell@centralbank.bank.in, cmdpcell@centralbank.bank.in Latest by 04/09/2026 up to 11:00 hrs.
Date and time for Pre-Bid Meeting,	04/09/2026 at 15:00hrs.
Last Date and Time submission of Bids Mode of bid submission & online portal's URL	28/09/2026 up to 15:00 hrs. Mode-Online Government e Marketplace (GeM)
Time & Date of Opening of technical bids	28/09/2026 at 15:30 hrs.
Address for Communication	Data Protection Officer Data Protection Cell RMD , Central Bank Of India 1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point, Mumbai 400 021. <u>Mail address:</u> dpo@centralbank.bank.in cmitdpcell@centralbank.bank.in cmdpcell@centralbank.bank.in
Contact Telephone Numbers	9981166123,7858842591

The pre bid meeting will be held in person with the Bidders. For any clarification with respect to this RFP, the 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	Bidder's Query/Suggestion/Remarks

Exemption from submission of EMD shall be given to Bidders, who are Micro and Small Enterprises (MSE)/ Startup. Bidders claiming exemption as MSEs shall submit a valid NSIC Registration Certificate and Udyam Registration Certificate 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.

Signature of the Bidder with company Seal

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 Bidder(s) or applicants whether verbally or in documentary form by or on behalf of Central Bank of India (Bank), is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of unconditional bids. The purpose of this RFP is to provide the Bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Further that written clarifications/corrigenda issued by the Bank shall form part of the RFP. Notwithstanding the above, all requirements specified herein as being mandated by the DPDPA 2023, DPDP Rules 2025, or any applicable regulation shall be construed in accordance with the applicable law as it stands on the date of contract execution, and bidders are advised to independently verify all statutory requirements Nothing contained in this disclaimer shall be construed as limiting, excluding, or waiving any statutory or regulatory compliance obligations imposed on the successful bidder under applicable law.

1 Eligibility Criteria

The Bidder must fulfil following eligibility criteria:

Sl. No	Eligibility	Documents to be submitted
A	GENERAL	
1	The Bidder 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 Bidder
2	The Bidder should be registered under G.S.T. and/or tax registration in State where the Bidder has a registered office	Proof of registration with GSTIN
3	The Bidder must be an OEM/Authorized Partner, Service Provider (SP), or System Integrator (SI) of the Original Equipment Manufacturer (OEM) or Original Software Developer (OSD) in India, with the authority to perform implementation, customization and upgrades during the contract period with the Bank.	MAF/Certificate from the OEM/OSD as per Annexure 8
B	FINANCIAL	
4	The Bidder should have had an average annual turnover of at least Rs. 50 Crore 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. In case of MSE relaxation may be given if the bidder is fulfilling technical and qualifying criteria.	Copy of Audited Balance Sheet and Operating Statement(P&L) and Certificate of the Chartered Accountant for preceding three FYs
5	The Bidder 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 Operating Statement(P&L) and Certificate of the Chartered Accountant for preceding three FY
C	SOLUTION	

Sl. No	Eligibility	Documents to be submitted
6	The proposed solution should be aligned and complied with Digital Personal Data Protection Act (DPDPA) 2023, DPDP Rules 2025 & MeITY NeGD issued BRD Document and the Proposed Solution should have the capability to be deployed on premises in Bank DC and DR	Certificate from the OEM
7	The Bidder has to give an undertaking that they will enable Integration capability and complete the integration process whenever the National Consent Management Portal Framework / Consent Managers is made live by Government without any additional cost to Bank.	Submit Self-declaration & confirmation on Company's Letter Head.
D	EXPERIENCE	
8	The proposed solution of the Bidder/OEM shall have the capability to support all 11 modules specified in this RFP. Further, at least 5 of these modules are mandatory including Modules 1, 2 and 4, must have been implemented or be under implementation, either together or separately, in one or more BFSI organisations in India or globally, during the 5 years preceding the date of publication of this RFP. Where any implementation is ongoing, the relevant Purchase Order/Contract must have been issued at least 3 months before the date of publication of this RFP. Modules: 1. Consent Management 2. Cookie Consent Management 3. Record of Processing Activities (RoPA) 4. Data Discovery, Inventory, Classification and Data flow Mapping 5. Data Privacy Assessments 6. Data Principal Rights Management 7. Data Protection Impact Assessments (DPIA) 8. Privacy Notice Management 9. Data and Privacy Breach Management 10. Compliance Monitoring, Reporting and Governance Dashboard 11. Third Party Risk Management	Copy of Purchase Order & Completion/ Work in Progress certificate from Client OR Certificate from the customer who has engaged the OEM on their letter head providing details of the engagement OR Any other document which suffices the requirement to the satisfaction of the Bank

Sl. No	Eligibility	Documents to be submitted
9	The Bidder must have prior experience in the implementation of privacy and data protection governance to ensure compliance with the provisions of the Digital Personal Data Protection (DPDP) Act and its associated rules/ GDPR etc. The Bidder should have successfully completed at least one (1) such implementation for a client within the Banking, Financial Services, and Insurance (BFSI) sector in India / Global.	Documentary evidence, such as work orders & completion certificates, or client references, must be submitted to the claimed experience.
10	The BIDDER must have a minimum of 50 personnel on its payroll in India, with expertise in the fields of Data Privacy and Consent Management to provide services to the Bank and have Direct support/Service offices in Mumbai/Navi Mumbai and Hyderabad..	Undertaking on Company's Letter Head with the details of employees with experience in the relevant field and certification
11	The Bidder should have any one of the valid accreditations mentioned here under • ISO/IEC 27001:2022 Certification • ISO/IEC 27701:2019 Certification • SOC 2 Type 2 Certification	Copies of relevant Certificates.
E	DEFAULT	
12	At the time of bidding, Bidder must not have been any pending litigation or legal disputes in the last two (2) years between the Bidder and/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	If the BIDDER is from a Country that shares a land border with India, the BIDDER 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
14	The 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

Sl. No	Eligibility	Documents to be submitted
15	BIDDER should not have - NPA with any Bank /financial institutions in India. - Any case pending or otherwise, with any organization across the globe which affects the credibility of the BIDDER in the opinion of Central Bank of India to service the needs of the Bank.	Submit Self-declaration on Company's Letter Head.

The 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 Bidder will be bound to provide the same.

Central Bank of India reserves the right to verify references provided by the Bidder independently. The Bidder shall submit only such documents as are required under this RFP as evidence of the facts stated therein. The Bank may, at any stage of the evaluation process, call for additional documents, information or clarifications, and the Bidder shall promptly furnish the same.

The Bank reserves the right to independently verify any information, credentials, experience certificates, client references, declarations or other documents submitted by the Bidder. If, at any stage before award, during contract execution, or after completion of the project, any information, credential, experience certificate, client reference, declaration or document submitted by the Bidder is found to be false, misleading, forged or materially inaccurate, the Bank shall, without prejudice to any other contractual or legal remedy available under law, be entitled to reject the bid, terminate the contract, forfeit the Performance Bank Guarantee (where applicable), recover any loss suffered by the Bank, debar the Bidder in accordance with the applicable procurement policy, and report the matter to the appropriate Government or regulatory authorities.

The decision of the Bank in this regard shall be final and binding, subject to applicable law, the terms of this RFP, and the Bank's procurement policy. Bank reserves the right to accept or reject any bid, wholly or partly, at any stage of the process, in accordance with applicable law and procurement policy, without thereby incurring any liability to the Bidder.

- 1) 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 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) Bidder must provide credential letter or installation sign off document.

Signature of the Bidder with company Seal

- 5) Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.
- 6) While submitting the bid, the 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 Bidder/OEM or 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 Bidder will deliver to the customer.'*
- ii. *If an agent submits the bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.'*

2 Bid Security (Earnest Money Deposit-EMD)

An amount of ₹90,00,000.00 /- (Rupees Ninety Lakh 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 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/ 7977310 dated 31/08/2026 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 Bidder withdraws its tender during the period of tender validity specified by the Bidder; or
- 2) If the Bidder does not accept the correction of its Tender Price; or-
- 3) If the successful Bidder fails within the specified time to:
 - i. Sign the Contract; or
 - ii. Furnish the required security deposit.
- 4) The EMD / Bid Security will be refunded to the Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG).
- 5) The EMD / Bid Security of unsuccessful Bidders shall be returned as promptly as possible after completion of bidding process.
- 6) In the event that the Bank discovers that any information, document, or declaration submitted by the Bidder is false, fabricated, or misleading, the Bank shall, in addition to forfeiting the EMD, reserve the right to debar the Bidder from participating in future tenders for a period of 3 years and report the matter to GeM authorities and IBA.

3 Performance Bank Guarantee (PBG)

- 1) As mentioned above, the Successful 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

Signature of the Bidder with company Seal

months, (5 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance and shall remain in force/valid till the contract period. The PBG shall be submitted within 21 days of the PO acceptance by the 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 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 Bidder is unable to service the contract for whatever reason.
- 5) In the event of delays by Successful 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. Notwithstanding the 30-day cure period, where the Bidder's failure to perform results in or creates a material risk of a personal data breach or regulatory non-compliance under the DPDPA 2023 or DPDP Rules 2025, the Bank may invoke the PBG without awaiting expiry of the cure period, subject to providing written notice to the Bidder
- 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 Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.
- 7) The Bank shall also be entitled to make recoveries from the Successful 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 Bidder under the contract. However, no interest shall be payable on the PBG.
- 9) The Bank may exercise such remedies as are available under the RFP, the Contract and applicable law, including forfeiture of EMD where permissible and prior to its refund/release, and/or invocation of the Performance Bank Guarantee where applicable, depending upon the nature and stage of default

4 Cost of Bidding

The 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

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

Signature of the Bidder with company Seal

Scope of Work

6 Scope of Work for the BIDDER

The implementation of the solution including Hardware, Software and Services for enabling and supporting the Bank's compliance with the DPDP Act, 2023 and DPDP Rules, 2025 in Bank across all identified and in-scope products, services, channels and systems of the Bank as agreed during requirement finalization.

Bank across applicable systems to cover applicable stakeholders and implement a robust, scalable, and compliant platform that supports the centralized collection, management, enforcement, and monitoring of Data Principal consent, while enabling comprehensive data privacy governance aligned with Indian (DPDP Act 2023 & DPDP Rule 2025) and global standards (GDPR, CCPA). The Scope of Work shall include supporting and assisting the Bank for effective adherence to the obligations of the Digital Personal Data Protection Act 2023 & DPDP Rules 2025 by performing applicability assessment and gap assessment and creating an implementation roadmap to remediate the identified gaps. On the basis of the gaps identified, data privacy framework including supporting guidelines, processes and templates shall be developed along with implementation support. The implementation shall include all configuration changes, workflow modifications, reports, templates and documentation reasonably required to align the implemented solution with amendments to the DPDP Act, DPDP Rules or official Government implementation guidelines issued during the implementation period, without additional licence or implementation charges. The implementation shall not be deemed complete merely upon installation of software. Completion shall be achieved only upon successful deployment, integration, configuration, testing, user acceptance, and submission of all agreed deliverables, remediation of critical and high-priority observations identified during implementation, knowledge transfer, and issuance of a Completion Certificate by the Bank.

The proposed solution shall be AI-enabled, cloud-ready, deployable on the Bank's on-premises in DC & DR location and capable of supporting future technology and regulatory requirements.

A. Gap Assessment, Solution Architecture and Implementation Planning:

The Bidder shall conduct a comprehensive assessment of the Bank's existing privacy governance framework, policies, procedures, systems, applications, contracts, and data processing activities to identify compliance gaps against DPDP Act 2023 and DPDP Rules 2025. The Gap Assessment Report shall classify each observation as Critical, High, Medium or Low Risk, identify the applicable statutory or regulatory requirement, specify the recommended remediation approach, identify the responsible stakeholder, and propose implementation timelines. The scope shall include privacy maturity assessment, policy and contract review, current-state and target-state assessment, design of enterprise privacy framework, preparation of data lifecycle models, data flow diagrams, DPIA framework, implementation roadmap, operating model, risk assessment, and project execution strategy to comply the DPDP Act 2023 & DPDP Rules 2025.

The AI components of the proposed solution shall not make autonomous decisions affecting the rights of Data Principals without human review. Any AI-based inference or classification of personal data shall be documented in the RoPA, and outputs shall be made
Signature of the Bidder with company Seal

available to the Bank's Data Protection Officer for audit purpose. The Bidder shall provide adequate documentation, audit logs and relevant information relating to the AI model to enable the Bank, its auditors and the Data Protection Officer to understand, verify and audit AI-assisted decisions relating to the processing of personal data. However, the Bidder need not be required to disclose its proprietary source code, confidential AI model architecture or proprietary training datasets, unless such disclosure is required under applicable law or is mutually agreed upon by the parties.

B. Infrastructure and Hardware Supply & Configuration

The Bidder shall supply, install, configure, commission, and maintain all required hardware, software, licenses, databases, operating systems, and supporting infrastructure required for deployment of the proposed solution. The proposed solution shall capable of deployment on the Bank's on-premises DC & DR location. The Bidder shall ensure high availability, disaster recovery readiness, scalability, performance optimization, and future cloud portability without additional cost to the Bank. . The Bidder shall ensure compatibility of the proposed solution with supported versions of the Bank's infrastructure components during the implementation period and shall carry out all necessary compatibility testing, configuration adjustments and integration activities without additional implementation charges

C. Data Privacy and Consent Management Solution

The Bidder shall provide and implement a fully integrated Data Privacy and Consent Management Platform covering the following modules:

1. Consent Management
2. Cookie Consent Management
3. Record of Processing Activities (RoPA)
4. Data Discovery, Inventory, Classification and Data Flow Mapping
5. Data Privacy Assessments
6. Data Principal Rights Management
7. Data Protection Impact Assessments (DPIA)
8. Privacy Notice Management
9. Data and Privacy Breach Management
10. Compliance Monitoring, Reporting and Governance Dashboard
11. Third-Party Risk Management

The proposed solution shall comply with CNCF standards and WCAG 2.1/2.2 accessibility requirements. The solution shall provide centralized privacy governance, workflow automation, regulatory compliance monitoring, consent lifecycle management, audit trails, risk assessments, reporting, analytics, dashboards, and management oversight capabilities required for effective implementation of privacy and data protection obligations.

D. Implementation of Proposed Solution

The Bidder shall undertake end-to-end implementation of the proposed solution, including installation, configuration, customization, integration, migration, testing, user acceptance testing, security validation, performance testing, disaster recovery testing, production deployment, and go-live support. The proposed solution shall be integrated with the Bank's Signature of the Bidder with company Seal

Core Banking System, Internet Banking, Mobile Banking, Omni Channel platforms, DLP solutions, customer-facing channels, Data ware house and other business applications in the Bank.

E. Support Services and Maintenance

The Bidder shall provide comprehensive post-implementation support and maintenance services throughout the contract period, including application support, infrastructure support, preventive and corrective maintenance, security patch management, version upgrades, incident management, problem management, SLA monitoring, performance optimization, and regulatory compliance support. The Bidder shall ensure continuous availability, operational stability, and effective functioning of the proposed solution.

F. Training and Knowledge Transfer

The Bidder shall provide comprehensive training, knowledge transfer, and handholding support for administrators, privacy officers, compliance teams, business users, and technical personnel. The scope shall include preparation of user manuals, technical documentation, standard operating procedures, configuration documents, architecture documents, operational runbooks, training materials, and knowledge transfer sessions to enable the Bank to independently manage and operate the proposed solution.

Brief details of the Proposed Data Privacy and Consent Management Platform should cover the following modules:

Sr. No.	Module Name	Details
1.	Consent Management Solution	The Bidder shall implement a Centralized Consent Management Platform with the following capabilities: 1. Consent capture across digital, physical channels, Phygital (Hybrid) and IVR Journey flows etc. 2. Support explicit & Affirmative, informed, granular, and purpose-based consent. 3. Consent collection through: - o Internet Banking - o Mobile Banking - o Website - o Branch channels - o Contact centre - o Third-party interfaces - o Other relevant applications 4. Consent lifecycle management including: - o Creation - o Modification - o Withdrawal - o Expiry - o Renewal 5. Purpose limitation and lawful usage validation. 6. Consent version management. 7. Multi-language consent support. 8. Time-stamped consent records with audit trail. 9. Centralized consent repository. 10. Consent validation and verification of single and multiple request from the applications. 11. Consent orchestration workflows. 12. Preference management dashboard for customers. 13. Consent synchronization across systems. 14. Automated consent revocation propagation along with monitoring. 15. Consent analytics and reporting. 16. Integration with Bank various application like CBS, Digital Banking, LMS, Digital Journey etc. 17. Role-based access controls and maker-checker workflows. 18. Tamper-proof audit logs. 19. Compliance reporting for regulators and auditors. 20. Integration with identity and authentication systems

Signature of the Bidder with company Seal

Sr. No.	Module Name	Details
		21. In order to prove who captured consent, the solution must include a digitization workflow with: a timestamp of the original collection, b. identity of the Bank official who digitized the consent, c. scanned archival of the physical form linked to the digital consent record, and d. a process to inform the Data Principal of their digital consent record. 22. The solution shall not implement pre-selected consent options, bundled consent, or default consent mechanisms. Every consent must be obtained through a clear, distinct, and affirmative action by the Data Principal for each specific purpose.
2.	Cookie Consent Management	The Bidder shall implement Enterprise Cookie Consent Management with the following capabilities: 1. Cookie discovery and scanning across Bank websites and portals. 2. Classification of cookies into categories. 3. Cookie inventory management. 4. Cookie consent banner implementation. 5. Granular consent options for cookie categories. 6. Multi-language cookie notices. 7. Geo-based cookie policy support. 8. Consent logging and audit trails. 9. Consent withdrawal and preference modification. 10. Real-time blocking of non-essential cookies prior to consent. 11. Cookie lifecycle monitoring. 12. Integration with web applications and CMS platforms. 13. Reporting dashboard for cookie compliance. 14. Alerts for unidentified or non-compliant cookies. 15. Automated periodic cookie scanning. 16. Policy updates management. 17. Support for mobile web and responsive applications. 18. Compliance mapping to DPDP and global privacy requirements where applicable.
3.	Record of Processing Activities (RoPA)	The Bidder shall implement RoPA management capabilities including: 1. Centralized RoPA repository. 2. Identification and documentation of processing activities. 3. Capture of: - o Purpose of processing - o Categories of personal data - o Data principals - o Data recipients

Sr. No.	Module Name	Details
		○ Data retention ○ Cross-border data transfer details ○ Legal basis 4. Business unit-wise mapping. 5. Application and process mapping. 6. Data flow visualization. 7. Automated workflow for RoPA approvals. 8. Version management and historical tracking. 9. Integration with data discovery and inventory modules. 10. Automated updates based on system changes. 11. Search and filter capabilities. 12. Regulatory reporting support. 13. Risk tagging and classification. 14. Review and recertification workflows. 15. Audit trail and change management. 16. Dashboard and analytics for processing activities
4.	Data Discovery, Inventory, Classification and Data flow Mapping	The Bidder shall implement Enterprise-wide Data Discovery and Classification and Data Flow Mapping capabilities including: 1. Use automated tools/mechanisms for discovery across structured and unstructured repositories. 2. Discovery across: ○ Databases (oracle , DB2 , MySql , postgresQL , MongoDB etc) ○ File servers ○ Endpoints ○ Email systems ○ Applications ○ Data Warehouse / lakes ○ Cloud environments 3. Personal data identification. 4. High-risk personal data / critical personal data categories as may be identified. 5. AI/ML-based classification capabilities. 6. Pattern-based and rule-based discovery. 7. Data inventory creation and maintenance. 8. Data lineage mapping. 9. Metadata management. 10. Classification based on criticality and sensitivity. 11. Data owner and custodian mapping. 12. Data retention and archival tagging. 13. Duplicate and redundant data identification.

Sr. No.	Module Name	Details
		14. Risk-based data scoring. 15. Data flow mapping. 16. Continuous discovery and monitoring. 17. Dashboard and analytics. 18. Compliance reporting. 19. The solution must explicitly support legacy mainframe environments and the Bank's Core Banking System (CBS) architecture
5.	Data Privacy Assessments	The Bidder shall implement Data Privacy Assessment management capabilities including: 1. Privacy assessment framework creation. 2. Configurable questionnaires and templates. 3. Automated assessment workflows. 4. Privacy risk scoring. 5. Assessment tracking and monitoring. 6. Business process assessment. 7. Product and application privacy reviews. 8. Vendor privacy assessments. 9. Compliance gap identification. 10. Risk remediation tracking. 11. Review and approval workflows. 12. Evidence attachment and document management. 13. Risk heatmaps and analytics. 14. Centralized assessment repository. 15. Automated reminders and escalations. 16. Integration with DPIA and RoPA modules. 17. Audit trails and reporting. 18. Regulatory compliance mapping.
6.	Data Principal Rights Management	The Bidder shall implement Data Principal Rights Management capabilities including: 1. Intake and management of Data Principal requests. 2. Support for rights requests as per DPDP Act 2023 and DPDP Rules 2025 including: - o Access - o Correction - o Erasure - o Consent withdrawal - o Grievance handling - o Nomination requests etc. 3. Digital, Omni & other Channel request intake 4. SLA-based request tracking.

Sr. No.	Module Name	Details
		5. Automated workflow orchestration. 6. Data - Principal dashboard. 7. Audit trail and evidence management. 8. Closure approvals and notifications. 9. Escalation workflows. 10. Multi-language support. 11. Notification Engine
7.	Data Protection Impact Assessments (DPIA)	The Bidder shall implement DPIA capabilities including: 1. DPIA template and workflow management. 2. Automated DPIA initiation based on risk triggers. 3. Risk assessment and scoring. 4. Identification of high-risk processing activities. 5. Mitigation planning and tracking. 6. Workflow-based approvals. 7. Risk acceptance mechanisms. 8. Integration with RoPA and privacy assessments. 9. Regulatory compliance mapping. 10. Dashboard and risk visualization. 11. Historical tracking and version management. 12. Automated reminders and escalations. 13. Reporting for management and regulators. 14. Audit trail maintenance. 15. Evidence and document repository. 16. Residual risk assessment. 17. Centralized DPIA repository.
8.	Privacy Notice Management	The Bidder shall implement Privacy Notice Management capabilities including: 1. Centralized Privacy Notice repository. 2. Privacy Notice template management. 3. Multi-language privacy notices. 4. Version control and archival. 5. Automated publishing workflows. 6. Consent-linked privacy notices. 7. Dynamic notice rendering. 8. Notice acknowledgement tracking. 9. Channel-wise privacy notice management. 10. Policy update workflows. 11. Review and approval processes. 12. Audit trail and compliance reporting. 13. Integration with Bank various websites and applications. 14. Automated notification for notice changes.

Sr. No.	Module Name	Details
		15. Search and retrieval capabilities. 16. Regulatory mapping and reporting.
9.	Data and Privacy Breach Management	The Bidder shall implement Data Breach Management capabilities including: 1. Integration with SIEM, SOC, and incident management systems and other relevant systems. 2. Breach incident intake and logging. 3. Incident categorization and severity assessment. 4. Automated breach response workflows. 5. Root cause analysis tracking. 6. Impact assessment management. 7. Affected data principal identification. 8. Regulatory notification workflows. 9. Internal escalation mechanisms. 10. Evidence and forensic record management. 11. Corrective and preventive action tracking. 12. SLA tracking and monitoring. 13. Audit trail maintenance. 14. Dashboard and analytics. 15. Closure and approval workflows. 16. Reporting for regulators and management. 17. Integration with risk management systems. 18. Lessons learned and improvement tracking 19. The breach management module shall be capable of: (a) automatically identifying and quantifying affected Data Principals based on the systems/databases impacted by the breach; (b) generating regulatory notification reports in the format prescribed by the Data Protection Board of India; and (c) integrating with the DPBI's digital portal for breach notification when such portal is made operational, at no additional cost to the Bank
10.	Compliance Monitoring, Reporting and Governance Dashboard	The Bidder shall implement Centralized Controls, Reporting, and Dashboard capabilities including: 1. Enterprise privacy compliance dashboard. 2. Real-time monitoring of compliance status. 3. Role-based dashboards. 4. Executive and board-level reporting. 5. Compliance scorecards. 6. Risk heatmaps and trends. 7. Customizable reports. 8. Regulatory reporting templates. 9. SLA monitoring dashboards.

Signature of the Bidder with company Seal

Sr. No.	Module Name	Details
		10. Alerting and notification mechanisms. 11. Audit and compliance reporting. 12. Export capability in multiple formats. 13. Drill-down analytics. 14. Historical trend analysis. 15. Centralized policy compliance monitoring. 16. Automated compliance evidence generation. 17. Dashboard access controls. 18. API support for reporting integration
11.	Third Party Risk Management	The Bidder shall implement Third Party Privacy Risk Management capabilities including: 1. Third-party inventory management. 2. Vendor privacy assessment workflows. 3. Third-party data processing assessment. 4. Contract and DPA tracking. 5. Risk scoring and categorization. 6. Due diligence workflows. 7. Continuous monitoring of third-party risks. 8. Evidence and certification management. 9. Compliance tracking. 10. Vendor on boarding and off boarding monitoring workflows. 11. SLA and remediation tracking. 12. Integration with vendor management systems. 13. Regulatory compliance mapping. 14. Dashboard and analytics. 15. Automated reminders and escalations. 16. Audit trail and reporting. 17. Cross-border data transfer tracking. 18. Periodic review and reassessment workflows.

6.1 Project initiation and planning:

- Define the objective based roadmap with milestones and goals to implement Centralized Consent Management and Data Privacy Management Tool.
- Develop a detailed implementation plan with timelines and deliverables.
- Develop comprehensive project plan with pre-requisites and dependencies.
- Program governance – weekly, monthly and quarterly.

6.2 Requirements, Design Configuration and Setup:

- Understand the business landscape to capture the as-is requirements and convert them into business use cases to be implemented.
- Document functional and non-functional requirements of Centralized Consent Management and Data Privacy Tool.
- Develop detailed system architecture, including High-Level Design (HLD) and Low-Level Design (LLD), ensuring alignment with technical, regulatory, and business requirements.
- Install and configure the Consent & Privacy Management Tools according to data privacy landscape and regulatory guideline in the Bank.
- Configure all integrations with applications of the Bank which process personal data along with ITSM, IT GRC tools etc.

6.3 Functional Scope for Study the Bank System, Prepare PII Data Inventory, GAP Assessment, Prepare a Roadmap / Approach / Implementation Plan and Implement the solution, Policy Review , Framework Design ,Integration and Implementation:

6.3.1 Applicability Assessment: This section defines the scope and the extent to which DPDP Act 2023 & DPDP Rules 2025 requirements are applicable to Bank's operations, data handling practices, and overall business activities.

- Study & understand comprehensively the provisions & requirements of Digital Personal Data Protection Act 2023 & DPDP Rules 2025 and any subsequent amendments/ updates. Identify the list of products and services offered by the Bank. Assess applicability of provisions of the DPDP Act 2023 & DPDP Rules 2025 for each Function/Department of the Bank.
- Conduct walkthroughs with the respective Department & Key Stakeholders to understand applicability of DPDP Act 2023 & DPDP Rules 2025 on business processes processing personal data of customers, employees, contractors, third parties etc. with respect to Data Principals within India across core business processes and support functions.
- Analyse the present organizational structure, governance, policies, and procedures related to data flow, security, and privacy with the focus to implement necessary measures as per applicable Laws & Regulations with the objective to assist the Bank for effective adherence to the regulatory obligations.
- Documentation policies and procedures for encryption, safeguarding all sensitive information in accordance with relevant Information Security policies
- Study the consequences outlined in the DPDP Act 2023 & DPDP Rules 2025 for non- compliance. Identify and enlist the legal implications and financial penalties that may be attracted if the Bank fails to adhere to the stipulated data protection measures and highlight the same to stakeholders of the Bank.
- Analyse and share with Bank the insights of its definitions, stipulations, obligations, and the scope of the DPDP Act 2023 & DPDP Rules 2025 in applicability to the Bank.

- Assess applicability of provisions of the act on the operations, products, processes, channels, systems and in overall Data Infrastructure of the Bank.
- Identification of Digital Personal Data in the organization and its lifecycle stages - creation, storage, usage (processing), transfer and elimination / purging. This includes review of existing processes and controls, products and services and data governance standards applied by the Bank.
- Identification of vendors / third parties processing Organization's data, usage as per SLAs processing undertaken, evaluation of data security measures applied.
- Discuss and finalize the Applicability Assessment report with the relevant stakeholders.

6.3.2 Gap Assessment: Aims to study the existing privacy practices, policies and processes within Bank against DPDP Act 2023 & DPDP Rules 2025, requirements and Perform gap Assessment basis the Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025 thereon

- Identification and Gap Assessment of existing processes/products, practices vis-à-vis DPDP Act 2023 and DPDP Rules 2025 requirement.
- Create the Privacy control matrix/framework with respect to requirements as per DPDP Act 2023 and DPDP Rules 2025.
- Study existing roles, responsibilities and reporting structures covering all the stakeholders, divisions, offices responsible for Data Security/Privacy for the Bank.
- Identify & Assess All Data Touch Points in existing structure of the Bank and associated third Party platforms for Data related functions like Data Entry, Exit, Process, Storage, Erasure, and other Data Handling activities/all types of Data Flows, either digital personal data, including personal data collected in physical form and subsequently digitised being handled in the Bank/of the Bank/for the Bank
- Understand exhaustively the existing Data Infrastructure which shall include Identify and Assess comprehensively the tools, systems, software, applications, channels, and other technological infrastructure employed/used in the entire data handling process/functions at all the points within the Bank when Data is in transit, use and at rest (i.e. Data Entry, Exit, Storage, Processing, Sharing, Retention, Disposal, etc.) as part of extant data management infrastructure.
- Conduct an entity level privacy gap assessment for the existing controls, key business processes, transfer, and movement of personal data within and outside Bank.
- Analyse the existing privacy policies, procedures, and other relevant documentation & templates to identify gaps against the control framework.
- Study the Existing Grievance Redressal Structure & Governance of the Bank and propose necessary changes for compliance of DPDP Act 2023 & DPDP Rules 2025.
- Analyse the IT posture (e.g., various encryption solutions, anonymization, pseudonymization, Redaction, Secure Multi Party Configurations, private set intersection, Synthetic Data etc.), while integration with other applications, sharing data on a required basis etc. against the control framework.

Signature of the Bidder with company Seal

- **Develop a risk classification framework for personal data based on sensitivity, volume, business criticality and regulatory impact further** considering factors like Gaps in the existing Framework/Structure of Data Privacy in the Bank, criticality and volume, with the objective of complying with provisions outlined in the Act & Rules

6.3.3 Third party Contract Review: This step shall assess key privacy risk and identify contractual and process level controls to mitigate third party risk from data privacy standpoint.

- Obtain list of third party with whom personal data is shared for processing.
- Develop a Control framework and questionnaire based on the DPDP Act 2023 and DPDP Rules 2025 to assess vendor's privacy posture.
- Perform contract review with Bank's external vendors (data processors) to assess data processing agreement clauses and obligations to comply with DPDP Act 2023 and DPDP Rules 2025 requirements.
- Identify gaps in contracts and data protection clauses to be incorporated in such contracts.

6.3.4 Framework Design to establish a structured and comprehensive set of guidelines, policies and processes: This section provides a clear blueprint that ensures the processes align with DPDP Act 2023 & DPDP Rules 2025 requirements.

6.3.4.1 Develop Data Privacy Framework as per DPDP Act 2023 & DPDP Rules 2025 requirements

- Study the overall organizational structure & set up of the Bank, identifying departments in Central Office, Zonal Offices, Regional Offices, Branches, other Offices along with the hierarchy of reporting.
- Study existing roles, responsibilities and reporting structures covering all the stakeholders, divisions, offices responsible for Data Security/Privacy for the Bank.
- Review, assess, create, and update all policies, procedures, SOPs, templates, checklists, playbooks, and other governance related documents as per DPDP Act 2023 and DPDP Rules 2025 prescribed.
- Identifying Privacy Enabling Technology.
- Clearly define and distinguish between security and privacy concerns and requirements.
- Develop/ Update Privacy Framework based on DPDP Act 2023 and DPDP Rules 2025 requirements for handling personal data including (but not limited to) data collection, processing, storage, retention, sharing and disposal. This shall include:
 - Privacy Policy
 - Consent management policy
 - Data Processing Policy
 - Data Breach Management Policy

- Data Principal Request Handling Guidelines
- Data Retention Policy & Guidelines
- Grievance Redressal Policy
- Third Party Risk Management Policy
- Data Principal Rights Management Policy
- Breach Management guidelines & SOP
- Update Existing contractual clauses.
- Vendor audit checklist
- Roles and responsibilities of DPO, CISO, CDO, CTO in view of DPDP Act 2023 and DPDP Rules 2025.
- Develop data privacy organization structure along with defined roles and responsibilities.
- Privacy notice and cookie policies
- Document Data Privacy Organization structure along with roles and responsibilities to align with Bank requirements and obtain signoff.

6.3.4.2. Consent Management (In line with “MeiTY NeGD issued BRD” Document)

- Design and Operationalize Enterprise Level Consent Management Framework with appropriate policies, procedures, templates, technical measures to be implemented across all products and internal business functions.
- The framework should be able to cater measures for collection, storage, modification, and withdrawal of consent as well as demonstrating recording of the said process.
- Framing appropriate model consent form (physical/digital) for different categories of products/ processes/ purposes as per the DPDP Act 2023 & DPDP Rules 2025 requirement.
- Identify the consent collection points across each product/business function and coordinate with the various product owners to integrate DPDP Act 2023 and DPDP Rules 2025 consent requirements within their respective consent journeys.
- Coordinate with relevant teams and implement Progressive consent log management, tagging and effectively ensure that consent including its modification and revocation journeys with the personal data element.
- Evaluate internal tools / processes for meeting the requirements as per the Act/Rules.
- Identify and connect with various departments/business functions to determine and communicate their accountability and responsibility with respect to consent management.
- Coordinate with relevant teams and implement the integration with various internal applications, Bank’s website, Data warehouse/ Single Data Repository etc.
- Analyse and propose cookie consent and preference management framework with a detailed cookie notice. Integrate the cookie consent across the data processing systems to ensure consensual processing of data collected through cookies.
- Review, assess and create cookie policy.

Signature of the Bidder with company Seal

- Analyse the impact of consent modification/revocation by Data Principals on processes/customer relationship management/business intelligence/marketing leads generation, etc.
- Identify the list of services/processes/sub-processes for which Essential and Optional consent requirements shall be required
- Define **Essential and Optional consent requirements** based on the type of product/services as per purview of the act.
- Designing of format for following:
 - “Notice” that will be served to the customer while collecting personal data as per the requirements of the Act/Rules.
 - “Consent” that will be obtained from the customer while collecting personal data as per the requirements of the Act/Rules..
 - **Mechanism for receipt, recording and implementation of withdrawal of consent** that should be obtained from customer.
 - “Parental Consent” that will be obtained from the parents/lawful guardians while collecting personal information of children while collecting personal data as per the requirements of the Act/Rules..
 - Notifying the concerned authorities and customers in case of any data breach etc as per DPDP Act 2023 & DPDP Rules.
- Formulate SOPs & Mechanism for serving notice to customers and obtaining & withdrawal of consent of customers
- Prepare an automated framework/ mechanism for processing/ managing/ adding/modifying/deleting the user data consent and preferences, ensuring compliance with privacy regulations.
- Drive the integration of system-level changes to automatically accommodate the changes in system/database based on consent received from user/customer and manages alterations in the system/database in the event of consent withdrawal.
- Implement Bank wide consent Mechanism repository and drive the integration of various customer touch points into consent repository.
- Devise a strategy for Automated Integration & management of impact on the processes & services upon addition/modification/removal of the consent by Data Principals/their nominees.
- Devising a mechanism to limit the use of consent for the purpose it is obtained.
- Develop processes for obtaining and managing consent and provide mechanisms for users to express their data preferences. Further, define operational processes to seamlessly address customer consent in day-to-day operations.
- Design and drive the implementation of online and offline “Consent Management Platform”, from which customers can submit/modify/withdraw their consent.
- Formulation of guidelines considering the requirements of the other extant acts and regulations applicable to the Banks for retention of the customer data if customer withdraws the consent.
- Develop consent management guideline documents to manage consent across the business functions of Bank to cover the scenarios below:

- Collection of personal data via website, apps or physical copies & from third party systems.
- Disclosure of information to government agencies
- Procedure to respond, handle and manage consent withdrawals.
- Process of sharing data with business partners, third parties, Govt. Agencies, and between various systems.
- Transfer of data between entities, if any
- Develop/update consent management form (Physical, digital or otherwise).
- Develop business requirement documents and evaluate vendors for implementing tools to manage consent

6.3.4.3. Notice

- Understand personal data processing activities across each product/ process and type of personal data processed, in a way Data Principals can exercise their data privacy rights and raise grievances.
- Review content of Bank's displayed notice across various public facing products/Bank's website or any such platform accessible to public.
- Frame appropriate Notices for different categories of products/processes/purposes as per the DPDP Act 2023 & Rules 2025 requirement.
- Implement Privacy Notice wherever required (Applications / Processes) as per DPDP Act 2023 and DPDP Rules 2025 prescribed.
- Drafting of Privacy Notice and Consent Format (The Privacy Notices will be finalized in English and translated into 22 languages) where consent need to be obtained. Drafting of notices for cases where consent of processing of personal data already stored with Bank.

6.3.4.4. Grounds for processing personal data

- Assess the personal data processing activities undertaken within each product/ business function across channels and platforms and all levels of governance (Central office, Back office, Admin offices, Zonal Office, Processing Centre, Branches etc.) to understand personal data infrastructure and landscape of the Bank.
- Inventory the personal data processed within the said product/ business function across all levels of governance.
- Review the existing template to assist the departments to identify grounds for processing personal data for each product/business function and suggest changes and implement the same.
- Identify, determine and document the specific lawful ground for each personal data processing activity in accordance with the Digital Personal Data Protection Act, 2023, including consent, certain legitimate uses or any other legally permitted basis.
- Data Minimization & purpose limitation to be ensure.
- Determine rounds of processing personal data while introducing new banking services delivery mode/channel or while offering new product in addition to exiting processing landscape during the currency of contract period.

Signature of the Bidder with company Seal

- Prepare Inventory of Expressly for processing personal data which banks shall consider while processing personal data
- Identify and document processing activities that are not supported by consent, certain legitimate uses, statutory obligation, regulatory requirement, contractual necessity or any other lawful basis recognised under applicable law, and specify the safeguards or corrective actions required for such activities.

6.3.4.5. Certain Legitimate Uses

- Determine the applicability of each legitimate use with regards to personal data processing activities undertaken by the Bank across each product, processes, and internal business function.
- Identify legitimate uses and integration of these uses/ purposes with the privacy management framework including consent management.

6.3.4.6. General obligations of Data Fiduciary/ Significant Data Fiduciary

- Design and Develop Key Performance Indicators (KPIs) to track overall compliance of the Bank with the provisions mentioned under the DPDP Act 2023 & DPDP Rules 2025, especially its obligations as a Data Fiduciary / Significant Data Fiduciary.
- Third party privacy management (Data Processors):
 - Review existing policies, procedures, documents etc. in view of DPDP Act 2023 and DPDP Rules 2025 and suggest necessary changes.
 - Frame guidelines to identify and record lists of third parties with access to personal data of the Bank across all levels of operations including corporate Centre, circle/regional offices, central processing centers, branches, specialized offices such as training centers etc.
 - Assess the existing standard vendor agreements with data processors from a data privacy perspective and identify any gaps in obligations enumerated therein.
 - Provide illustrative templates/changes to existing data processor agreements between Bank and Data processors.
 - Provide guideline/ checklist for detailed assessment of data processors including their facilities, with respect to implemented data privacy and security measures, as required from DPDP Act 2023 and DPDP Rules 2025 perspective.
- Personal Data Governance:
 - Study the existing data sharing practices and identify the Data Fiduciaries/ processors with whom personal data is shared.
 - Design and develop detailed recommendations to remediate any gaps/risks identified through the said assessment.
 - Identify stakeholders in remediating these risks.
- Data Retention and Erasure:

- Identify and document if data retention periods are determined for all structured data. If not, connect with relevant teams to determine the same.
 - Develop a centralized data retention & disposal process applicable across organization.
 - Develop mechanism in existing applications to integrate and comply with DPDP Act & DPDP Rules 2025.
 - Device guideline/ mechanism to provide timely alerts with respective stakeholders for deletion of personal data.
 - Review and advise changes in the Bank's Policy on Record and Data Retention, erasure, archival along with related Procedures SOPs.
 - Design Framework mechanism/template to tag such retention period highlighted above, to personal data stored/processed across all platforms used to process such personal data where regulatory mandatory retention obligations (under BR Act, PMLA, FEMA, and RBI directions) take precedence over DPDP consent-based erasure obligations. Develop mechanism to clearly communicate to the Data Principal, upon a request for erasure, the specific legal basis under which data is being retained despite the request
- **Grievance Redressal:**
 - Study and analyse existing grievance redressal systems within the Bank.
 - Review the existing centralized grievance redressal mechanism, to leverage all data privacy related grievances can be centrally received, acknowledged, tracked, and responded through this system within specified timeline and suggest necessary changes.
 - Create grievance redressal process/workflow to meet the grievance redressal deadlines issued by the Act/Rules.
 - Connect with legal teams to templatize/frame playbook, responses and prevent any risks while responding to the grievances.
 - Create an RACI/ escalation matrix with oversight from relevant departments.
 - **Technical and Organizational Measures:**
 - With the help of relevant teams, review technical measures being implemented by the Bank to ensure privacy of personal data processed.
 - Review the governance and operating model implemented by the Bank to ensure effective implementation of data privacy preserving controls across people, process, and technology.
 - Review if the organizational measures are implemented across all levels of operations is adequate i.e., corporate Centre, regional offices, processing centres, branches etc.
 - Review the detailed roles and responsibilities matrix across each layer of operations and governance to ensure complete coverage across the Bank.

- Provide detailed recommendations and assist the Bank in implementing the same.

6.3.4.7. Processing of Personal Data of Children and PWD

- Identify products/processes that collect personal data of children and persons with disabilities and check the requirement of legal guardian is fulfilled.
- Review with business teams/ departments for specific products to ensure personal data is not used for any profiling activities or any activities which may be deemed harmful for the child as per DPDP Act 2023 and DPDP Rules 2025 prescribed.
- Assess if verifiable consent of the child's guardian is obtained before or at the time of collection of personal data.
- Design/ update the existing mechanism to recognize children/ persons with disabilities and obtain verifiable consent as suggested in DPDP Act 2023 and DPDP Rules 2025 prescribed.

6.3.4.8. Data Principal Rights Management

- Develop Data Principal Rights Management process covering identity verification, recording, validation, and timely response to data principal request.
- Discuss with relevant stakeholders to obtain their input and signoff.
- Develop business requirement documents and implement the tools to manage data principal rights.
- Identify and Review organization's policies for legal grounds of processing personal data for each product/business function and suggest for changes.
- Established Data minimization and data limitation Principles
- Create Data Principal Rights Management Process with input from relevant stakeholders.
- Understand personal data processing activities across each product/ process and type of personal data processed, in a way Data Principals can exercise their data privacy rights and raise grievances.
- Create operational procedures where nominee of Data Principal is to exercise the rights of Data Principal.
- Identify the databases which will be queried/access obtained for providing access requests.
- Review existing applications and prepare standards for new applications to cater for the Rights of Data Principals.
- Create response templates for each type of Data Principal request to ensure complete and effective resolution in a timely manner as per the prescribed format of the DPDP Act 2023 and DPDP Rules 2025.
- Create a detailed RACI with all stakeholders to ensure tracking of accountability and responsibility of all stakeholders.

- Integration of existing nominee management of Bank for products with Nominee made under Data Principal Capacity by the virtue of DPDP Act 2023 and DPDP Rules 2025.

6.3.4.9. Personal Data Breach Management/ Incident Management and response

- Assess, review, and update the existing incident management policies and procedures.
- Develop breach management guidelines for detecting, reporting, and responding to data breaches in compliance with DPDP Act 2023 and DPDP Rules 2025 requirements.
- Discuss the updated guidelines with concerned stakeholders to obtain their input and obtain signoff.
- Develop internal and external communication plans to manage internal and external stakeholders in case of data breach.
- Formulate an incident management and response framework to effectively address and mitigate data privacy incidents.
- Recommend and assist the Bank in establishing clear procedures for reporting incidents, conducting investigations, and implementing corrective actions.
- Explore the modes & authentication mechanism through which data is made available/accessible
- Formation of policies, frameworks, SOPs, and mechanisms for continuous Risk Management to mitigate data protection risks.
- Prepare accountability and responsibility chart regarding data protection throughout the organization.
- Engage in continuous monitoring and updates of security measures to adapt to evolving threats and technological advancements.
- Collaborate with external cybersecurity experts for periodic assessments and recommendations on improving data security practices.
- Define parameters for classification and assessment of personal data breach.
- Develop a robust incident response structure for Data Breaches which shall include but not limit to Designing of policies, frameworks, roles & responsibilities, escalation matrix, hierarchy and SOPs for the prompt identification, handling and reporting of Data Breaches. The framework should cover all the aspects of security & privacy as per DPDP Act 2023 & DPDP Rules 2025 and the Bank's requirements.
- Develop Breach/incident reporting framework/policy.
- Design, develop and implement the SOP with relevant RACI matrix for communicating to Data Protection Board and Data Principals as per DPDP Act 2023 and DPDP Rules 2025.
- Develop Privacy Incident Response Plan separately or update the existing Information Security Incident Response plan and note observations from tests through simulations.

- Conduct multiple table top simulations to help stakeholders identify their respective roles during crisis situations.
- Integrating Breach management into various Process of Bank such as Customer Support, Social Media updates etc. and prepare a suitable playbook.

6.3.4.10. Processing of personal data outside India

- Identify if any personal data is processed outside India.
- Create a register to record all personal data processing undertaken outside India including that undertaken by the Bank's processors.
- Centralized Mechanism for monitoring cross border data transfer.
- Cross border data to be analyzed from applicability of the DPDP Act 2023 and DPDP Rules 2025 perspective

6.3.4.11. Data Privacy and Security in Cloud Environment

- Recognize the shared resources in cloud infrastructure operated by the Bank or by authorised third-party cloud service providers utilized for data sharing along with the diverse mechanisms employed to store and share such data with internal/external stakeholders.
- Conduct a comprehensive assessment of the existing cloud infrastructure to identify potential vulnerabilities and compliance gaps.
- Classify data hosted in the cloud, ensuring a clear understanding of the types of information stored.
- Review robust access control mechanisms to restrict and monitor user access to data within the cloud environment.
- Review and Assist encryption protocols to safeguard data during transmission and storage, adhering to industry standards and regulatory requirements.
- Verify that data stored/ processed in the cloud (whether data is processed in cloud in India or outside India) complies with legal and regulatory requirements regarding data localization and privacy.
- Conduct periodic reviews of cloud security policies, ensuring they remain aligned with evolving risks and compliance requirements.
- Engage in on-going collaboration with the cloud service provider to address emerging security challenges and optimize the security posture.
- Develop a communication plan to inform customers about the security measures in place and reassure them of the bank's commitment to data privacy within the cloud environment

6.3.4.12. Conduct DPIA

- Identify business processes or products, departments and applications involved in high-risk processing of personal data.
- Create a data protection impact assessment SOP including assessment methodology, checklists, and report templates to conduct effective data protection impact

assessment exercise across all products/business functions including all levels of operations as per DPDP Act 2023 and DPDP Rules 2025.

- Create DPIA calendar to ensure complete coverage of all products and processes in a timely manner and provide training to appropriate Business User department and relevant teams to complete the DPIA.
- Develop a DPIA questionnaire and share with the business functions / department.
- Conduct walkthroughs with the identified business units to understand the associated data privacy risks
- Identify and document the risks, provide detailed recommendations for mitigation, and track them for implementation with the respective product owners.
- Perform Data Protection Impact Assessment (DPIA) on all business processes/products, Business/Third Party arrangements as per applicable data privacy regulations.
- Conduct Application based DPIA for IT applications and for the key applications (No. of applications can be mentioned) processing personal data.
- Prepare DPIA reports outlining the high risk involved in processing activities and pertaining applications.
- Prepare a risk Categorization Matrix based on risk analysis during DPIA and Data Privacy risk assessment and treatment plan for Privacy related risks identified.
- Support in obtaining approvals and signoffs from the Data Protection Officer before releasing the reports

6.3.4.13. Additional Obligations of Significant Data Fiduciary

- **Data Protection Officer:**
 - Assess and update the roles and responsibilities of the Data Protection Officer and members of the Data Privacy Team.
 - Data Privacy Office – Operations & support
- **Data Privacy Audits:**
 - Conduct self-assessment as per DPDP Act 2023 and DPDP Rules 2025 and Rules.
 - Integrate DPIA with existing audits of the Banks to prevent any overlaps and gaps.

6.3.5. Conduct DPIA and Create DFD shall help in understanding the flow of personal information across data life cycle along with identification of impact on key applications and infra elements processing personal data

6.3.5.1. Develop Data Flow Diagram and Data Inventory

- Define Data in terms of Data Privacy, Data Classification, Data Quality, Data Flow and Data Control.
- Identify and define the relevant statutory rights , obligations, rights, roles and responsibilities under the DPDP Act 2023 and DPDP Rules 2025 (such as Data

Principal, Data Fiduciary etc.) together with the Bank's internal Data governance role such as Business Data owner / Data Custodian / Data Stewards etc.

- Identify, Assess and segregate the various types of digital and physical data being handled at all the offices of the Bank during its Lifecycle of such data handling.
- Undertake measures for maintaining data accuracy and security.
- Identify Type of Data Processing/Handling Activities in each Process Step and segregate the involved PII/ personal data of higher risk, criticality or confidentiality.
- Assess the mapping of Data Flows across Business Processes & its accessibility at all levels in alignment with Data Handling Purpose.
- Create a Know Your Data Module:
 - Type of Data Collected
 - Source/Medium of Data Collection
 - Record and Log of such Data Put to Use
 - Accessibility of Such Data
 - Purpose of Collection
 - The potential and Limit of Usage of such data/consented data to be/ being collected or already collected.
- Identify business processes, departments and assets involved in high-risk processing of personal data.
- Conduct walkthroughs with stakeholders to understand the flow of personal data for the key business processes (covering all departments, products and business processes) along with the identification of application and underlying infrastructure involved.
- Design department-level Personal Data Inventory that covers the personal data lifecycle of each personal data elements.
- Prepare detailed Data Flow Analysis Document/Report to cover/capture all the processes followed in the respective department/office. The document should also capture all the journeys related to handling of sensitive data in the department like:
 - Data ingress and egress points
 - Data handling, storage and sharing mechanism.
 - Data access rights/privileges.
 - Types of data files and formats (for fingerprinting in DLP).
 - Classification of the identified data as per the bank's policy.
 - Security of data in transit, in use and at rest.
 - List of all the data sharing platforms like SFTPs etc
 - SharePoint, Emails etc.
- Assess the quantum of Data on which various functions are executed viz. a viz. the quantum of Data actually required to be processed. Identify the redundancy/irrelevant/excess information or data used in such processes.
- Identify the details of data storage in the department/branch which includes Understanding the various endpoints and review mechanism used to store the received and processed data for e.g., Data stored in local systems, data stored on file servers, etc. along with recording and analysing the type of data being stored.

- Reviewing all the involved process and analysing the risks associated with the security of data in transit, use and at rest.
- Details and review of all the risks associated with the stored data in the department/branch
- Establish a systematic approach for classifying and mapping data, creating an inventory to understand the types of data the Bank processes.
- Implement measures for secure storage, retrieval, and disposal of sensitive information.
- Examine and analyze the details of access rights and permissions pertaining to data at all stages and across all levels

6.3.6. Implementation Roadmap covers creation of roadmap to implement controls for DPDP Act 2023 & DPDP Rules 2025 compliance based on the gaps identified in current state assessment.

- Based on the gaps identified in current state assessment and actionable as per defined Privacy Framework and other phases, create an implementation roadmap based on effort and priority matrix.
- Create an implementation tracker mapped to each observation with further action steps and responsibility

6.3.7. Data Life Cycle for Personally Identifiable Information (PII)

- Define process to Identify PII (Personal Identifiable Information) and clearly define Personal data in accordance with the obligations of the Act & Rules.
- Establish a structured Data Life Cycle for Personally Identifiable Information (PII) data.
- Clearly define stages from data collection to disposal within the life cycle.
- Outline processes for the acquisition, secure storage, processing, and transmission of PII data.
- Emphasize compliance with data protection regulations throughout the entire life cycle.
- Incorporate mechanism for on-going risk assessment and mitigation at each stage.
- Implement access controls, encryption, and anonymization techniques to safeguard PII.
- Regularly review and update the data life cycle to adapt to changing regulatory requirements.
- Ensure secure disposal procedures for PII data at the end of its life cycle.

6.3.8. Data Discovery, Classification Lineage and Data Flow Mapping

- Identify internal and external sources of personal data collection, processing mechanisms of such personal data, storage locations (physical and system), onward transfers (internal/external), access and deletion to the said personal data in all the products & processes of the bank.

- As per DPDP Act 2023 and DPDP Rules 2025, Data Dictionary to be reviewed from personal data perspective, based on Industry practice.
- Review the existing Data discovery solution and may utilize the same in the data mapping exercises with seamless integration, to identify and document personal data held within the organization's systems and processes.
- Create / Review of data flows from DPDP Act 2023 & DPDP Rules 2025 compliance standpoint and ROPA (Records of Processing Activities) Sheet for Data Mapping.
- Explore existing process for data lineage and recommend changes.
- Design and develop processes to ensure periodic updation and review of the personal data inventory with documentation demonstrating alignment with regulatory/statutory standards. Design and develop Data Discovery templates for the Bank.
- Review existing practices and guide Bank to assess, establish and improve the data quality standards and processes across the organization to comply with DPDP Act and Rules.
- Study and assess the Bank's existing IT environment, applications, databases and data repositories to recommend the most appropriate architecture and approach for implementation.
- Clearly outline and document all stages of personal data lifecycle along with the controls implemented across each stage of the data lifecycle (in the form of DPIA / ROPA/Dataflow diagrams - where applicable and required).
- Highlight the risks identified during review of the personal data lifecycle covering relevant processes such as change management processes, etc.
- Bidders need to factor required data discovery tool/s for the project.
- Bidders need to review existing IT architecture and provide any gaps in relation to DPDP Act 2023 & DPDP Rules 2025.
- Bidders need to discover the present processes undertaken by Bank in connection with security safeguards to prevent personal data breach and finding of GAPS and suggesting solution.

6.3.9. Implementation Support: Current state assessment and actionable as per defined Privacy Framework Implementation shall include the following:

- Create organizational privacy vision and mission statement. Formulate privacy governance models.
- Data privacy operational support for remediation of gaps identified in current state phase of the data privacy initiative.
- Establish the structure in formation of privacy governance structure.
- Provide implementation assistance for operationalization of business processes by processing personal data.
- Operationalize consent management process across channels such as applications and services

- Operationalize procedure for receiving Data Principal Rights request and grievances.
- Operationalize Data breach management process
- Provide support for any privacy tool/ technology implementation.
- Conduct and support Periodic Data Privacy Audits
- Develop/ update Data Inventory and DFDs based on changes in the data privacy framework/ process/ technology.
- Perform period Data Protection Impact Assessments for in-scope departments, products, processes and applications
- Perform data processing agreements/ contracts from a data privacy standpoint.
- Privacy by default and Privacy by design in Bank's new projects
- Any other actionable/implementation to be done as per the requirement of DPDP Act 2023 and DPDP Rules 2025 and government/regulatory guidelines.
- Conducting internal readiness assessments and mock audits.
- Providing documentation, evidence, and compliance reports required for independent audits.
- Supporting closure of gaps identified during internal reviews or external audits.
- VA/PT/IS Audit observation/Periodic Data privacy audit/Independent Audit etc. till closure.

6.3.10. Training and Awareness

- Design/Review a comprehensive training and awareness program that will help Bank to drive privacy first culture across the organization.
 - Conduct training sessions (in person or virtual) to educate the Bank stakeholders about the Privacy framework, policies, and processes.
 - Develop training materials including mailers, Privacy posters and training deck for Bank.
 - Knowledge Transfer and Handholding to Bank officers for the proposed solution tools for day to day Technical and functions operation (This should include but not limited to Training sessions (online/ offline), broadcast messages, Quiz, Table top exercise, Mock drills etc., on periodically basis during the contract period)
- a) **Functional Training for users :** Onsite functional training program for the 30 users of the proposed solutions implemented in the Bank
- b) **Technical Training:** One (1) week onsite training program to Bank team for Knowledge transfer, handholding and handover of tools implemented. The training shall cover:
- i) System architecture and deployment model
 - ii) Functional workflows
 - iii) Consent lifecycle management
 - iv) Regulatory compliance features
 - v) Integration framework

Signature of the Bidder with company Seal

- vi) Security controls and audit logs
- vii) Incident handling and reporting mechanisms
- c) **Documentation Deliverables:** Bidder shall provide comprehensive documentation in editable soft copy format (MS Word / PDF) including:
 - i) Functional User Manual
 - ii) Technical Architecture Document
 - iii) System Administration Guide
 - iv) Standard Operating Procedures (SOPs)
 - v) Frequently Asked Questions (FAQ)
 - vi) Integration Guide
 - vii) Regulatory Compliance Mapping Document
 - viii) Training Presentations and reference materials. All documentation shall become property of the Bank and shall be reusable and modifiable without restriction

6.3.11. Maintenance Support:

Support to continuously maintain Bank's compliance with DPDP guidelines during the contract period with update in government/data protection board/any other regulatory body's policies/guidelines during contract period.

Additional instructions for all activities mentioned in the scope of work:

- Create, review, modify, and update all policies and procedures as per the requirements of the Act. Developing detailed RACI/Roles and responsibilities matrix for each policy/ SOP drafted/updated.
- Review of existing Policies such as but not limited to Bank's Policy on Record and Data Retention, Outsourcing Policy along with related Procedures/ SOPs, Information Security and Cyber Policy, IT and SOP, etc with reference to DPDP Act 2023 and Rules 2025 compliance and provide recommendations for updating the documents.
- Incident Response Plan Review & Recommendation for compliance from DPDP Act 2023 and Rules 2025 perspective and suggest suitable changes.
- Propose modifications to existing processes, IT systems or suggest for new solution requirements and assist in review and implementation as required to ensure effective implementation of consent, data principal rights management systems, Grievance mechanism and any other system as per DPDP Act 2023 and Rules 2025 requirements.
- Identify and connect with various departments/business functions to determine and communicate their accountability and responsibility with respect to above existing/new implementation.
- Assessing privacy enhancing technologies and involve in implementation with respect to any of the data privacy domains and may require in future as per Rules prescribed.

- Obtaining signoffs from relevant stakeholders on the completed deliverable/proposed implementation steps/recommendations.
- As part of overall Privacy framework of the Bank, assess DPDP Act 2023 and Rules 2025 compliance requirements from foreigners' data processing/ Indian residents data processed outside India.
- Actionable/Implementation to be in compliance with existing regulations impacting banks.
- During the contract period, any new rules/guidelines issued on DPDP Act 2023 and Rules 2025 issued by GOI/regulators/statutory bodies, are to be covered by the Bidder without any additional cost to the Bank.
- Preparation of periodic privacy decks for user awareness across Bank.
- VAPT/IS Audit Observation closure.

6.4. Technical & Functional Scope for Data Privacy and Consent Management Solution and Other privacy Applications/Platforms

The following data protection & privacy modules are required in the Privacy & Consent Management Tool for India DPDPA 2023 & DPDP Rules 2025:

6.4.1 Consent Management Solution

6.4.1.1 Granular Consent Management

- Configure consent capture for onboarding, account opening, service enrolment, marketing, profiling, analytics, cross-sell, data sharing, call-centre capture, branch-assisted capture, partner journeys, and employee or vendor use cases where required.
- Implement multilingual consent notices and capture journeys with version control, legal and compliance approval, and linkage to channel, business purpose, product, and customer segment
- Propagate consent status to upstream / downstream systems through APIs, events, and batch interfaces so that processing is allowed, suppressed, restricted, or refreshed based on valid consent state.
- Provide mechanisms for granular consent at the Unique Customer Identification Code (UCIC) level, ensuring purpose specific Consent Management as per Clauses of DPDP Act 2023 and DPDP Rules 2025.
- Enable explicit & Affirmative consent collection, storage, and retrieval. The solution shall not implement pre-selected consent options, bundled consent, or default consent mechanisms. Every consent must be obtained through a clear, distinct, and affirmative action by the Data Principal for each specific purpose.
- Proposed solution shall enable users to set granular preferences for purposes like data sharing, marketing communication.
- Support for incorporating consent templates based on business requirements.
- Design, collect and manage consents as per DPDP Act, 2023, DPDP Rules and other relevant regulatory requirements for ex. Reserve Bank of India (RBI), Insurance Regulatory & Development Authority of India (IRDAI), UIDAI etc.

Signature of the Bidder with company Seal

- Support for hierarchical consent structures based on purposes and user attributes.
- Maintain Consent record with Mode/Channel, timestamp, purpose, and data shared etc.
- Track Consent revocation tracking and enforcement for the consent.
- The consent management platform shall be capable of integrating with any consent infrastructure, framework or interoperability standard that may be notified, prescribed or adopted by the Government of India or any competent authority in future. Whenever a customer withdraws, modifies or when a consent expires, the updated consent status shall be automatically reflected in all connected applications, systems, channels and data repositories within the time period specified by the Bank. The Bidder shall ensure that all integrated systems are updated with the latest consent status and shall maintain a complete audit trail of all such updates.
- Consent collection in the platform should support all three modes of Personal Information input Digital, Physical that is digitized subsequently, through third party agencies collected in physical / digital format-on behalf of the Bank, while maintaining appropriate audit trails, digital personal data, including personal data initially collected in physical form and subsequently digitised
- Support for incorporating consent templates based on business requirements.
- Implement mechanisms for obtaining digitally verifiable Parental/ Guardian consent for minors as per the DPDP Act.
- Implement mechanism for obtaining digitally verifiable consent from Persons with Disability (PwDs) and illiterates persons requiring assisted or supported consent mechanisms.
- Migration and validation of existing Consent Captured in various applications.
 - The solution shall support integration with Data Privacy and consent management Solution to associate each identified personal data element with its corresponding consent status, processing purpose, and validity lifecycle.
 - The platform shall enable identification of data processed without valid consent and support enforcement actions where consent is withdrawn or expired.

6.4.1.2 Consent Lifecycle Management & Auditability

- Should facilitate automated consent lifecycle management, including:
 - Collection, storage, Renewal, revocation, logs, security (immutability), and auditability.
 - Coverage across digital, physical and hybrid (phygital) journeys.
- Centralized repository for managing user consents.
- Maintain an audit trail of consent records, including timestamps, purposes, associated processing activities as required under DPDP Act 2023.
- Ensure that all records relating to consent are securely maintained in a manner that can be produced and relied upon for audit, regulatory inspection and legal proceedings, in accordance with applicable law.
- Implement consent retention and expiration mechanisms as per legal and regulatory requirements.

- Notification Engine for trigger necessary communications (email/SMS/Whatsapp/in-app) for expired/expiring consent.
- Capability to rollout Privacy Notices in all Regional languages mentioned in Schedule 8 of Indian Constitution to legacy/Existing customers digitally and record/store their consent.

6.4.1.3 Notice & Transparency Mechanisms

- Ability to generate customizable & dynamic notices tailored to different products and journeys.
- Provide downloadable consent receipts/artefacts for transparency.
- Ensure translation and transliteration of notices into all Regional languages mentioned in Schedule 8 of Indian Constitution.
- Provide banking options (logos & themes) to relate with the Bank's design language.

6.4.1.4 Version Control

- Maintain version control for all notices generated within the user journey.
- Record and store multiple versions of consent agreements and maintain historical consent changes for audits.
- Audit trail for all consent related activities and same cannot be altered.
- Ensure identification and notification of Data Principals who consented to outdated versions.

6.4.1.5 Integration & Centralized Consent Management

- Integrate seamlessly with third-party systems/Consent Management Platform as per DPDPA Act 2023/ UIDAI/ Digi Locker/ IRDAI/ any other platform mandated by Government of India or other Statutory Bodies to centralize consent and preferences records and ensure consistency across platforms.
- Maintain a centralized repository for consents and preferences collected via third-party platforms.
- Enable syncing of updated consent records with internal and external systems.
- Platform must support multi device and multi-channel consent synchronization across web, app, kiosk, chatbot and future digital interfaces to ensure consistency and compliance across all user touch points.
- Implement robust security measures such as encryption, access controls, and secure data handling practices to protect consent artefacts/ user data.
- The solution should be scalable to handle increasing volumes of consent data as the organization grows.
- Provide an intuitive interface for users to easily manage their consent preferences.
- Ensure clear and transparent communication with users regarding their consent choices and data usage

6.4.2 Cookies Consent Management

6.4.2.1 Cookie Scanning and Categorization

- Discover and catalogue cookies, scripts, tags, trackers, and similar technologies across the Bank internal and external applications.
- Classify cookies by purpose, duration, first-party or third-party origin, business owner, and data category collected
- Implement configurable cookie banners and preference centres with category-based controls for necessary, analytics, personalization, advertising
- Maintain audit-proof records of cookie, preferences recorded
- Auto-Scanning of sub-folders and sub-domains of the website and extracting cookies.
- Auto-categorization of cookies into essential, functional, analytics, marketing and performance.
- Auto-blocking of cookies, including 3rd party scripts and tags, based on consent provided by the user.
- Cookie consent and preference management

6.4.2.2 Cookie Banner

- Customizable banner template.
- Support multilingual deployment of approved translated content in English and such Eighth Schedule languages as required by the Bank

6.4.3 Record of Processing Activities (ROPA)

- Enterprise ROPA & Risk Management Solution: Deliver and configure a comprehensive Records of Processing Activities (ROPA) solution covering all applications, systems, business processes, and third-party vendors across the enterprise. The solution shall maintain a centralized and structured inventory of all personal data processing activities and incorporate processing risk assessment (DPIA) as an integral component of the ROPA framework to ensure visibility of associated privacy and data protection risks in alignment with the DPDPA Act and Rules.
- Implement structured workflows to capture, validate, review, and approve processing records. Assign clear ownership to designated responsible departments/functions, ensuring defined accountability and oversight.
- Provide workflow-based data collection from business owners, application owners, and support functions
- Link RoPA records with applications, interfaces, notices, consents, third parties, assessments, incidents, and remediation items.
- Automate the generation of statutory registers, processing assessments, and risk reports. Capture key attributes including processing purposes, data categories and elements, recipients/processors, cross-border transfers, retention schedules, and implemented safeguards in alignment with Bank's Policy, DPDPA Act and DPDPA rules requirements.

- Configure automated risk triggers for qualifying changes (e.g., new purposes, personal data categories, transfers etc.), initiating or refreshing DPIAs with RBAC-based approvals, evidence capture, and dashboard visibility, aligned to SDF obligations.
- The Bidder shall ensure that the RoPA is automatically updated, wherever technically feasible, whenever there are changes to processing activities or key processing attributes.

6.4.4 Data Discovery, Inventory and Classification and Data flow Mapping

6.4.4.1 Data Catalogue

- Discover personal data across databases, files, emails, endpoints, collaboration systems, cloud repositories, backups, and archived environments
- Organize personal data assets across structured and unstructured formats.
- Seamless cataloguing of personal data across cloud storage platforms and on premise storage.
- Supports unstructured files, RDBMS, and data warehouses IBM DB2, Databases like MSSQL, Mongo DB, Oracle etc. (The list is illustrative and not exhaustive. The solution must support all in-scope systems and repositories identified by the Bank during implementation including legacy systems and future equivalent technologies identified by the Bank during implementation) for a complete view.
- The solution shall provide a centralized data catalogue to organize personal data assets across structured and unstructured environments, including file systems, databases, cloud storage platforms, and data warehouses.
- The catalogue shall support full enterprise coverage across on-premises and cloud environments, including but not limited to file shares, collaboration platforms, relational databases, NoSQL databases, and data lakes.
- All personal data, sensitive customer data, transactional data, logs, metadata and outputs generated under the proposed solution shall ordinarily be stored, processed and analysed within infrastructure located in India. Any cross-border processing, remote access, support intervention, or transfer of personal data or metadata shall be permitted only where (i) legally permissible under applicable law including the Digital Personal Data Protection Act, 2023, (ii) compliant with applicable regulatory requirements of the Reserve Bank of India, and (iii) subject to written communication to the Bank, with full audit trail, encryption, and contractual safeguards

6.4.4.2 Data Lineage

- Tracks personal data lineage across internal systems and 3rd parties.
- Create lineage diagrams basis the detection of data flow.
- Automatic Identification, classification and Metadata tagging of personal data of Children (minors below 18 years) and persons with disabilities who require guardian consent

6.4.4.3 Data Discovery & Classification

- Existing Data discovery solution may utilize for Data Discovery, Data Classification and data mapping exercises with seamless integration.
- Identifies and categorizes personal data of higher sensitivity, confidentiality, risk or criticality elements continuously with high accuracy, especially for Indian PII across structured and unstructured data without reliance on sampling methodologies for unstructured data, ensuring complete data visibility across file systems, databases, cloud environments, and collaboration platforms.
- Unstructured data to include PDF, Images, XLSX, DOCX, etc.
- The solution should have various pre-built patterns for DPDPA and Indian Banks like PAN, Aadhaar, GST, Indian Passport Number, Indian Driving License, Indian Mobile Phone Number, Indian Address, Credit Card Number, Credit Card Pin, Credit Card CVV, SWIFT, IBAN etc.
- The system should accurately identify historical versions of Indian-specific identifiers such as Aadhaar, PAN, Voter ID, Driving License belonging to all Indian states, etc.
- Tags personal data within the organization-wide data dictionary.
- The solution should also support usage of custom policies by creating patterns via regular expressions, keywords/dictionaries.
- Solution should not be having any limitation on nested files and folders which discovering critical information.
- Solution should also support Optical character recognition for detecting sensitive information in images.
- The solution should provide options to customize discovery policies through proximity based search (Look for content next to specific keywords/patterns)
- Solution should be able to discover the content based on last modified date, creation date, file size, file type.
- Solution should be able to discover content based on Metadata, file names, header & footer in documents.
- Solution should also support various predefined file types and also can include custom file types which needs detection for sensitive information.
- The solutions should provide data classification policies based on regex patterns, positive and negative keywords as well as algorithmic validators like Luhn, GST Checksum, Verhoef and BIN where possible to discover and classify sensitive columns.
- The solution should have options for incremental scanning to ensure we do not do full scans always. The solution should do incremental scans in real time once any modification is seen on the files, incremental scans should not be scheduled.
- Scans needs to detect real time changes to data and ensure its current and latest Status.
- Solution should also support on demand scans for specific locations/drives/folders for specific data type. This scan should not impact the overall scan running on the entire data store and should provide results along with environment wide scan results.
- Solution should also be capable of integrating with structured data stores/databases. The databases could be on premise like MS SQL, MySQL, Oracle, PostgreSQL, MongoDB, DB2 etc.

- Solution should be able to provide custom scoping to scan dedicated area on the databases, rather than scanning the entire database.
- Solution should support file analysis module where analysing actual content from files should be available which are classified against a data type.
- Solution should provide capability to analyse and map permissions incrementally. Like the any permission changes (physical or effective) solution should be able to map the new permissions immediately to keep the data updated on console and in reporting.
- Solution should provide complete visibility on all users who have access to specific data types with complete permissions assigned to
- Solution should provide visibility to all files and folders a user can access on integrated data stores irrespective of data types.
- Solution should discover the actual roles and assigned permissions with having general view to show the user/roles has the full control, creation, Read, write etc on every data store. The solution should incorporate classification information into permissions reports, ensuring a comprehensive overview of access levels linked to data classification.
- It must offer various interactive, graphical view types, including hierarchical and list views, enabling flexible and intuitive data navigation.
- The solution should provide only specific roles to analyse actual files
- The solution should provide comprehensive reports to track discover tasks.
- The solution should report multiple/all sensitive data types identified in a single file, for instance if a file has PCI, PII, HIPAA and credentials all these data types should be reported against the single file.
- Solution should provide reporting on PII data which is created, deleted, modified on specific date and also in a time range.
- Reports can be exported in CSV, XLSX, PDF formats and must also be scheduled on custom filters to get them on emails by all relevant stake holders.

6.4.4.4 Endpoint discovery

- Cataloguing and classification of endpoint devices.
- Support from Windows 8 to the latest Windows version, MacOS, Linux, and Ubuntu.
- Unified endpoint management using mobile device management.
- Ability to set up and manage policies for endpoint devices.

6.4.4.5 Data Inventory & Tagging

- Maintains an inventory of personal data for compliance and governance.
- Captures and maintains metadata for each data element, including creation date, modification history, data owner, classification and sensitivity level.
- Links the Data Dictionary with assessment automation for streamlined compliance workflows.
- System should involve third party processors handling PII data, cross border transfers and data retention checks to initiate the assessments.

Signature of the Bidder with company Seal

6.4.4.6 Secure Deployment

- Single-tenant configurations ensure secure, isolated environments for enhanced data protection.
- Capability to discover personal data from central servers, all databases, and all storage systems.

6.4.4.7 Integration between Data Discovery and Consent Management

- Ability to map data assets to one or more business processes.
- Integration to ensure the business process is in sync with the data assets across the organization.

6.4.4.8 Data Privacy/Security Posture Management

- Platform must have the ability to provide data security posture and access governance capabilities.
- The bidder shall deploy a Privacy Threat Modelling solution supporting DPDP-compliant methodologies (e.g., LINDDUN or equivalent/higher) to analyse privacy threats across data collection, storage, processing, and sharing stages.
- The solution shall model and assess privacy threats related to insider misuse, unauthorized access, third-party data leakage, profiling risks, and excessive exposure of personal data.
- The solution shall enable simulation and evaluation of privacy risks in Data Principal Rights fulfilment processes.
- The solution shall provide structured risk scoring, impact analysis, and mitigation recommendations for identified privacy threats.
- The bidder shall privacy management platform integrating automated consent tracking, purpose enforcement, data minimization, and privacy monitoring across systems in alignment with the Bank's Policy, Digital Personal Data Protection (DPDP) Act, 2023 and DPDP Rules, 2025
- Consent-based access control using encryption, tokenization, and masking
- Technical safeguards for limited consented processing
- Technical safeguards for exempted continuous processing
- Technical safeguards for continuous processing like AI and 3rd-party sharing (Expert anonymization, Differential Privacy, Synthetic Data)
- Data retention, encryption/tokenization, and erasure procedures
- Segregation of test and production data
- Privacy implementation methods (synthetic data, PETs) in non-production environments
- Conversion of identifiable/relatable data into unrelatable data to minimize compliance exposure
- Protection beyond Confidentiality, Integrity, Availability (CIA) risks for continuous processing

Signature of the Bidder with company Seal

6.4.4.9 Data Flow Mapping

- End-to-end data flow diagrams and cryptographic architecture.
- Standardized Data Flow Diagram (DFD) conventions, modelling templates, documentation standards, etc.
- Prepare a detailed data flow analysis covering below
 - data entry and egress points,
 - mechanisms for handling, storage, and sharing,
 - access rights and privileges,
 - data classification based on Bank policies,
 - security protocols for data in transit, in use, and at rest, and
 - Platforms used for data sharing (e.g., Secure File Gateways, SFTPs, SharePoint, Emails, etc).
- Review departmental/branch storage mechanisms including endpoints (local systems) and file servers, analyse types of stored data and its security posture.

6.4.5 Data Privacy Assessment of Applications

6.4.5.1 Core Privacy Assessment Features

- Privacy Impact Assessments (PIAs):
 - Automated workflows for conducting PIAs.
 - Built-in templates aligned with DPDPA
 - Risk scoring and mitigation recommendations.
 - Integration with data maps and business processes.
- Assessment Assignment & Response Tracking:
 - Ability to assign assessments to projects or data assets.
 - Role-based access for stakeholders to complete and review assessments.
 - Audit trails and exportable reports.
- Customizable Assessment Templates:
 - Create assessments tailored to specific data uses or business units.
 - Modify built-in templates to suit organizational needs.
 - Support for multilingual and region-specific compliance.
 - Compliance & Risk Management Features
- Consent Management Integration:
 - Track and manage user consent across platforms.
 - Support lawful collection and processing of personal data by enabling consent management, purpose mapping and auditability
 - Real-time updates for regional compliance
- Vendor Risk Management:
 - Assess third-party compliance posture.
 - Automate vendor assessments and reporting.
 - Maintain records of vendor data handling practices.
- Incident & Breach Management:
 - Real-time alerts and breach notification workflows.
 - Regulatory reporting templates.

- Post-incident analysis and remediation tracking.

6.4.5.2 Operational & Strategic Features

- Role-Based Access & Governance:
 - Define roles like Privacy Curator, Data Curator, and Privacy Reader.
 - Control who can create, edit, approve, or view assessments.
- Automated Compliance Workflows:
 - Trigger assessments based on privacy rules or data conditions.
 - Integration with CRM, ERP, core banking application and data governance platforms.
 - Continuous monitoring and compliance scoring.
- Reporting & Analytics:
 - Dashboards for privacy metrics and compliance status.
 - Exportable reports for audits and board-level reviews.
 - Benchmarking against industry standards.
- Identify Gaps, establish, track, monitor and report privacy assessments of all products/applications in the Bank with automated MIS Reporting.
- The bidder shall deploy a Privacy Threat Modelling solution supporting DPDP-compliant methodologies to analyse privacy threats across data collection, storage, processing, and sharing stages
- Maintain evidence, comments, review history, sign-offs, and periodic reassessment capability.

6.4.6 Data Principal Rights Management/Facilitation

6.4.6.1 Rights Management & Request Handling

- Portal for Data principals to view and manage their consents.
- Data principals should be able to download a copy of their consent history.
- Enable mechanisms for Data Principals to raise requests under all rights encapsulated in DPDPA, including:
 - Right to Access Consent
 - Right to revoke Consent
 - Right to Correction and Erasure of Data (Section 12), including third-party workflow integrations
 - Right to Grievance Redressal
 - Right to Nominate (in the event of death or Incapacity) – Allow to Nominate, modify or revoke a nominee, enable nominees to access withdraw, erase. Etc as per DPDP Act.
 - Ensure clear and transparent communication with Data Principals throughout the request process.
 - Life cycle from invitation to closure.
 - The rights management workflow shall be configured to enforce response timelines in strict conformity with the timelines prescribed under DPDP Rules 2025 as amended from time to time. Any statutory

amendment to response timelines shall be implemented in the system within 30 days of such amendment at no additional cost to the Bank.

6.4.6.2 Workflow Automation & Compliance Adherence

- Implement internal workflows to receive, process, and respond to Data Principal Requests efficiently with upstream and downstream applications.
- Orchestration of SMS / Email/Whatsapp/in-app notifications to Data Principals via communication gateways/Mobile Banking/Internet Banking etc.
- Ensure view consent and revoke consent request could be handled in a self-serve manner to reduce number of tickets to be handled by privacy team or DPO's office.
- Workflow management should be configurable to streamline the entire process from intake till fulfilment.
- Seamless integration with existing systems and data sources to facilitate efficient data discovery and retrieval.

6.4.6.3 Integration & Multi-Level Workflow Capabilities

- Orchestrate data deletion requests between the Fiduciary and the Data Processors. Enable authorised Bank personnel to verify consent artefacts and discover Personal data relating to the deletion request and take appropriate action.

6.4.6.4 Tracking, Reporting & Auditability

- Maintain a centralized register/tracker to record all Data Principal Requests, responses, and resolution times, demonstrating compliance.
- Securely log and track all requests to enable verification, audits, and regulatory reporting.
- The solution shall provide configurable internal workflow SLAs for acknowledgement, routing, escalation, tracking and closure of Data Principal requests, together with automated alerts and dashboard monitoring, so as to enable the Bank to comply with applicable statutory and regulatory timelines.

6.4.7 Data Protection Impact Assessment (DPIA)

6.4.7.1 Comprehensive DPIA Templates & Workflows

- Provide standardized templates and workflow support for conducting and documenting Data Protection Impact Assessments (DPIAs), wherever required under applicable law, regulatory requirements, the Bank's policies, or risk-based internal governance covering
 - Description of processing activities, including involvement of third parties.
 - Risk assessment matrix to evaluate risks and automated risk calculation & Categorization of all products/process wise.
 - Regulatory and industry specific DPIA templates, customizable as per business needs.

- Automation & Workflow Management
 - Enable multi-level workflow capability to facilitate role-based access, permissions, and approvals.
 - Allow customization of roles, permissions, and review processes to align with organizational structures.
 - Support auto-reminders, query escalation, and follow-ups to streamline DPIA completion.
 - Provide the ability to upload supporting documents and artefacts when responding to specific queries.
- Periodic & Proactive Assessments
 - Support periodic DPIA reviews to ensure ongoing compliance with regulatory requirements.
 - Proactively launch assessments for new business processes, with a timeline view for accountability and visibility.
- Collaboration & Vendor Engagement
 - Enable seamless sharing of DPIA assessments with data processors and vendors, ensuring end-to-end compliance.
 - Provide functionality to add team members and external stakeholders for collaborative assessments.
- Smart Assessments
 - Auto-fill assessments using AI leveraging knowledge base of consent artefacts, processors, configurations and data discovery findings.
 - The selected bidder warrants that any embedded artificial intelligence, machine learning models, or natural language processing libraries used within the platform strictly adhere to the Central Bank of India's internal Artificial Intelligence Policy and algorithmic security baselines. The vendor must support periodic, independent vulnerability testing and code reviews of the underlying models at no additional cost to the Bank.
- Assess necessity, proportionality, data categories, risk to Data Principals, control adequacy, residual risk, and mitigation actions.
- Enable review by business, compliance, legal, information security, architecture, risk, and privacy stakeholders
- Link DPIA outputs with RoPA, controls, notices, consents, vendors, and remediation plans.

6.4.8 Privacy Notice Management

6.4.8.1 Notice & Transparency Mechanisms

- Implement central authoring, review, approval, publication, archival, and retirement of privacy notices, layered notices, just-in-time notices, and channel-specific privacy text.
- Ability to generate customizable & dynamic notices tailored to different products and journeys.

- Provide downloadable consent receipts/artefacts for transparency.
- Ensure translation and transliteration of notices into all 22 Indian languages as per Schedule 8 of the Constitution. Support translation/transliteration of privacy notices into languages required by the Bank, including languages specified under the Eighth Schedule of the Constitution, based on customer requirements.
- Provide banking options (logos & themes) to relate with the Bank's design language.

6.4.8.2 Version Control

- Maintain version control for all notices generated within the user journey.
- Record and store multiple versions of consent agreements and maintain historical consent changes for audits.

6.4.8.3 Audit & Reporting

- Audit trail for all consent related activities and same cannot be altered.
- Ensure identification and notification to Data Principals who consented to outdated versions.

6.4.9 Data and Privacy Breach Management

- Support intake, triage, severity classification, affected-record estimation, root-cause analysis, containment actions, remediation, and closure.
- Provide workflows and alerting for reporting cyber incidents to CERT-In within 6 hours of noticing or being informed, where applicable under CERT-In directions.
- Support DPDP-related notification workflows to affected Data Principals and the competent authority in the prescribed manner, including templates, approvals, and evidence. Support breach notification workflows to the Data Protection Board of India and affected Data Principals in the manner prescribed under the DPDP Act, 2023 and DPDP Rules, 2025, and to CERT-In where applicable.
- Implement end-to-end privacy incident and personal data breach management integrated with the Bank's cyber incident response, SOC and other related applications / functions.
- The workflow of breach investigation & intimation should align the requirement as per Rules of the DPDP Act 2023 & Rules 2025.
- Seamless reporting to the Data Protection Board and Data Principals.
- Maintains a repository of pre-approved templates for quick and compliant breach reporting.
- Document steps taken to contain the breach, ensuring transparency and trust.
- Send initial and final breach reports to both impacted Data Principals and Data Protection Board.
- Maintain a comprehensive audit trail of all breach-related actions for demonstration of compliance. The solution shall automatically generate the information required for regulatory notifications, identify affected Data Principals, provide workflow-based approvals, and maintain real-time monitoring of applicable statutory notification timelines until closure of the incident.

- Create cohorts of Data Principals to ensure that the notification is only going out to the affected Data Principals.
- Automated breach notices sent to impacted Data Principals within the timeframe as defined by DPDPA Act and rules 2025.
- Configurable templates for breach intimation, ensuring compliance and clarity.
- Suggest remedies to impacted Data Principals to mitigate risks.
- Show steps taken to contain the breach, ensuring transparency and trust.

6.4.10 Compliance Monitoring, Reporting and Governance Dashboard

- Centralized Compliance Dashboard for DPO and Privacy Stewards / Nodal Officer.
- Real Time Monitoring: Dashboard should provide real time Visibility into the initiation, review, approval and closure of DPIAs across all Branches and Business functions.
- SLA Based Time Tracking: The tool must include automated time tracking of each DPIA process step, with configurable Service Level Agreements (SLAs) and dynamic indicators (e.g. red/yellow/green flags) for SLA compliance.
- Alerts and Escalations: Support for automated alerts and escalations to DPOs, Privacy Stewards, or relevant functionaries in case of SLA breaches or pending approvals.
- Branch Wise & Function Wise Compliance Overview: Ability to generate compliance scorecards and dashboards for each branch, Region, Zone, Department or business Vertical.
- Role-Based Access Controls (RBAC): The system should allow differentiated access for
 - DPO – Global access with configuration and oversight privileges
 - Privacy Stewards/Nodal officer – Access to DPIAs within their assigned branches/Verticals
 - Branch/Region/Zone – Access to DPIAs initiated or owned by their teams
- The platform must be scalable to on-board all branches and new privacy stakeholders as per future organizational requirements
- Solution should provide Data Privacy awareness dashboard.

6.4.11 Third Party Risk Management

- Implement inventory and lifecycle management for all vendors, processors, sub-processors, cloud providers, outsourcing partners, and service providers handling or accessing personal data
- Record services, systems accessed, personal data categories handled, processing purpose, hosting location, sub-contracting, incident history, and contract status
- Provide due diligence questionnaires for privacy, security, breach management, retention, subcontracting, log maintenance, incident reporting, audit rights, and legal compliance
- Support inherent risk scoring, control evaluation, residual risk scoring, onboarding approval, periodic reassessment, and offboarding workflows
- Track contract clauses relating to confidentiality, purpose restriction, breach reporting, deletion or return of data, audit rights, processor obligations, and support for Data Principal request handling

Signature of the Bidder with company Seal

- Integrate third-party incidents, findings, certifications, assessments, and remediation status into a single risk dashboard
- Integration with existing vendor management and contract management systems.
- Create an audit trail with data processors to ensure compliance as per consent updation/revocation by data principal.
 - Ability to Raise Deletion requests to Processors
 - Route deletion requests from Data Principal Rights Management to processor (Manual and auto)
 - Ability for Data Processors to acknowledge, upload proofs and comply with deletion requests
- Create, assign Third party risk assessments to vendors and manage the lifecycle.
- Measure compliance with Data Sharing Agreements.

6.4.12 Integration of System

- Proposed solution shall have capabilities to integrate with existing systems like Mobile banking, Internet banking, CBS, various digital and other journeys initiate by the Bank.
- APIs shall be used for seamless integration with internal and 3rd party systems.
- Other systems to be able to get real-time status of consent via API integration.
- The consent artefact should be available in JSON, Xml etc format, so that it can be integrated with other systems.
- Consent governance and Data principal rights management portal must be integrated.
- Consent governance and Breach intimation modules must be integrated.

6.4.13 Security and Compliance

- Ensure encryption of all personal data and Bank confidential information at rest and in transit.
- Comply with industry-standard certifications (e.g., ISO 27001, SOC 2 Type 2).
- The tool should support standard authentication with OAuth 2.0 / SAML.
- Solution should be accessible from any network, but should allow restricting access to a definable corporate network range for specific populations of users (applicable for all applications for Data Fiduciary facing).
- Connection/Transmission to the on-prem applications should be over encrypted channel.
- Solution shall have data encryption (at rest and in transit).
- All confidential information such as passwords, Security Questions/Information should be over secured encrypted channel.
- System should support setup of password policy and enforcement, MFA enforcement, role-based access control, maker-checker for setting up business processes & policies.
- Audit trail for system access should be maintained as per agreeable retention policies.
- Solution shall provide regular security updates and patches.

6.4.14 Privacy by Design

- To provide internal teams with an end-to-end mechanism for identifying personal data related changes in applications and processes and raise a Privacy by Design (PbD)

request that can be evaluated, managed and monitored by Bank privacy team as per Privacy by Design (PbD) principles.

6.4.15 Testing and Validation:

- Test cases to be prepared by bidder and to capture the testing artefacts and share it with Bank.
- Conduct performance testing of tool.
- Test the integration of the tool with critical applications, including version control systems, build systems, and issue tracking tools.
- Work with business teams to execute UAT for all integrations and releases.
- Testing shall include functional testing, integration testing, security testing, performance testing, user acceptance testing and validation of all statutory privacy workflows before production deployment

6.4.16 Reporting and Metrics:

- Set up reporting mechanisms to track key performance indicators (KPIs) and security metrics.
- Generate and distribute reports to relevant stakeholders.

6.4.17 Security Requirements:

- The tool should support standard authentication with AD / SAML.
- Support different authentication methods for different populations of users.
- Solution should be accessible from any network but should allow restricting access to a definable corporate network range for specific populations of users.
- Connection/Transmission to the on-prem applications should be over encrypted channel.
- All confidential information such as passwords, Security Questions/Information should be over secured encrypted channel.

6.4.18 Compliance and Governance

- Ensure that the tool aligns with industry standards and regulatory requirements stated in India DPDPA.
- Implement governance model.

6.4.18.1 Operational & Strategic Features

- Role-Based Access & Governance:
 - Define roles like Privacy Curator, Data Curator, Privacy Reader.
 - Control who can create, edit, approve, or view assessments.

Signature of the Bidder with company Seal

- Automated Compliance Workflows:
 - Trigger assessments based on privacy rules or data conditions.
 - Integration with core Banking application, Digital channel applications, Data warehouse and data governance platforms etc.
 - Continuous monitoring and compliance scoring.
- Reporting & Analytics:
 - Dashboards for privacy metrics and compliance status.
 - Exportable reports for audits and board-level reviews.
 - Benchmarking against industry standards.
 -

6.4.19 Implementation Deliverables:

- Maintain detailed documentation of the implementation process, configurations, version updates and any customizations made
- Detailed pre-requisites, dependencies, assumptions, risks
- Project Management Plan
- Meeting Briefings/Presentations
- Status Reports (Weekly, Monthly, Quarterly)
- Test Plan Strategy
- Test Cases (Dev, UAT & Production)
- Uptime reports
- Ensure stability of the services (including application migration/role-back plan in case of failure)
- Four Environments (Dev, UAT & Production (DC & DR))
- Create and / or update the requirement documents
- Create and/or update design document (HLD, LLD)
- Maintain the bug, lesson learn tracker (make sure it is referred at every stage of the project).
- VA & PT closure of the tool before go live in Bank DC/DR.

6.5. Project Requirements

1. Architecture Review & Approval:
 - The architecture of the proposed solution must be reviewed and approved by the Bank's Security team.
 - In case any modifications or recommendations are suggested by the EA team, the bidder shall incorporate all such changes during the design phase itself, without impacting project timelines or cost.
 - Any new Bank application, channel or business process introduced during the implementation period, which processes Digital Personal Data and is reasonably comparable in nature to the agreed implementation scope, shall be incorporated into the implementation without additional implementation

Signature of the Bidder with company Seal

charges, provided such inclusion does not require procurement of additional third-party software products.

2. Vulnerability Assessment & Penetration Testing (VAPT):

- The solution shall not go live unless all Critical and High VAPT observations are closed, and Medium/Low observations, if any, are accepted with a Bank-approved remediation plan
- The bidder is solely responsible for the first third party Cert-In Empanelled VAPT and closure of all VAPT findings related to the solution without additional cost to the bank.

3. Operating System Vulnerability Closure:

- Although the Bank will provide the underlying infrastructure (including virtual machines) for hosting the proposed solution, it is the sole responsibility of the bidder to remediate all OS-level Vulnerability Assessment (VA) observations throughout the contract period.

4. Hardware/VM Hygiene and Compliance:

- The bidder must ensure that all Hardware/VM are integrated with the Bank's centralized patch management system and antivirus solution.
- The bidder shall also ensure that:
 - ✦ Antivirus definitions are updated regularly.
 - ✦ All Hardware/VM are maintain system stability and compliance and to avoid any audit observations.

5. Audit Observation Closure:

- The bidder shall coordinate and ensure the closure of all observations raised by internal and external auditors during the contract period.
- No additional cost shall be borne by the Bank for the closure of such audit observations.

6.6. Onsite Resource Deployment and Governance

1. **On Site Resources – (Implementation):** The Bidder shall deploy adequate, qualified, and experienced on-site resources at the Bank's premises for the purpose of implementation, configuration, integration, governance, regulatory alignment, and operational readiness of the Consent & Data Privacy / Consent & Privacy Governance Platform.

The on-site implementation team shall consist of a minimum of five (5) resources. In addition to the minimum team strength, the team shall mandatorily include the following key personnel:

1. One (1) dedicated Project Manager
2. One (1) Technical Subject Matter Expert (Technical SME)
3. One (1) Functional Subject Matter Expert (Functional SME)

These resources shall be deployed on-site throughout the implementation period, or as otherwise required by the Bank. However, Bidder should deploy additional resources to achieve the milestone and timeline to avoid any delay in implementation without any additional cost to the bank.

2. On-Site Support Resources (Post go-Live) - Project Manager / Team Lead:

On-site resource proposed for post Go Live operations of the proposed solutions. The details of some of requirement are as under:

The Bidder shall deploy minimum 1 on-site Project Manager/Team to Manage the Proposed solution / application and Coordinate with the onsite team & Banks team for the operational, functional , Technical & application-level operational support for the proposed solution. The resource shall be responsible for uninterrupted application operations, functional configuration, and timely resolution of audit and compliance observations related to consent management, data principal rights, and privacy governance etc.

3. On-Site Support Resources (Post go-Live) - Application & Operation Support: On-site resource proposed for post Go Live operations of the proposed solutions. The details of some of requirement are as under:

The Bidder shall deploy minimum 1 on-site L2 Application & operation support resources per shift for three shifts per day to provide 24x7x365 end-to-end functional and application-level operational support for the proposed solution. The resource shall be responsible for uninterrupted application operations, functional configuration and timely resolution of audit and compliance observations related to consent management, data principal rights, and privacy governance etc.

The resource shall provide combined functional support for the proposed solution modules. The resource shall ensure uninterrupted functional coverage including weekends, holidays and peak regulatory periods.

4. On-Site Support Resources (Post Go-Live): Infrastructure / System Administrator/ DBA. On-site technical (infrastructure) resource proposed for post Go-Live operations. The resource shall ensure uninterrupted operational coverage. The bidder will ensure Minimum one (1) L2 Technical Resource is available per shift for three shifts per day to provide (24x7x365) and adequate no of resource at DR location in case of any Disaster/outage/downtime.

The Bank reserves the right to increase or decrease the number of deployed resources during the five-year contract period based on business and operational requirements. Any addition or deletion of resources shall be communicated by the Bank, and payments shall be made on a pro-rata basis from the date of deployment or withdrawal. The bidder shall ensure uninterrupted 24x7x365 availability of qualified resources after Go-Live. Any additional manpower required to meet support, operational, SLA, or business continuity requirements shall be provisioned by the bidder at no extra cost to the Bank and must be included in the commercial bid.

Interview and Approval by Bank: The Bank reserves the right to conduct interviews for all proposed onsite resources. Only upon the Bank finding the candidate suitable, the resource shall be formally on boarded for the project. If, at any point during the contract period, the Bank assesses that a deployed FM resource is not contributing effectively to the project or is not up to the required standards, the Bank shall issue a 30-day written notice to the bidder to initiate replacement of the said resource.

Replacement Resource Eligibility:

- The replacement resource proposed by the bidder must meet the eligibility criteria as defined in the RFP or contract.
- The replacement shall be subject to the same evaluation and interview process by the Bank, and only upon approval, the resource will be accepted and onboarded.

Education Qualification for On-site Resources:

Section	Competency / Requirement
Team Composition: Certifications (IAPP / ISACA / DSCI)	Team members certified in privacy (IAPP/ISACA/DSCI) CIPP / CIPM / CIPT (IAPP) certification
Team Composition: Technical Breadth	Team with high-level knowledge of ReST APIs, JavaScript, JSON/XML, and modern web/mobile tech (HTML, CSS, JS, Web Components)
Resource: Education & Experience	Graduate (any discipline) with experience in privacy operations solution design, implementation & management
Resource: Regulatory Knowledge	Introductory understanding of DPDPA and familiar knowledge with GDPR, CCPA, etc.
Resource: Privacy Ops Automation Experience	3+ years in design/implementation/management across: Cookie Consent, Universal Consent, Breach Management, Data Principal Rights, Privacy Notice Management, Assessment & Workflow Automation, Integrations
Resource: Infrastructure / System Administrator	3+ years of experience in management of critical Hardware Infrastructure.

S.No.	Role	Years of Experience	Working Hours
1	Project Manager / Team Lead	7-10 Yrs	Bank's Working Hours
2	Infrastructure / System Administrator/DBA. (Minimum 1 L2 Resource in a Shift)	3-7 yrs	24*7*365
3	Application & Operation Support Engineer: (Minimum 1 L2 Resource in a Shift)	3-7 yrs	24*7*365

6.7. Additional Scope of Work

- Proposed Solution shall support explicit, implicit, opt-in, and opt-out consent models.
- Proposed Solution shall have capabilities Integration with existing systems like Mobile Banking, Internet Banking, CBS, CRM, various Digital and Other Journey initiated by Bank etc. API shall be used for seamless integration with internal and third-party systems or other secure integration as per agreed by Bank.
- Proposed Solution shall Customizable consent forms like Branding options (logos, themes), Dynamic content based on user location or preferences etc.
- Proposed Solution shall record and store multiple versions of consent agreements and maintain historical consent changes for audits.
- Proposed Solution shall have Audit trails for all consent-related activities and same cannot be altered. Integrity to be ensured for the same. Further, Detailed logs of consent-related activities for audits.
- Proposed Solution shall have feature for Real-time consent updates and synchronization across systems.
- Proposed Solution shall support for hierarchical consent structures like consent for specific data types or purposes etc.
- Bidder shall provide SBOM, HBOM, CBOM & AIBOM (Software Bill of Material, Hardware Bill of Material, Cryptographic Bill of material and Artificial Intelligence Bill of Material) of proposed solution to the bank.
- Proposed Solution shall have Centralized repository for managing user consents
- Proposed Solution shall have dashboard for end-users to view and manage their consents, Download a copy of their consent history,
- Proposed solution shall enable users to set granular preferences like data sharing, marketing communications etc.
- Proposed Solution shall support for self-service consent revocation.
- Proposed Solution shall have feature for Real-time reporting on consent metrics like consent rates, revocation trends, Geographic distribution of consents etc.
- Proposed Solution shall have automated consent expiration and renewal workflows.
- Proposed Solution shall have ability to handle large user bases and high transaction volumes.

- Proposed Solution shall have Low-latency operations for real-time consent capture and verification.
- Proposed Solution shall have Data encryption (at rest and in transit).
- Proposed Solution shall have feature for secure deletion of consent records valid request or expiry of the applicable retention period or fulfilment of the purpose for which the consent was obtained, subject to applicable legal, regulatory and record-retention requirements.
- Proposed Solution shall have built-in feature for compliance with major data privacy laws.
- Proposed Solution shall provide regular security updates and patches.
- Proposed Solution shall have feature for Real-time system health dashboards.
- Proposed Solution shall have feature for alerts for failures, latency issues, or integration errors.
- The solution should support DC/DR integration and periodic DR drill execution as per the Bank's IT/BCP policy.
- The system must have the capability to adapt to any future regulatory requirements issued by DPBI/ MeitY/RBI or any Regulatory Agencies under the DPDP Act, 2023 or any relevant Act.
- Bidder shall arrange and submit to the Bank an annual Source Code Security Review and Compliance Validation Report of the proposed application, conducted by a CERT-In empanelled audit organization, covering source code security assessment, vulnerability analysis, dependency review, secure coding compliance, and validation against applicable CERT-In directions, OWASP standards, and the Bank's Information Security Policy, without any additional cost to the Bank.
- The Bidder shall, at no additional cost to the Bank, arrange and submit a compliance validation report of the proposed solution against the applicable requirements of the DPDP Act, 2023 and the DPDP Rules, 2025, together with a Vulnerability Assessment and Penetration Testing (VAPT) report conducted by a CERT-In empanelled audit organisation

Bidder should ensure that proposed solution should have capability to address the specific requirement of EASE 9.0 metrics and assist and support bank to comply the requirements.

- Customer-facing digital journeys on MB/IB with embedded consent capture (consolidated portfolio, spend analyser, net worth, loan/card eligibility, tier upgrade, salary conversion)
- Measurement of consent journey coverage and consent capture effectiveness
- Capture and maintain consent metadata (purpose tag, status, timestamp, reference ID, etc)
- Priority customer segment list for targeted consent capture
- Branch/RM-assisted consent journeys: tier upgrade, SA-to-salary, credit card, retail loan etc.(via CBS or sourcing portals/touch point)
- Enterprise-wide Consent Management Platform: repository, customer self-serve, revocation workflows, proactive notification, exception handling

Signature of the Bidder with company Seal

- Consent withdrawal enforcement and data scrubbing: stop processing, remove/scrub attributes, suppress marketing outreach
- Channel-level consent management via MB/IB for AA, DigiLocker, and bureau consents – dashboard, self-serve withdrawal, central logging and enforcement
- Internal policies / SOPs for Data Principal Rights (access, correction, deletion, withdrawal, grievance, nomination)
- DPR request tracking: resolution within 90 days (DPDP mandate) and within 30 days; average response time
- Coverage of customer consent – ratio of consent withdrawals to new consents granted in reporting period
- The vendor shall design, develop, and integrate the following consent-embedded value-added journeys on the Bank's Mobile Banking (MB) , Internet Banking (IB) platforms and other digital channels. Journeys must be accessible from a prominent location (home page tile, Offers/Insights section, or contextual prompt).
- Embed consent capture for each Account Aggregator data category at journey entry.
- Spend Analyser / Expense Insights journey: monthly spend trends across all bank accounts, category splits (groceries, fuel, travel, utilities, shopping), cash/digital/card breakdown. Consent captured before data aggregation.
- Consent captured for AA data pull from third-party FIs.

Implement tracking and reporting of consent journey metrics:

- Total customers shown the incentive journey on MB/IB landing page;
 - Customers who initiated the journey;
 - Customers who provided other-FI relationship data through the journey (active, non-expired, non-revoked consent).
- The vendor shall implement the capability to capture, store, and maintain consent metadata: purpose tag(s), consent status (active/revoked), consent timestamp, and consent reference ID etc. Every attribute must have a defined source, data owner, and intended usage documented.
 - Preferred communication channel — self-declared (MB, WhatsApp, SMS, etc.)
 - Preferred communication channel — bank-estimated (based on historical behaviour)
 - Preferred language of communication — self-declared
 - Preferred language of communication — bank-estimated
 - In addition to digital journeys, the following product-journey and branch/RM-assisted consent workflows to be implemented in various bank module
 - Implement Branch/RM Tier Upgrade journey via CBS/CRM screen or sourcing portal with explicit purpose-tagged consent capture for profile data usage in tier assessment and personalisation/marketing.
 - Implement Branch/RM SA-to-Salary Account Conversion journey with explicit consent for salary/employer data capture and use for conversion and analytics/personalisation.
 - Implement Credit Card Sourcing/Eligibility branch journey (via portal) with explicit consent for eligibility assessment, bureau pull, document verification, and

personalisation use. Portal-based sourcing must have consent linked to bureau pull and card eligibility.

- Implement at least one Retail Loan branch/RM sourcing portal journey with embedded consent for AA-based account statement retrieval used for loan eligibility/underwriting.
- The vendor shall implement an enterprise-wide Consent Management Platform as the single system of record for all customer consents across channels. The CMP must integrate with CBS, CRM, MB, IB, other digital channels, branch portals, AA layer, DigiLocker, and bureau interfaces etc.
- Implement the Enterprise Consent Repository: a single system of record storing all customer consents with: consent purpose tag, timestamp, consent status (active/revoked/expired), reference to notice version provided to customer, and consent reference ID etc. Repository must support multi-channel ingestion (digital, branch, RM).
- Implement self-serve consent management for customers on MB/IB: ability to view all active consents, modify consent preferences, and withdraw consent.
- Implement consent revocation workflow enforcement: when a customer modifies or revokes consent, the change must propagate to all relevant downstream systems within defined SLAs (immediate/T+1 for digital channels). Confirmation and audit log generated for each revocation event.
- Implement automated proactive customer notification for material consent changes: change in processing purpose, data categories, third-party sharing, retention period, or consent terms. Notifications to be delivered across email, in-app, website, WhatsApp. SOP/process documentation required.
- Implement exception handling processes for: wrong consent mapping, consent disputes, and failed revocation propagation. Exceptions must be linked to the Bank's grievance handling system with defined resolution timelines.
- Implement automated stop-processing workflow: when a customer withdraws consent, all consent-dependent data processing (profiling, personalisation, AA-based processing) ceases for that purpose within defined timelines.
- Implement automated data scrubbing/deletion workflow: upon consent withdrawal, remove/mask/anonymise consent-captured attributes and all derived stores (data marts, feature stores, analytics extracts) where legal/regulatory retention does not mandate retention.
- Implement marketing/promotional consent suppression: on withdrawal of marketing consent, automatically suppress the customer from all outbound campaigns — SMS, WhatsApp, email, app push, outbound calls, dialers, MarTech tools, and partner platforms.
- Implement MB/IB Consent Dashboard for channel-level consent management covering AA data access, DigiLocker document access, and credit bureau (CIBIL) checks. Dashboard must show at minimum: purpose, status (active/revoked/expired), and validity/expiry date for each consent.

- Implement self-serve modify/withdraw function on MB/IB for AA, DigiLocker, and bureau consents. On modification/withdrawal, customer receives a confirmation with reference ID and updated status visible immediately.
- Implement central consent log and enterprise enforcement: all consent events (grant/modify/withdraw/expiry) logged centrally with audit trail (customer ID, timestamp, channel, purpose, validity etc). Status changes propagated to AA layer, DigiLocker integration, bureau interfaces, underwriting/eligibility workflows, and CRM/analytics within defined SLA.
- The vendor shall implement a Data Principal Rights management capability enabling customers to exercise their rights under the DPDP Act. All DPR requests must be tracked with receipt and closure dates and resolved within the statutory timeline.
- Develop and implement internal policies and SOPs for all Data Principal Rights request types: access/information requests, correction/rectification, deletion/erasure, withdrawal of consent/preference changes, privacy grievance redressal, and nomination (where applicable). SOPs must define intake channels, processing steps, responsible teams, and resolution timelines.

Implement DPR request tracking and reporting capability:

- Total DPR requests received in reporting period;
- Count resolved within the timelines (90 days) prescribed under the DPDP Act, 2023, the Rules framed there under, and applicable Bank policy.
- Count resolved within 30 days;
- Average response time. System must maintain receipt date and closure date per request with auditable trail.

Implement average response time measurement and reporting for DPR requests in the reporting period.

Implement consent coverage measurement:

- Count of customers who gave active new consent in the reporting period (across any channel);
- Count who withdrew consent. Ratio to be reportable per EASE scorecard cycle.

6.8 Hardware Scope & Sizing for the Platform Infrastructure

Bidder has to provide the necessary Enterprise class Hardware, Software, Network Components, Storage Solutions, Virtualization and Containerization and required accessories for the proposed Platform Infrastructure at DC and DR location of Bank.

Bidder has to provide server racks that 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.

Note – Rack space, Network up link connectivity and power supply till rack will be provided by the bank.

Signature of the Bidder with company Seal

Indicative Infrastructure Configuration

The Bidder should consider the Bank's volumetric data, expected growth, transaction load, concurrent users, integrations, reporting requirements, data retention, high availability, disaster recovery, and all other functional and technical requirements before proposing the final infrastructure in the Bill of Material.

The Bidder may propose infrastructure specifications wherever necessary to meet the performance, scalability, availability, and service level requirements of the Bank.

The bidder shall carry out comprehensive sizing and capacity planning for the proposed solution, taking into account all infrastructure, operating system, database, middleware, application, security, monitoring, backup, patch management, and management tool requirements.

The Bidder shall ensure that the proposed infrastructure is adequately sized to support the complete solution throughout the contract period with a 10% incremental workload per year while maintaining resource utilization below the prescribed thresholds (CPU, Memory, Storage and Network utilization not exceeding 70% at any point of time).

The proposed hardware sizing shall adequately cater to the resource overheads arising from:

- Endpoint Security / Anti-Malware Solutions
- Endpoint Detection and Response (EDR/XDR) Solutions
- Security Monitoring and Log Collection Agents
- Infrastructure and Application Monitoring Tools
- Patch and Vulnerability Management Solutions
- Backup and Recovery Agents
- Privileged Access Management (PAM) Components
- Data Loss Prevention (DLP) Agents (where applicable)
- Any other software, agents, utilities, or tools mandated by the Bank for operational, security, compliance, audit, or regulatory purposes.

The bidder shall ensure that the proposed infrastructure maintains the agreed service levels, response times, throughput, and performance requirements even after accounting for the resource consumption of the above-mentioned components.

Hardware sizing shall be performed considering:

- Peak load conditions
- Growth projections during the contract period for Production environment.
- High Availability (HA) and Disaster Recovery (DR) requirements
- Security, monitoring, and management tool overheads
- Operating system and database resource requirements
- Concurrent user load and transaction volumes

The bidder shall provide detailed sizing calculations, assumptions, benchmarks, and resource utilization estimates, clearly indicating CPU, memory and storage. The Bank reserves the right to seek justification, independent validation, or revision of the proposed sizing if found inadequate during implementation, testing, or production operations.

Signature of the Bidder with company Seal

Any additional hardware, software licenses, storage, memory, CPU, or infrastructure components required due to inadequate sizing by the bidder during the contract period shall be supplied, installed, and configured immediately by the bidder at no additional cost to the Bank.

The Indicative infrastructure Configuration for the proposed solution is as follows:

Components	Indicative Configuration
Production Application Servers DC	Active-Passive in HA
Production Database Servers DC	Cluster/HA
CPU for Application Server DC	196 Physical Cores or 392 virtual Cores or equivalent with One/Multiple Node including Management / Utility Server
CPU for Database Servers DC	16 Physical Cores or 32 virtual Cores or equivalent with One/Multiple Node.
GPU (For data discovery ,classification , language translation etc)	As per the RFP Scope & requirements
Application Server Memory	1024 GB RAM DDR 5
Database Server Memory	256 GB RAM DDR 5
Operating System Disk	500 GB Enterprise class SSD with RAID 1
Application Storage	8 TB Enterprise SSD/SAN/Object Storage (expandable) with RAID -5/6
Database Storage	10 TB Enterprise SSD/SAN/Object Storage (expandable) with RAID-10
Backup Storage (immutable)	15 TB usable capacity.
Backup Software (immutable)	As per the proposed solution and licensed in the name of Bank with back-to-back enterprise/production support from OEM/providers.
Ethernet Network Interface	2x 25Gbe Gbps Network Interfaces (card level redundancy is a must)
Ethernet Network	25Gbps switches as per proposed solution requirement in redundant mode.
SAN Network	32Gbps throughput to be configured at port and switch level. Switches as per proposed solution in redundant mode.
Operating System	As per the proposed solution and licensed in the name of Bank with back-to-back enterprise/production support from OEM/providers with Patching and upgrades.
Database	As per the solution requirement and licensed in the name of bank with enterprise/production class back to back support from respective OEMs/providers.
Virtualization / Container Platform	VMware/Hyper-V/KVM/Nutanix/OpenShift or equivalent licensed in the name of Bank with back-to-back Enterprise/production class support from respective OEMs/providers.
High Availability	No Single Point of Failure.
Disaster Recovery (DR) Production	100% replica of DC Production environment.

Signature of the Bidder with company Seal

Components	Indicative Configuration
environment	
UAT Environment	It should be a separate environment with 30% of Production configuration
Development Environment	It should be a separate environment with 10% of Production configuration
Application Load Balancer	Enterprise class product with back to back support from OEM
Observability	a unified enterprise-class observability platform for monitoring all infrastructure and application components. The Bidder may leverage the Bank's existing HEAL monitoring solution and bring required licenses. Any additional observability components, licenses or OEM subscriptions required shall be provided in the Bank's name at no additional cost and support infrastructure, application, log and performance monitoring.
Comprehensive Onsite Warranty Support	5 Years, 24x7 with Enterprise Class back to back support from respective OEMs for all the products quoted under proposed Solution
Backup Network	Dedicated Backup VLAN/Network isolated from Production and Management Networks for Backup, Restore and Replication Traffic
Management / Utility Server	1 dedicated server for Solution Management Console, Monitoring, Logging, Scheduler, Configuration Management and Administrative Services.

The above specifications are Indicative Infrastructure Configuration/sizing only and shall not relieve the Bidder from its responsibility to provide adequate infrastructure based on actual sizing/ Configuration calculations and bidder is liable to meet all the SLA requirement of performance matrix at no additional cost to the Bank during the contract period.

If, at any stage during the contract period, the proposed infrastructure is found inadequate due to incorrect sizing/ Configuration, underestimation of workload, data growth, transaction volume, integrations, or any other capacity planning deficiency attributable to the Bidder, the Bidder shall, at its own cost and without any financial implication to the Bank, provide, install, configure, and commission all additional hardware, software, licenses, storage, compute resources, network components, database resources, and associated infrastructure required to meet the contractual performance and availability requirements.

No additional payment shall be made by the Bank for such augmentation, and the Bidder shall ensure that such upgrades are carried out without disruption to production services or impact on the agreed service levels and project timelines.

The proposed infrastructure sizing/ Configuration shall form part of the contractual commitment of the successful Bidder.

Signature of the Bidder with company Seal

6.8.1 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.
- Warranty that all 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 and throughout the contract period.

6.8.2 Infrastructure Sizing and Design

- Determine and provide the optimal sizing of all infrastructure components, including but not limited to:
 - Enterprise class Hardware: Servers, Processors (CPUs, GPUs), Memory, Storage etc.
 - System Software: Operating systems, Middleware, Platform Applications, Development Tools, Monitoring and Management etc.
 - Network Components: High-Speed Networking, Load Balancers, Network Segmentation, LAN / Optical Cables, Switches etc.
 - Storage Solutions: Primary Storage (SSD, HDD), Backup and Recovery, Archival Storage, Data Tiering etc.
 - Virtualization and Containerization: Virtualization Platforms, Containerization, Bare Metal Management etc.
- The infrastructure design shall align with the Bank's business objectives, scalability requirements, and Service Level Requirements (SLRs). The BIDDER shall ensure that the solution meets performance, reliability, security, compliance, and cost-effectiveness criteria.
- Provide all necessary components, tools, and utilities required for the seamless setup, operation, 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 BIDDER shall quote for dedicated infrastructure for each component listed in the Bill of Materials (BoM) , SBOM , HBOM , CBOM & AIBOM (Software Bill of Material , Hardware Bill of Materials and Cryptographic Bill of material, Artificial Intelligence Bill of Material), 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): 30% of production capacity
 - Development (Dev): 10% of production capacity

6.8.3 Leverage Bank's existing resources

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

When incorporating the Bank's existing resources, BIDDER must ensure full interoperability with the proposed solution. If this cannot be guaranteed, the BIDDER 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 Data Masking and Sub setting Pack Oracle Advance Data Guard	Oracle Golden Gate license is not available with the bank.
ITSM Tool	Motadata Serviceops	-
Anti-Virus	Trend Micro Deep security-Enterprise	-
LDAP / AD	Microsoft Active Directory	'On-premises' version
HSM	IBM HSM Crypto Express	HSM services to cater needs upto 25 TPS
KMS	IBM Encryption Platform	3 - 5 licenses for KMS
PIM	Privileged Identity Management	
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 shared links of 5gbps each (Both active)
TOR Switch	Cisco N9X-XXXXXXXX-XXX With 10G/25G multimode fiber SFP and 1G Copper SFP	Bank Will Provide 1 TOR Switch at DC & DR, Any additional requirement to be arranged by the bidder and should be compatible with Bank existing TOR Switch.
WAF	F5 XXXXX	WAF is also used as LB for DMZ segment which is exposed to internet.
Firewall (Perimeter, Internal and DMZ)	Not Applicable	-

Signature of the Bidder with company Seal

Category	Technology	Additional Comments
Firewalls)		
IDS		-
IPS		-
Aggregation Switch	Not Applicable	-
Secrets Manager	Not Applicable	
SAN Storage	Hitachi Vantara Model: VSP XXXX	Upto 200 TB for storage may be provided
SAN Switch	OEM: Cisco Model: DS-CXXXX-XX	
Backup Solution	Commvault	Integration with existing backup solution, Capacity licence, Backup tapes to be arranged by the bidder without any additional cost to the Bank.

The above-mentioned tools / solution / agents / device may be provided by Bank. However, Installation, Configuration and integration will be carried out by the Bidder in coordination with the Bank's Team.

The Bank reserves the right, at its discretion, to provision the Oracle licenses through its existing ULA at a later stage. In such a scenario, the Total Cost of Ownership (TCO) will be suitably adjusted based on the commercial values quoted by the bidder for the respective licenses.

Cyber Security Solutions and Controls implemented or under implementation in the Bank

Sr .No	Name of Cyber Security Tool / Application
1	Network Access Control
2	AD Security
3	Breach and Attack Simulation
4	Attack Surface Management
5	Security Orchestration, Automation, and Response (SOAR)
6	Privileged Identity Management (PIM)
7	Anti-DDoS
8	Digital Rights Management (DRM)
9	Data Loss Prevention (DLP)
10	Brand Protection
11	Host-based Intrusion Prevention System (HIPS)
12	Mobile Device Management (MDM)
13	Governance, Risk, and Compliance (GRC)
14	Vulnerability Assessment
15	Application Security (Web Inspect)
16	Firewall Analyser
17	Phishing Simulation
18	Data Discovery and Classification
19	Decoy (HoneyPot)

Signature of the Bidder with company Seal

20	Secure Data Backup & Recovery
21	Security Information and Event Management (SIEM)

6.8.4 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, the Data Centre (DC), and the Disaster Recovery Centre (DRC).
- All proposed Hardware & software should include 24x7x365 support from the Original Equipment Manufacturer (OEM). Community editions or open licenses shall not be accepted by the Bank
- Provide requisite licenses for system software, including but not limited to operating systems, compilers, multi pathing software, file systems, volume managers, server hardening tools, failover agents, and clustering software, with no restrictions on usage or instances.
- All licences, connectors, APIs, plug-ins, agents, middleware, databases, reporting utilities and supporting software necessary for successful implementation and operation of the proposed solution shall be deemed included.

6.8.5 High Availability and Disaster Recovery

- Design and implement the DC and DRC in an Active -Passive mode with High Availability and no single point of failure.
- 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.

6.8.6 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 (including, ToR etc.)
- Install, maintain, and manage antivirus software for servers at the DC and DRC.
- The solution must support secure communication over both IPv4 and IPv6 networks

6.8.7 Performance and Scalability

- Ensure that servers are load-balanced to prevent performance degradation in the event of server failure.
- The solution shall be designed to support enterprise-scale deployment for an organization, ensuring consistent performance under peak load conditions.
- The proposed solution for Structured Data Discovery shall be designed and sized to support an enterprise database environment across structured data platforms.
- 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.
- The bidder shall leverage and integrate with the Bank's existing tools and platforms, including but not limited to Patch Management, Monitoring, and Disaster Recovery (DR) automation systems.
- The Bidder shall define measurable performance benchmarks including response time, concurrent user capacity, batch processing timelines, report generation time and system availability, which shall be validated during User Acceptance Testing

6.8.8 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.

6.8.9 Additional Requirements

- Ensure that all goods supplied under the contract are fully insured against loss or damage during transportation, storage, assembly, implementation, and maintenance.
- 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.

6.8.10 Compliance with Future Regulatory and Statutory Requirements

Bidder to give an undertaking that during the contract period all new/subsequent changes necessitated due to DPDPA Act/ Regulatory/ Statutory/ Guidelines/ Notifications involving customization/ configurations/ integrations/ enhancements/ upgrade are to be carried out without any additional cost to bank.

6.8.10.1 Regulatory Adaptability & Support

The solution must be adaptable to accommodate changes in laws, rules, or government policies without requiring architectural overhauls or additional licensing costs. The support for managing these updates/upgrades will be for a period of 5 years from platform Go-live date.

6.8.10.2 Timely Updates

The bidder shall be responsible with no delays beyond the statutory effective date for implementing updates or enhancements to the solution in a timely manner to ensure continued compliance with evolving regulatory frameworks.

6.8.10.3 No Additional Cost

Any modifications required to meet future statutory or regulatory obligations shall be provided as part of the scope of work and shall not incur additional cost to the Bank.

6.8.10.4 Documentation and Support

The bidder shall provide documentation and support for all updates made to comply with new regulations, including change logs and impact assessments.

6.8.10.5 Failure to Comply

Non-compliance with future regulatory requirements may result in penalties, termination of contract, or other actions as deemed appropriate by the Bank.

7 Required Artefacts

The BIDDER 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. 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. Application/Software Licensing 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

8. Project Timelines

The successful bidder should complete the following Activities and modules within 210 days from the date of acceptance of Purchase Order. Non-receipt of acceptance of PO within 7 days of issuance shall be deemed accepted. The bidder should adhere to the project schedule as stipulated in the below table. Failure to do so would be liable for LD as stated in the bid, unless Bank grant an extension to the bidder in writing for completion of the activities beyond the timelines as mentioned below. It is completely at the discretion of Bank to grant such an extension based on reasons recorded in writing.

The project timelines from the date of acceptance of the Purchase Order as under:

Phase Wise Implementation Plan

Phase	Activity/Scope	Timeline (Completion from date of acceptance of PO) (Cumulative)
Phase 1	Study ,GAP Assessment and Project Management - Commencement of the project - Project Planning and Roadmap - Current State Assessment for Applicability Assessment of DPDPA Act 2023 & Rules 2025, Develop Data Privacy Framework as per DPDPA requirements as mentioned in scope of work	Date of commencement will be Kick off Meeting Within 45 days from date of acceptance of PO
Phase 2	Study ,GAP Assessment and Project Management - Perform gap Assessment as per the Digital Personal Data Protection Act (DPDPA) 2023, DPDP Rules 2025, and RBI Advisory & Consent Management as mentioned in BRD document of MeitY of all Personal Data Touch Points along with Grounds of Processing. - Completion of Gap assessment requirements related Third Party Risk Management, Grounds for processing personal data, Legitimate Uses, Minor/PwD data processing - Privacy & Consent Management solution Initiation & Planning Requirements & Architecture Design. Infrastructure/ Hardware - Supply and Delivery of software and hardware components at DC, DR	Within 90 days from date of acceptance of PO
Phase 3	Project Management Implementation Roadmap & Execution Support Continuous Compliance & Monitoring	Within 135 days from date of acceptance of PO

Signature of the Bidder with company Seal

Phase	Activity/Scope	Timeline (Completion from date of acceptance of PO) (Cumulative)
	- Framework Design & Policy Development - Data Discovery, Inventory classification & lineage, Personal Data governance, Cross Border Data transfer, Data Flow Mapping. Infrastructure/ Hardware - Installation and configuration of hardware and software components of UAT, Development and production at DC and DR	
Phase 4	Solution Implementation - Implementation of Consent Management, Data Principal Rights Management and Privacy Notice management and Integration with Downstream and Upstream Applications - Implementation of Cookie Consent Management and Privacy Policy of internal and external application separately - RoPA, Privacy Assessment Automation – DPIA, Data Privacy Assessments, Implementation of Compliance Dashboards Privacy by Design - Data and Privacy Breach Management, Compliance - Monitoring reporting and governance dashboard - Third Party Risk Management - Compliance of VA/PT observation	Within 180 days from date of acceptance of PO
Phase 5	Training and Compliance Training including Technical Training, Knowledge Transfer and Capacity Building to take over the activities by the Bank Team & Implementation Monitoring, support, review, improvements, fine tuning, DPDP Privacy/IS Audit & Compliance of Observation. Completion of other deliverables as per Scope of Work	Within 210 days from date of acceptance of PO
Total timeline to Complete the implementation of above phases		Within 210 days from date of acceptance of PO

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 Bidder during the implementation, if a need arises. As there are many
Signature of the Bidder with company Seal

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 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 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 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 BIDDER 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 BIDDER has to perform and support without any additional cost to the Bank.

During the maintenance period, the Bidder shall progressively transfer operational knowledge to designated Bank personnel through structured documentation, workshops and hands-on training to enable effective day-to-day administration of the solution

Section-3

Terms & Conditions

10. Liquidated Damage

The successful 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 Bidder's performance. In that event, the Bank is forced to cancel an awarded contract (relative to this RFP) due to the successful Bidder's inability to meet the established delivery dates, and also the Bank may take suitable penal actions as deemed fit.

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

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

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

B. Penalty for Delay in Production Deployment.

If the 'production deployment and sign-off', 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 for each full week of delay, subject to the following escalating rates:

1. Initial Rate: The penalty shall commence 0.1% of the TCO 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 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:

Note:

- a. A "week of delay" refers to a continuous period of seven (7) calendar days beyond the agreed Go Live date for the specific wave.
- b. The penalty shall be applied on a pro-rata basis for any partial week of delay.
- c. 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 fixed at 10% of TCO quoted by the Bidder of the Summary Sheet of Commercial bid

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

Signature of the Bidder with company Seal

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 concern 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 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. Bidder should submit the undertaking in **Annexure 17: 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 Bidder from a Country which shares a Land Border with India will be eligible to bid in this tender only if the Bidder is registered with Competent Authority.
- 2) "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 Bidders stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.
- 3) "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

Signature of the Bidder with company Seal

- 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 Bidder must provide the Bank access to various monitoring and performance measurement systems. The successful 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 Bidder. These tools should be a part of the proposed solution.

13. Bid Submission

- 1) 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 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/ 7977310 dated 31/08/2026** 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.
- 7) The Bidder shall strictly submit the bid in accordance with the formats, templates, annexures, schedules, declarations, certificates, and other documents prescribed in this RFP. Any deviation, modification, alteration, conditional submission, omission, addition, or non-compliance with the prescribed formats, annexures, terms, conditions, eligibility criteria, technical specifications, commercial formats, declarations, undertakings, or supporting documents shall render the bid liable for rejection at the sole discretion of the Bank. The Bidder shall not modify the wording, structure, sequence, content, or format of any Annexure, Appendix, Schedule, Declaration, Compliance Statement, Technical Bid Format, Commercial Bid Format, or any other document provided as part of this RFP unless specifically permitted by the Bank through a written corrigendum or clarification. Incomplete bids, bids containing qualifications, assumptions, conditions, deviations, exceptions, alterations, or reservations to any provisions of the RFP shall be treated as non-responsive and may be rejected without further correspondence. The Bank reserves the right to reject any bid that does not conform to the requirements of this RFP, including but not limited to deviations from the prescribed formats and annexures, without assigning any reason thereof.

Tender Schedule (Key Dates):

The 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.12-14) 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 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 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 Bidder will be disqualified, and bid submitted by them will not be considered for process.

Commercial Bids of only technically qualified 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** Masked Commercial Bid.

- 1) The Commercial Offer should be in Compliance with Technical Configuration / Specifications as per the scope.

Signature of the Bidder with company Seal

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

15.1 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 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 for next stage of evaluation is 70%.
- 3) 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 Bidder.
- 4) In case, any of the successful 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 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 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.

16. 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 Bidder. The assessment methodology is covered in the next section. The proposals will be evaluated in three stages.

Stage 1 - Eligibility Criteria Evaluation

Stage 2 - Technical Evaluation- 70% Weightage for Technical bid

Stage 3 - Commercial Evaluation- 30% Weightage for Commercial bid

16.1 Stage 1 - Eligibility Criteria

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Eligibility Criteria Section to this document. The Bidders who meet all these criteria would only qualify for the second stage of technical evaluation as per Annexure 12 . The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

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

16.2 Stage 2 -Technical Evaluation

The objective of technical evaluation and shortlisting of the bidders is to facilitate the selection of the most optimal Solution(s) that appropriately meet the requirements of the Bank. The Bank will evaluate the technical bids of the bidders complying with Eligibility Criteria and the proposals meeting the said criteria will only be taken up for further technical evaluation. Bidder should Score 70 % or more for eligible in technical evaluation. In Case of only one Bidder eligible in technical evaluation Bank may at sole discretion to consider to reduce the threshold of 70%.

As part of the technical bid, the bidder should submit all the specified documents/information covering all the clauses specified in the RFP. The eligible Bidders shall be required to deliver an exclusive presentation detailing the proposed architecture for various applications/Solutions, implementation approach, rollout strategy, etc. The bidders should submit the soft copy of the presentation to the Bank along with their technical and commercial bids. A bidder shall be scored based upon the scoring formula given below. Based on the scores, T1 shall be shortlisted, the decision of the Bank regarding evaluation would be final and binding on all the Bidders.

16.3 Stage 3– Commercial Evaluation Criteria

- a) Only those Bidders who have qualified after Stage 1 & 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).

Signature of the Bidder with company Seal

- b) The Bidder shall not add any conditions / deviations in the Commercial Bid. Any such conditions / deviations may make the bid liable for disqualification.
- c) The commercial evaluation would cover Compliance to the Commercial Bid as in **Annexure 2**: The Bidder is expected to provide their “compliance” against each item stated in the Commercial Bid, this means that the Bidder confirms to the provisioning of the stated product or service and the terms of the RFP and subsequent addendums.
- d) The Total cost of Ownership of this tender will be the Grand Total - TCO quoted by the Bidder of the Summary Sheet of **Annexure 2** Masked Commercial Bid.
- e) The Bidder shall not add any conditions / deviations in the commercial bid. Any such conditions / deviations may make the bid liable for disqualification.
- f) Any item, service or component reasonably necessary for successful implementation and operation of the proposed solution but omitted from the commercial bid shall be deemed included in the quoted price.

16.4 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 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 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 Bidders agree that they have no reservation or objection to the normalization process and all the technically short listed 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 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.

16.5 FINAL EVALUATION – WEIGHTED TECHNO-COMMERCIAL EVALUATION

All the bidders who qualify in the Technical evaluation process shall be considered for T score calculation. The bidders will be ranked as T1, T2 etc. based on net total score arrived basis the scoring formula mentioned below.

$$\text{Technical Score (T)} = \frac{\text{Bidder's Technical score}}{\text{Highest Technical Score}} \times 100$$

The commercial bid(s) of only those bidders, who are short-listed after technical evaluation, would be opened. The commercial score C would be calculated based on the following formula. The bidders will be ranked as C1, C2 etc. based on net total score arrived basis the scoring formula mentioned below.

$$\text{Commercial Score (C)} = \frac{\text{Lowest Commercial Price}}{\text{Bidder's Commercial Price}} \times 100$$

The final ranking of the bidders will be based on Techno Commercial evaluation i.e. 70% Weightage for Technical Score + 30% Weightage for Commercial Score. The final Score F will be calculated using the formula given below:

$$\text{Final Score (F)} = (\text{Technical Score} \times 0.7) + (\text{Commercial score} \times 0.3)$$

The bidders will be ranked as F1, F2 etc. based on net total score arrived basis the above scoring formula. The bidder who scores overall HIGHEST FINAL score F1 will be declared as winner (L1)

For Example:

Three bidders namely A, B and C participated in the bid process and their technical score are as under:

$$A=60, B=80, C= 90$$

After converting them into percentile, we get

$$T \text{ for } A = (60/90) \times 100 = 66.67 \text{ (T3)},$$

$$T \text{ for } B = (80/90) \times 100 = 88.89 \text{ (T2) and}$$

$$T \text{ for } C = (90/90) \times 100 = 100 \text{ (T1)}$$

The Commercial Bid prices of the bidders are as under: A= Rs. 8000, B= Rs. 9000, C= Rs. 10000

The final cost (lowest cost quoted in Commercial price bid, in this case is Rs 8000) quoted by the bidders converted into percentile score shall be as under:

$$C \text{ for } A = (8000/8000) \times 100 = 100 \text{ (C1)}$$

$$C \text{ for } B = (8000/9000) \times 100 = 89 \text{ (C2)}$$

$$C \text{ for } C = (8000/10000) \times 100 = 80 \text{ (C3)}$$

Signature of the Bidder with company Seal

As the weightage for technical parameter and cost are $TW = 70\%$ and $FW = 30\%$ respectively, the final scores shall be calculated as under:

$$F \text{ for A} = (66.67 \times 0.7) + (100 \times 0.3) = 76.67 (F3)$$

$$F \text{ for B} = (88.89 \times 0.7) + (89 \times 0.3) = 88.92 (F2)$$

$$F \text{ for C} = (100 \times 0.7) + (80 \times 0.3) = 94 (F1)$$

The proposal securing the highest combined marks and ranked F1 shall be recommended for award of contract as L1. In the event two or more bids have the same score in final ranking, the bid with highest technical score T1 will be the winner. In case of a discrepancy between amount in words and figures, the amount mentioned in words will be considered as final. Hence, the offer of bidder 'C' (being highest score) would be considered and the contract shall be awarded to 'C' at Rs. 10000, being the price quoted by C.

Note: The bidder with highest score shall not automatically qualify for becoming selected bidder and for award of contract by the Bank. The final decision on the successful bidder will be taken by the Bank. The implementation of the project will commence upon acceptance of LOI/purchase order by the selected bidder. If for some reason, the successful bidder fails to execute an agreement within a specified timeline, the Bank reserves the right to award the contract to the next most eligible bidder based on the final evaluation scope of technical evaluation scores and commercial prices quoted during tendering process. In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder. The Bank will calculate the scores up to two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points.

Award of Contract

The contract shall be awarded to and the order shall be placed with selected F1 Bidder (shall be called L1 bidder) securing the highest total combined score based on technical evaluation of quality and cost of the bidder. The selected bidder shall submit the acceptance of the order within seven days from the date of receipt of the order. Conditional or qualified acceptance will not be entertained and shall be rejected. On receipt of full and unconditional acceptance, bidder need to execute the required Contractual documents such as SLA, NDA, Deed of Indemnity, PBG, Escrow Agreement etc. of / with the bank in time. The effective date for start of provisional contract with the selected Bidder shall be the date of acceptance of the order by the bidder. Bank reserves its right to consider at its sole discretion the late acceptance of the order by selected bidder (s).

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 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.

17 General Terms

17.1 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 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) Bank will deduct applicable TDS, if any, as per the law of the land.
- g) The quoted fixed cost against each item shall remain unchanged till the completion of the Project(s).
- h) The base project location will be Mumbai/Navi Mumbai and Hyderabad.
- i) The TCO in words is amount on which the commercial evaluation will be conducted.
- j) All prices to be valid for a period of 5 years from the date of contract execution / signing / Go-Live.
- k) 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.
- l) Bidder shall depute resources on-site of the project implementation location(s) for carrying out the task as specified in this document.
- m) 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.
- n) The cost quoted also includes the cost of deliverables for all the phases of the Project.
- o) Further, we confirm that we will abide by all the terms and conditions mentioned in the Request for Proposal document.
- p) Fee is payable only on actual availing of services and no minimum or fixed fees are payable.
- q) Bidder is expected to provide detail bill of material along with the commercial proposal for the proposed hardware and appliances.
- r) 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 Masked

Signature of the Bidder with company Seal

- Commercial Bid. 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.
- s) The AMC/ATS cost of Hardware should be minimum 8% of the Product Cost.
 - t) The ATS cost System Software shall be minimum 15% of Product Cost.
 - u) 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.
 - v) The Successful Bidder shall, within thirty (30) days from the date of issuance of the Purchase Order and in any event prior to release of the first payment, open and maintain a designated operative account with Central Bank of India exclusively for the purpose of receipt of all payments and financial transactions arising out of this Contract. All payments by the Bank under this Contract shall be made only into the said designated account. The Bidder shall ensure that the account remains active and operational throughout the currency of the Contract

17.2 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.

18 Payment Terms

No escalation in price quoted is permitted for any reason whatsoever. Prices quoted must be firm till the completion of the contract period.

From the date of placing the order till the delivery of the systems, if any changes are brought in the duties such as excise/customs etc., by the Government resulting in reduction of the cost of the systems, the benefit arising out of such reduction shall be passed on to the Bank.

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:

18.1 Payment Terms:

18.1.1 The payment schedule will be as under and will release after execution of contract agreement:

Sl. No.	Payment Particulars	% of Payment / Period	Milestone
1.	Infrastructure / Hardware Cost	30% of Infrastructure / Hardware Cost of S.I No 1	On supply and delivery of Hardware for the setup of

Signature of the Bidder with company Seal

Sl. No.	Payment Particulars	% of Payment / Period	Milestone
	for Production, UAT, and Development at DC & DR with 3-year onsite warranty from the date of sign off.	of Table A of Commercial Bid	infrastructure in DC & DR for the proposed solution. Defined in Phase-2 of Project TimeLine
		50% of Infrastructure / Hardware Cost of S.I No 1 of Table A of Commercial Bid	On successful installation of Hardware / System software for the setup of infrastructure in DC & DR for the proposed solution. Defined in Phase-3. of Project Timeline
		10% of Infrastructure / Hardware Cost of S.I No 1 Table A of Commercial Bid	On successful implementation & go live of Module no 1, 2 & 3 of the proposed solution Defined in Phase 4 of Project Timeline
		10% of Infrastructure / Hardware Cost of S.I No 1 Table A of Commercial Bid	On Completion of 30 days after post sign-off of the Production and successful DR Drill.
	AMC / ATS Cost of the Hardware / Infrastructure	Quarterly	Payment will be done quarterly in arrears
2.	System Software's Cost for Production, UAT and Development in DC & DR with 1-year onsite warranty from the date of sign off.	80% of System Software's Cost of S.I No 3 of Table A of Commercial Bid	On supply, delivery and successful installation of required Software items for the setup of infrastructure in DC & DR for the proposed solution Defined in Phase-3 of Project Timeline.
		10% of System Software's Cost of S.I No 3 Table A of Commercial Bid	On successful implementation and go live of Module no 1, 2 & 3 of the proposed solution Defined in phase 4 of Project Timeline.
		10% of System Software's Cost of S.I No 3 Table A of Commercial Bid	On Completion of 30 days after post sign-off of the Production and successful DR Drill.
	AMC / ATS Cost of the system software	Quarterly	Payment will be done quarterly in arrears
3.	Enterprise wide Perpetual License cost of Data Privacy &	50% of Perpetual License Cost of Table B of Commercial Bid	On successful supply ,delivery and installation of the proposed solution Define in Phase – 3 of Project

Sl. No.	Payment Particulars	% of Payment / Period	Milestone												
	Consent Management Solution/Tools (Module wise) with One-year comprehensive Warranty and support from the date of Sign off.		Timeline												
		40% of Perpetual License Cost of Table B of Commercial Bid	On implementation and Go-live after VAPT of the respective module. Defined in phase 4 of Project Timeline												
		<table><tr><td>Sr No</td><td>% of payment</td><td>Module Sl. No</td></tr><tr><td>1</td><td>20%</td><td>1,2,3,4</td></tr><tr><td>2</td><td>10%</td><td>5,6,7,8</td></tr><tr><td>3</td><td>10%</td><td>9,10,11</td></tr></table>		Sr No	% of payment	Module Sl. No	1	20%	1,2,3,4	2	10%	5,6,7,8	3	10%	9,10,11
		Sr No		% of payment	Module Sl. No										
		1		20%	1,2,3,4										
2	10%	5,6,7,8													
3	10%	9,10,11													
10% of Perpetual License Cost of Table B of Commercial Bid															
		On Completion of 30 days after post sign-off of the Production and successful DR Drill.													
	ATS for four year after 1 st year warranty period of the proposed solution	Quarterly/ Yearly	Payment will be done Quarterly in arrears. Or Payment will be done Yearly in advance on submission of BG for the equivalent amount.												
4.	Study the Bank System GAP Assessment , Prepare a Roadmap / Approach / Implementation Plan and Implement the solution, Policy review and framework design etc for Complete Compliance of DPDP Act and Rules	50% of GAP Assessment Cost as per Table C Sr no 1 of Commercial Bid	On submission and acceptance of final Documentation (SOPs, Manuals, Reports etc) and successful completion/ implementation defined in Phase1, Phase-2 and Phase -3 of Project Timeline.												
		<table><tr><td>Sr No</td><td>% of payment</td><td>Milestone</td></tr><tr><td>1</td><td>5%</td><td>Phase 1</td></tr><tr><td>2</td><td>20%</td><td>Phase 2</td></tr><tr><td>3</td><td>25%</td><td>Phase 3</td></tr></table>		Sr No	% of payment	Milestone	1	5%	Phase 1	2	20%	Phase 2	3	25%	Phase 3
		Sr No		% of payment	Milestone										
		1		5%	Phase 1										
		2	20%	Phase 2											
3	25%	Phase 3													
40% of GAP Assessment Cost as per Table C Sr no 1 of Commercial Bid															
10% of GAP Assessment Cost as per Table C Sr no 1 of Commercial Bid															
		On Final Implementation and Go-Live of the Complete Solution and Audit compliance Defined in Phase-5 of Project Timeline													

Sl. No.	Payment Particulars	% of Payment / Period	Milestone												
5.	Implementation Cost of the Proposed Solution in DC, DRC & UAT infrastructure	80 % Implementation Cost as per Table C Sr no 2 of Commercial Bid	On successful Implementation and go-live of the proposed Privacy and Consent management solution and closure of VAPT observation. Defined in Phase 4 of Project Timeline.												
		<table><tr><th>Sr No</th><th>% of payment</th><th>Module SI No</th></tr><tr><td>1</td><td>40%</td><td>1,2,3,4</td></tr><tr><td>2</td><td>20%</td><td>5,6,7,8</td></tr><tr><td>3</td><td>20%</td><td>9,10,11</td></tr></table>		Sr No	% of payment	Module SI No	1	40%	1,2,3,4	2	20%	5,6,7,8	3	20%	9,10,11
		Sr No		% of payment	Module SI No										
		1		40%	1,2,3,4										
		2	20%	5,6,7,8											
3	20%	9,10,11													
20% of Implementation Cost as per Table C Sr no 2 of Commercial Bid	On Completion of 30 days after post sign-off of the Production and successful DR Drill.														
6.	Onsite Resources	Payment will be Quarterly in arrears on actual basis of Onsite resources as per Table-E of Commercial Bid													
7.	Additional requirements/ additional customization/ enhancement	Payment will be done on actual man days utilized for the Successful Customization and sign off by the Bank for Additional requirements/Integration cost as per Table – D of the commercial Bid.													
8.	Training	100% of Training Cost as per Table F of Commercial Bid payment will be released on successful Completion of Training as per scope.													

18.1.2 Bank will release the payment on completion of activity and on production of relevant documents/invoices. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.

18.1.3 The selected bidder has to submit installation report/Sign off report duly signed by the Bank officials of the respective Branch/offices in originals while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.

18.1.4 Bank will not pay any amount in advance unless otherwise specified in this RFP.

18.1.5 The Bank shall finalize the installation and acceptance format mutually agreed by the selected bidder. The selected bidder shall strictly follow the mutually agreed format and submit the same for each location wise while claiming installation and acceptance payment.

18.1.6 The payments will be released through NEFT / RTGS after deducting the application LD/Penalty, TDS if any, by centrally by Head Office at Mumbai

and the selected bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code etc.

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 **Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025** during the contract period as per the format in Commercial Bid: **Annexure 2** Masked Commercial Bid.

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 after 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. After the dispute is resolved. Bank shall make payment after 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 1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point, Mumbai 400021. 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.

Signature of the Bidder with company Seal

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.

19 Service Level Agreement

1. BIDDER 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 BIDDER to the Bank. BIDDER shall monitor and maintain the stated service levels to provide quality customer service to the Bank.
2. BIDDER 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 BIDDER 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 BIDDER 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 successful Bidder shall provide a mandatory, zero-cost shadow support and reverse transition period for a minimum of 90 days prior to the expiration of the contract or immediately upon the issuance of a termination notice. During this period, the Bidder must ensure a seamless handover of all operational processes, configuration artefacts, APIs, and data to the Bank or its designated replacement service provider. The Bidder is obligated to maintain all agreed Service Level Agreements (SLAs) without any degradation in performance or additional commercial charges to the Bank during this entire shadow support phase. Repeated failure to achieve the same SLA parameter for three consecutive measurement periods, or five occasions during any rolling twelve-month period, shall constitute a material breach entitling the Bank to invoke appropriate contractual remedies, including issuance of a corrective action notice or termination in accordance with the Contract.

4. Digital Personal Data Protection Compliance

The Service Provider / Vendor shall, always, 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 Service Provider / 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 the existing contract.

Further, the Service Provider / 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 the Signature of the Bidder with company Seal

SLA/RFP shall follow 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 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, unauthorized 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 Service Provider / 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.

5. Labour Law Adherence and Compliance with Court Directions

The Service Provider / 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 Service Provider / 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 contract.

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

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

The Service Provider / 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.”

6. The Bank expects the successful BIDDER 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 BIDDER.
- ii. The selected BIDDER should have 24X7X365 days monitoring, escalation and resolution mechanism.
- iii. Time bound problem addressing team (onsite) for the complete contract period.

- iv. BIDDER 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 BIDDER 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 BIDDER.

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

Key Metrics:

Category	SLA Metric	Target	Penalty Applicable	Penalty details
Support and Incident Management	Severity 1 Incidents - Response Time	Up to 60 minutes	Yes	
	Severity 1 Incidents - Resolution Time	Up to 2 hours	Yes	2 hrs < Resolution Time ≤ 4 hrs: 0.01 % of Total amount payable during the quarter 4 hrs < Resolution Time ≤ 6 hrs: 0.025 % of Total amount payable during the quarter 6 hrs < Resolution Time: 0.04 % of Total amount payable during the quarter
	Severity 1 Incidents - RCA Time	Up to 24 hours	Yes	
	Severity 2 Incidents - Response Time	Up to 120 minutes	Yes	

Signature of the Bidder with company Seal

Category	SLA Metric	Target	Penalty Applicable	Penalty details
	Severity 2 Incidents - Resolution Time	Up to 4 hours	Yes	4 hrs < Resolution Time ≤ 8 hrs: 0.01 % of the TCO amount 8 hrs < Resolution Time ≤ 12 hrs: 0.025 % of the TCO amount 12 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 4 hours	Yes	
	Severity 3 Incidents - Resolution Time	Up to 8 hours	Yes	8 hrs < Resolution Time ≤ 16 hrs: 1% of Total amount payable during the quarter 16 hrs < Resolution Time ≤ 24 hrs: 2% of Total amount payable during the quarter 24 hrs < Resolution Time: 3% of Total amount payable during the quarter
	Severity 3 Incidents - RCA Time	Up to 72 hours	Yes	
	Severity 4 Incidents - Response Time	Up to 8 hours	Yes	
	Severity 4 Incidents - Resolution Time	Up to 1 Calendar days	Yes	
	Severity 4 Incidents - RCA Time	Up to 4 Working days	Yes	

Category	SLA Metric	Target	Penalty Applicable	Penalty details
System Availability	Uptime of Platform (including underlying Infrastructure, ingestion, processing, access, consumption capabilities)	$\geq 99.95\%$ (Monthly) < 21.91 minutes of downtime per month	Yes	Refer to the table 'Penalty for Downtime of Production environment of the Platform' below
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	99.9% success rate for all backup jobs (daily, weekly, fortnightly, monthly etc) measured and enforced monthly, for applicable penalty.	Yes	98 % $\leq$ Backup Success Rate < 99.95 %: 1% of Total amount payable during the quarter Backup Success Rate < 98 %: 2% of Total amount payable during the quarter
API Performance SLA	API Response	99.95% availability monthly	Yes	≤ 200 ms normal load ≤ 300 ms peak load

- v. Wherever the SLA is not met due to Software/ Configuration/Performance issues then the Successful bidder must enhance / upgrade the Solution accordingly without any additional cost to the Bank within a months' time
- vi. Successful BIDDER 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:

- a. Downtime percentage - Unavailable Time divided by Total Available Time, calculated monthly.
- b. 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)
- c. Unavailable Time - Time involved while the solution is inoperative or operates inconsistently or erratically.

- vii. The successful BIDDER should demonstrate that the proposed solution meets the required key metrics.
- viii. 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 ATS/AMC charges of proposed Solution for the payable amounts during the contract duration of Respective year)
99.95% =< A <= 100 %	No Penalty
99.30% <= A < 99.95 %	1% of Total amount payable during the quarter
99 % <=A < 99.30 %	2% of Total amount payable during the quarter
A < 99.00 %	3% of Total amount payable during the quarter

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

Uptime Range (measured Monthly)	Penalty Details (will be deducted from ATS/AMC charges of proposed Solution for the payable amounts during the contract duration of Respective year)
99.00% =< A <= 100 %	No Penalty
97.00% <= A < 99.00 %	1% of Total amount payable during the quarter
95 % <=A <=97 %	2% of Total amount payable during the quarter
A < 95.00 %	3% of Total amount payable during the quarter

The BIDDER is responsible for performing sizing and provisioning hardware to ensure that the utilization of Compute, Memory, and Storage for all production hardware infrastructures at both the DC and DRC remains below 70% throughout the contract period.

Others compliance related:

Description	Penalty Time above resolution time	Penalty Details (will be deducted from ATS/AMC charges of proposed Solution for the payable amounts during the contract duration of Respective year)
Quarterly VAPT/any other Regulatory/Statutory Compliance Confirmation	Up to 15 Days	NIL
	16 to 30 days	3.0% of Total amount payable during the quarter
	>30 days	5.0% of Total amount payable during the quarter

Penalty for Non-performance:

- a) If the up time for the platform and/or implemented solution is below the guaranteed level, the Bank will impose a penalty as specified.

Availability Service Level Default

- a) Service Levels will be measured on a monthly basis. The BIDDER'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) Service Levels will include Availability measurements and Performance parameters.
- d) BIDDER 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 BIDDER performance measurement for that period.
- e) Performance measurements would be accessed through reports, as appropriate to be provided by BIDDER e.g., utilization reports, response time measurements report, etc.
- f) Cost Reference that is mentioned is billing value for the defaulted period & defaulted component for which SLA will be calculated.
- g) In case of any service default by the BIDDER, the OEM has to take up and deliver the work as defined in the SLA for the contract period.
- h) 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.
- i) BIDDER 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.

Signature of the Bidder with company Seal

Availability Service Level Default for Facility Management

- a) BIDDER 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 BIDDER should immediately provide the Bank with an equivalent standby resource for that resource.
- e) If BIDDER fails to meet the onsite Resource Availability in any month, then BIDDER 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 $\{(\text{Scheduled operation time} - \text{system downtime}) / (\text{scheduled operation time})\} * 100\%$.
- 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 BIDDER's help desk of the failure or the failure is known to BIDDER 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, BIDDER (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 BIDDER 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 BIDDER on these SLAs compliance as per the periodicity defined.
- n) BIDDER shall provide reports to verify the BIDDER'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 BIDDER 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 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 BIDDER 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.

Signature of the Bidder with company Seal

- s) BIDDER 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. BIDDER 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 BIDDER 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/application installation, the temporary substitute equipment/ application 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 BIDDER from payments due to them. In case no payments are due, the Bidder 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 BIDDER. 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 BIDDER 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, BIDDER 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. BIDDER 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 BIDDER 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 BIDDER as per the invoice. In case if there are no pending invoices to be paid by the Bank to the BIDDER, the BIDDER has to submit Credit Note / pay order / cheque payable at Mumbai/ Navi Mumbai in favor of Central Bank of India for the same within 15 days from the notice period from the Bank.
- g) BIDDER 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.
- h) Application of SLA service credits shall be without prejudice to the Bank's right to exercise any other contractual remedy available under the Agreement

Service Levels during Post implementation phase

- a) The BIDDER 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	Manager
1 hour	Senior Manager
2 hours	Chief Manager / Assistant General Manager
> 4 hours	Data Protection Officer

20 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.

21 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.

22 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 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 invoke / encash the applicable 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.

23 Indemnity

- 1) The Bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorney's fees) relating to, resulting directly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:
 - i. Bank's authorized / bonafide use of the Deliverables and/or the Services provided by Bidder under this RFP or any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - ii. Relating to or resulting directly from infringement of any third party patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
 - iii. An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP or, any or all terms and conditions stipulated in the SLA(Service level Agreement) or Purchase Order(PO) and/or
 - iv. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank and/or
 - v. Breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Bidder under this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - vi. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights and/or

Signature of the Bidder with company Seal

- vii. Breach of confidentiality obligations of the Bidder contained in this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - viii. Negligence or gross misconduct attributable to the Bidder or its employees, agent or sub-contractors.
 - ix. The Bidder shall indemnify and keep the Bank indemnified against all losses, damages, costs, claims, regulatory actions, penalties, liabilities and expenses arising directly from any defect, deficiency, malfunction, security vulnerability, failure to perform the contractual specifications, or breach of applicable law attributable to the Bidder, its personnel, subcontractors, software, or services.
- 2) The Bidder shall further indemnify the Bank against any loss or damage arising out of claims of infringement of third-party copyright, patents, or other intellectual property issued or registered in India, provided however,
- i. The Bank notifies the Bidder in writing immediately on aware of such claim,
 - ii. The Bidder has sole control of defense and all related settlement negotiations,
 - iii. The Bank provides the Bidder with assistance, information and authority reasonably necessary to perform the above, and
 - iv. The Bank does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and Bidders) rights, interest and reputation.
- 3) The Bidder shall compensate the Bank for direct financial loss suffered by the Bank, if the Bidder fails to fix bugs, provide the Modifications / Enhancements / Customization as required by the Bank as per the terms and conditions of this RFP and to meet the Service Levels as per satisfaction of the Bank.
- 4) Additionally, the Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings suffered by Bank due to the following reasons:
- i. that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used,

sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.

- ii. all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:
 - The Bidder has sole control of the defense and all related settlement negotiations.
 - The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.
- 5) Bidder shall have no obligations with respect to any Infringement Claims to the extent that the Infringement Claim arises or results from:
- i. Bidder's compliance with Bank's specific technical designs or instructions (except where Bidder knew or should have known that such compliance was likely to result in an Infringement Claim and Bidder did not inform Bank of the same);
 - ii. Inclusion in a Deliverable of any content or other materials provided by Bank and the infringement relates to or arises from such Bank materials or provided material;
 - iii. Modification of a Deliverable after delivery by Bidder to Bank if such modification was not made by or on behalf of the Bidder;
 - iv. operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Statement of Work by the Bidder; or
 - v. Use of a superseded release of some or all of the Deliverables or Bank's failure to use any modification of the Deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Bidder.
- 6) In the event that Bank is enjoined or otherwise prohibited, or is reasonably likely to be enjoined or otherwise prohibited, from using any Deliverable as a result of or in

connection with any claim for which Bidder is required to indemnify Bank under this section according to a final decision of the courts or in the view of Bidder, Bidder, may at its own expense and option:

- (i) Procure for Bank the right to continue using such Deliverable.
 - (ii) Modify the Deliverable so that it becomes non-infringing without materially altering its capacity or performance;
 - (iii) Replace the Deliverable with work product that is equal in capacity and performance but is non-infringing; or (iv) If such measures do not achieve the desired result and if the infringement is established by a final decision of the courts or a judicial or extrajudicial settlement, the Bidder shall refund the Bank the fees effectively paid for that Deliverable by the Bank subject to depreciation for the period of Use, on a straight line depreciation over a 5 year period basis. The foregoing provides for the entire liability of the Bidder and the exclusive remedy of the Bank in matters related to infringement of third party intellectual property rights.
- 7) The Bank warrants that all software, information, data, materials and other assistance provided by it under this Agreement shall not infringe any intellectual property rights of third parties, and agrees that it shall at all times indemnify and hold Bidder harmless from any loss, claim, damages, costs, expenses, including Attorney's fees, which may be incurred as a result of any action or claim that may be made or initiated against it by any third parties alleging infringement of their rights.

24 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 in to 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

Signature of the Bidder with company Seal

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

25 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.

26 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 The parties shall endeavour to mutually appoint a Sole Arbitrator within thirty (30) days of invocation of arbitration. If the parties fail to mutually appoint a Sole Arbitrator within the said period, the arbitration shall be conducted by a three-member Arbitral Tribunal, with each party appointing one arbitrator, and the two appointed arbitrators appointing the Presiding Arbitrator, in accordance with the Arbitration and Conciliation Act, 1996.

- 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. . Every arbitrator shall make the disclosures required under Section 12 of the Arbitration and Conciliation Act, 1996 and shall not be ineligible under the Seventh Schedule of the Act.
- 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.

27 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”.

28 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.

29 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.

30 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.

Signature of the Bidder with company Seal

- 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.

31 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

32 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.

33 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

Signature of the Bidder with company Seal

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.

34 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 Signature of the Bidder with company Seal

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.

35 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.

36 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.

37 Intellectual Property Rights

- The Bank intends to procure and own the Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025 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 Privacy & Consent Management Solution/Tools 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 Privacy & Consent Management Solution/Tools 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 Privacy & Consent Management Solution/Tools.
- 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

Signature of the Bidder with company Seal

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

38 Enterprise License:

38.1 The proposed Data Privacy & Consent Management Solution/Tools 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

38.2 Licenses for the Data Privacy & Consent Management Solution/Tools 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

Signature of the Bidder with company Seal

38.3 All software that is envisaged for delivery of Data Privacy & Consent Management Solution/Tools is required to be licensed to Bank.

38.4 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 Privacy & Consent Management Solution/Tools along with final customization should be VAPT certified at no extra cost to Bank. Bidder shall ensure the security assessment/Audit including VAPT and Compliance for all the deliverables before GO Live without any cost to the bank. Bank will not pay any customization charges till Go Live of respective solution.
- g) Ensure support contract for the Data Privacy & Consent Management Solution/Tools should include program updates, patches, fixes, and critical security alerts as required.

38.5 The Bidder must provide an unconstrained, Enterprise-Wide Perpetual License for all proposed modules, tools, and components. The commercial model must be strictly on a fixed-cost basis. The Bank explicitly prohibits any consumption-linked pricing models, including but not limited to variable transaction fees, per-API call charges, data volume thresholds, or user/branch/device count limitations. No additional commercial charges or subscription upgrades shall be payable due to the scaling of digital transaction volumes, data queries, or the onboarding of new applications and channels during the entire contract period

39 Termination

39.1 Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 30 (Thirty) 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

Signature of the Bidder with company Seal

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.

Bidder shall also have the right to terminate the agreement if the Bank commits a breach of the terms and conditions of the agreement and, where such breach is curable, fails to cure the same within 15 days provided for curing such breach.

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.

39.2 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.

39.3 Termination- Key Terms & Conditions

Either Party 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.

39.4 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 support and assistance as required.

39.5 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. 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

40 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

Signature of the Bidder with company Seal

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.

41 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.

42 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 and DPDP Rules 2025, RBI's "Master 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 master Directives on Outsourcing of IT Services are:-

- 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)

Signature of the Bidder with company Seal

- a) Data breaches
- b) Denial of service attacks
- c) Service unavailability
- d) Security vulnerabilities
- e) Unauthorized access
- f) System failures
- g) 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.

- ii. 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.

Signature of the Bidder with company Seal

- 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:
- Is shared with explicit written consent or authorization from the Bank.
 - Is required by law or regulation, including legal processes such as subpoenas.
 - 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 support and 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

Signature of the Bidder with company Seal

- 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.

42.1 Adherence to IT/Cyber Security Policy

- 42.1.1 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.
- 42.1.2 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.
- 42.1.3 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.
- 42.1.4 The Service provider shall put in place necessary controls within its organization for maintaining confidentiality of the Bank's and its customer's data.

42.2 Compliance with Laws

- 42.2.1 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.
- 42.2.2 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.

43 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-

44 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.

45 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.

46 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.

47 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
Signature of the Bidder with company Seal

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.

48 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.

48.1 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.

48.2 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.

48.3 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.

48.4 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

48.5 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.

48.6 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.

Signature of the Bidder with company Seal

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.

49 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.

50 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.

51 Remote Access

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

52 Business Continuity and Disaster Recovery

52.1 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.

52.2 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, retention, archival and retrieval.
- 3) Clear steps to restore services to full functionality, including resource allocation and escalation procedures.

Signature of the Bidder with company Seal

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

53.1 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.

53.2 Cooperation

The Service Provider agrees to provide all necessary information, documentation, support 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.

53.3 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.

53.4 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.

54 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.

55 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.

56 Escrow Arrangements

The bidder has to facilitate for Escrow Agreement between all the parties (Bank as beneficiary, ESCROW Agent, OEM and System Integrator/bidder 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.

.....

Section-4

Annexures

Checklist for Submission

Any deviation, modification, alteration, conditional submission, omission, addition, or non-compliance with the prescribed formats, annexures, terms, conditions, eligibility criteria, technical specifications, commercial formats, declarations, undertakings, or supporting documents shall render the bid liable for rejection at the sole discretion of the Bank

Note - All letter/Annexures should be on the letterhead of the bidder

Sr No	Particulars	Bidders Remark (Yes/No)
1	Certificate of Incorporation and Proof of Registration with GSTIN	
2	Audited Balance sheets and operating profit (P & L) of last three years -	
3	Certificate from the OEM for proposed solution aligned and complied with Digital Personal Data Protection Act (DPDPA) 2023, DPDP Rules 2025 & MeITY NeGD issued BRD Document	
4	Submit Self-declaration & confirmation on Company's Letter Head with undertaking that they will enable Integration capability and complete the integration process whenever the National Consent Management Portal Framework / Consent Managers is made live by Government without any additional cost to Bank.	
5	Undertaking on Company's Letter Head for minimum of 50 personnel on its payroll in India, with expertise in the fields of Data Privacy and Consent Management to provide services to the Bank and have Direct support/Service offices in Mumbai/Navi Mumbai and Hyderabad	
6	Copies of Valid accreditations ISO/IEC 27001:2022 Certification • ISO/IEC 27701:2019 Certification • SOC 2 Type 2 Certificate	
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, Financial institutes for any reason or non-implementation/ delivery of the	
8	Self-declaration on Company's letter head stating Bidder/OEM should not have any pending litigation or any dispute in the last 5 years	
9	Self-declaration on Company's letter head regarding • NPA • Any case pending	
10	Document Cost	

Signature of the Bidder with company Seal

Sr No	Particulars	Bidders Remark
11	Annexure 1: Conformity Letter	
12	Annexure 2: Masked Commercial Bid	
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: Technical Evaluation Sheet	
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, Hardware, Cryptographic Bill of Material Format	
34	Annexure 24- Template for Third Party Due Diligence Questionnaire	
35	Annexure 25: Bidder's Particulars on Company Letter Head	
36	Annexure 26: List of Hardware and Software Components	
37	Annexure 27: Letter for Refund of EMD	
38	Annexure 28: Format for Submission of Client References by Bidder	
39	Annexure 29: Undertaking for Data Privacy	
40	Annexure 30: Undertaking for 5 Years Roadmap	
41	Annexure 31: Format for Local Content	
42	Annexure 32: Proposed Team Profile	
43	Annexure 33: Volumetrics	
44	Annexure 34: Declaration of Source Code Audit	
45	Annexure 35 : Technical/functional Specifications	
46	Annexure 36 : Format for Credential Letter (For Bidder)	
47	Annexure 37: Format for Credential Letter (For OEM)	
48	Annexure 38: Undertaking for Infrastructure Sizing and Capacity Planning	

Signature of the Bidder with company Seal

Annexure 1: Conformity Letter

Date

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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: Masked Commercial Bid

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Notes

1. These details should be on the letterhead of Bidder and each & every page should be signed by an Authorized Signatory with Name and Seal of the Company.
2. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
3. Do not change the structure of the format nor add any extra items.
4. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

Table – A

Cost of Hardware and other items for implementation Data Privacy & Consent Management Solution/Tools

[Amount in Indian Rupees]

Sl. No.	Requirement Details	Yearly Breakup					Total Cost with Comprehensive Onsite Warranty and AMC / ATS (Excl. of tax)	Tax for Column f		Total Cost with Comprehensive Onsite Warranty and AMC / ATS (Incl. of tax)
		1 st Year (License Cost)	2 nd year	3 rd Year	4 th year	5 th year		% tax	Tax Amt.	
		a	b	c	d	e		g	h	
1.	Enterprise class Infrastructure / Hardware Cost (server , storage, tape library and tapes etc ,System Software, Network device, Load Balancer, Reverse proxy , LAN Cables ,etc)	XX					XX	XX	XX	XX

Signature of the Bidder with company Seal

Sl. No.	Requirement Details	Yearly Breakup					Total Cost with Comprehensive Onsite Warranty and AMC / ATS (Excl. of tax)	Tax for Column f		Total Cost with Comprehensive Onsite Warranty and AMC / ATS (Incl. of tax)
		1 st Year (License Cost)	2 nd year	3 rd Year	4 th year	5 th year		% tax	Tax Amt.	
		a	b	c	d	e		g	h	
	for Production , UAT ,Development in DC & DR with 3-year onsite warranty from the date of sign off.						F=a+b+c+d+e			i= f+h
2.	AMC / ATS Cost of the Infrastructure / Hardware				XX	XX	XX	XX	XX	XX
3.	System Software Cost (OS Database Licenses, Backup solution, archival solution etc) for Production , UAT ,Development in DC & DR with 1-year onsite warranty from the date of sign off.	XX					XX	XX	XX	XX
4.	AMC / ATS Cost of the system software		XX	XX	XX	XX	XX	XX	XX	XX

Note: 1. The bidder shall provide detailed item-wise pricing for all proposed components, including but not limited to Hardware, Storage, Operating Systems, Databases, Middleware, Software Licenses, Security Components, Licenses, Subscription Costs, and any other associated products or services. Each component shall be quoted separately with complete technical specifications, quantities, unit costs, and total costs in distinct line items/sheets of the commercial bid. AMC of the consumables items like Rack, Tapes, LAN Cable, SAN Cables etc to be excluded.

2. The Database/other License cost shall be quoted as a separate line item. The Bank reserves the right, at its sole discretion, to procure the database/other license independently or through the successful bidder. Accordingly, the cost of the database/other license shall be evaluated.

3. Delivery of Software license should be after delivery of Hardware and required Infrastructure for the proposed solution and confirmation from the Bank.

Signature of the Bidder with company Seal

Table – B

Enterprise perpetual License cost for Data Privacy & Consent Management Solution/Tools with comprehensive Support & Maintenance for five Years

[Amount in Indian Rupees]

Sl. No.	Requirement Details	Yearly Breakup 2 nd Year Warranty/ATS commence from date of go live sign off					Total Cost with one Year Comprehensive Onsite Warranty and 4 year of AMC / ATS (Excl. of tax)	Tax for Column a		Total Cost (Incl. of tax)
		1 st Year (License Cost)	2 nd year (ATS Cost)	3 rd Year (ATS Cost)	4 th year (ATS Cost)	5 th year (ATS Cost)		Tax %	Tax Amt.	
		a	b	c	d	e		f= a+b+c+d+e	G	h
1.	Application / Product cost of following modules / components of the proposed solution									
	a. Consent Management	XX					XX	XX	XX	XX
	b. Cookie Consent Management	XX					XX	XX	XX	XX
	c. Record of Processing Activities (RoPA)	XX					XX	XX	XX	XX
	d. Data Discovery inventory & Data Classification Personal Data Lineage and cataloguing	XX					XX	XX	XX	XX
	e. Data Privacy Assessments	XX					XX	XX	XX	XX
	f. Data Principal Rights Management	XX					XX	XX	XX	XX
	g. Data Protection Impact Assessments (DPIA)	XX					XX	XX	XX	XX
	h. Privacy Notice Management	XX					XX	XX	XX	XX
	i. Data and Privacy Breach Management	XX					XX	XX	XX	XX

Signature of the Bidder with company Seal

2.	j. Compliance Monitoring, Reporting and Governance Dashboard	XX					XX	XX	XX	XX
	k. Third Party Risk Management	XX					XX	XX	XX	XX
	l. Any other Software/ Licenses to comply DPDP act and rules	XX					XX	XX	XX	XX
	AMC / ATS Cost of the above Mention Items in SI No. 1									
	a. Consent Management		XX	XX	XX	XX	XX	XX	XX	XX
	b. Cookie Consent Management		XX	XX	XX	XX	XX	XX	XX	XX
	c. Record of Processing Activities (RoPA)		XX	XX	XX	XX	XX	XX	XX	XX
	d. Data Discovery inventory & Data Classification Personal Data Lineage and cataloguing		XX	XX	XX	XX	XX	XX	XX	XX
	e. Data Privacy Assessments		XX	XX	XX	XX	XX	XX	XX	XX
	f. Data Principal Rights Management		XX	XX	XX	XX	XX	XX	XX	XX
	g. Data Protection Impact Assessments (DPIA)		XX	XX	XX	XX	XX	XX	XX	XX
	h. Privacy Notice Management		XX	XX	XX	XX	XX	XX	XX	XX
	i. Data and Privacy Breach Management		XX	XX	XX	XX	XX	XX	XX	XX
	j. Compliance Monitoring, Reporting and Governance Dashboard		XX	XX	XX	XX	XX	XX	XX	XX

Signature of the Bidder with company Seal

k. Third Party Risk Management		XX	XX	XX	XX	XX	XX	XX	XX
l. Any other Software/ Licenses to comply DPDP act and rules		XX	XX	XX	XX	XX	XX	XX	XX

Note: 1. The Bidder should separately quote the cost of the tool for above line items. The Bank reserves the right not to procure the tool for all. However, if the Bank chooses to use the tool for the entire dataset, the quoted price shall be payable to the bidder.

2. Delivery of Software licence should be delivery of Hardware and required Infrastructure for the proposed solution and confirmation from the Bank.

Table-C

One-time Gap Assessment and Implementation Cost

[Amount in Indian Rupees]

Sl. No.	Description	Total cost (excl. of taxes)	Tax for column "a"		Total cost (incl. of tax)
			% of tax	Tax amt.	
		A	b	c	d=a+c
1.	Study the Bank System GAP Assessment, prepare a Roadmap / Approach / Implementation Plan and Implement the solution, Policy review and framework design etc for Complete Compliance of DPDP Act 2023 and Rules 2025.	XX	XX	XX	XX
2.	Implementation cost for DC, DRC & UAT infrastructure of Various Modules	XX	XX	XX	XX
Total cost for One-time Gap Assessment and Implementation					XX

Note - The Bidder shall include the cost of a one-time independent third-party compliance audit for DPDP Act, 2023 and DPDP Rules, 2025, along with CERT-In empanelled VAPT, including audit execution, reporting, remediation validation, re-testing, and submission of closure reports.

Signature of the Bidder with company Seal

Table-D

Cost for any additional requirements /additional customization/ enhancement / Additional Application Integration

[Amount in Indian Rupees]

Sl. No.	Description	Charges Per Man day / Integration (Excl. of Tax)	No. of man days/ 20 Integration for 5 Years #	Total Cost (Excl. of Tax)	Tax for column d		Total Cost (Incl. of Tax)
					% Tax	Tax amt.	
		A	B	c=(a*b)	d	E	f=c+e
1.	Cost for any additional requirements/ additional customization/ enhancement	XX	100	XX	XX	XX	XX
2.	Additional Application Integration Cost for 20 Integration	XX	20	XX	XX	XX	XX
3.	Total Cost for any additional requirements/ additional customization/ enhancement / Additional Application Integration						XX

The price quoted by the bidder is fixed for entire contract period of 5 year and number of man days and Additional Application Integration mentioned above is indicative only. However, the no. of man-days and Additional Application Integration may vary from time to time in total and utilize after Go-Live of the proposed solution.

Table – E

Charges for Onsite Resources Post Go-live

[Amount in Indian Rupees]

Sl. No.	Description	Charges for one resource per month [excl. of taxes]	No. of months	No. of resources	Total charges for resources for 5 years [excl. of taxes]	Tax for column d		Total charges for 5 years [incl. of taxes]
						% of tax	Tax Amt.	
		A	B	C	d=a*b*c	e	F	g=d+f
1	Project Manager/Team Lead	XX	60	1	XX	XX	XX	XX
2	Infrastructure Engineer /System Administrator support/Database Administrator	XX	60	4	XX	XX	XX	XX
3	Application Support Engineer	XX	60	4	XX	XX	XX	XX

Signature of the Bidder with company Seal

Total Charges of Onsite Resources:

Note: The Bank reserves the right to increase or decrease the number of deployed resources during the five-year contract period based on business and operational requirements. Any addition or deletion of resources shall be communicated by the Bank, and payments shall be made on a pro-rata basis from the date of deployment or withdrawal. The bidder shall ensure uninterrupted 24x7x365 availability of qualified L2/L3 resources after Go-Live. Any additional manpower required to meet support, operational, SLA, or business continuity requirements shall be provisioned by the bidder at no extra cost to the Bank and must be included in the commercial bid.

Table-F
Total Cost of Training

Sl. No.	Description	Total cost (excl. of taxes)	Tax for column "a"		Total cost (incl. of tax)
			% of tax	Tax amt.	
		A	b	c	d=a+c
1.	Functional Training for users	XX	XX	XX	XX
2.	Technical Training, Knowledge Transfer and Capacity Building to take over the activities by the Bank Team.	XX	XX	XX	XX
Total cost for Training					

Table-G
Total Cost of Ownership for 5 Years Contract Period

Sl. No.	Particulars	Details	Total Cost (Exclusive of taxes)	Total Cost (Inclusive of taxes)
1	Hardware and Infrastructure	Total Cost of Hardware , System Software as per Table-A	XX	XX
2	Data Privacy & Consent Management Solution	Total Cost for Enterprise Perpetual License cost as per Table-B	XX	XX
		Total Gap Assessment and Implementation Cost as per Table-C	XX	XX
		Total Cost for any additional requirements /additional customization/ enhancement / Miscellaneous as per Table-D	XX	XX
3	Support & Training	Total Cost for Onsite Resources as per Table-E	XX	XX
		Total Cost for Training as per Table-F	XX	XX

Signature of the Bidder with company Seal

		Total Cost of Ownership for a period of 5 years (Sum of Sr. No. 1 to 3)	XX	XX
		TCO in words		

[Amount in Indian Rupees]

Undertaking

- Bill of material is submitted on the letter head and is signed by an Authorized Signatory with Name and Seal of the Company.
- We confirm that we have gone through RFP clauses, subsequent amendments and replies to pre-bid queries (if any) and abide by the same.
- We have not changed the structure of the format nor added any extra items. We note that any such alternation will lead to rejection of Bid.
- We agree that no counter condition/assumption in response to commercial bid will be accepted by the Bank. Bank has a right to reject such bid.
- We are agreeable to the payment schedule as per "Payment Terms" of the RFP.

Date:

Place:

Signature with seal

Name:

Designation

The Bidder is expected to ensure compliance with the stated guidance.

Instructions	
S.No	Guidelines
	Summary of Total Cost
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.
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.

Signature of the Bidder with company Seal

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 <u>masked</u> 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	The Bidder must provide an unconstrained, Enterprise-Wide Perpetual License for all proposed modules, tools, and components. The commercial model must be strictly on a fixed-cost basis. The Bank explicitly prohibits any consumption-linked pricing models, including but not limited to variable transaction fees, per-API call charges, data volume thresholds, or user/branch/device count limitations. No additional commercial charges or subscription upgrades shall be payable due to the scaling of digital transaction volumes, data queries, or the onboarding of new applications and channels during the entire contract period
16	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.

Signature of the Bidder with company Seal

II	Hardware
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 , model 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.
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
IV	Installation, Implementation & Migration
1	Bidder shall comply to the Installation & commissioning, implementation scope provided in the RFP
2	Bidder should quote for end-to-end Installation & commissioning, implementation 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.
V	AMC & ATS
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.
3	The AMC, ATS costs for Production DC & DR have to be quoted separately
4	If required, the Bidder has to create additional line items in this section.
VI	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

Signature of the Bidder with company Seal

Annexure 3: Bidder's Information

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

#	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 Design, Supply, Install, Manage and Maintenance of Privacy & Consent Management Solution & 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:

Signature of the Bidder with company Seal

Annexure 4: Letter for Conformity of Product as per RFP

Date

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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:

Signature of the Bidder with company Seal

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 Signature of the Bidder with company Seal

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

Signature of the Bidder with company Seal

‘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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

With reference to RFP for **RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules:**

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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

With reference to RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025:

We understand that Bank shall be placing Order to the Successful Bidder inclusive of taxes only.

1. We shall be responsible for payment of all applicable GST and other indirect taxes, if any, in accordance with the applicable provisions of law in respect of the goods and/or services supplied under the Contract.
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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Dear Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Sir,

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.

The model(s) / product(s) proposed in this contract is covered under 3 Years onsite comprehensive warranty & support from the date of installation of product. Further, we assure you that the said product will not attain end of support upto 5 years from the date of supply.

We hereby extend our warranty as per terms & conditions of the RFP and the agreement, for the equipment and services supplied/offered against this RFP by the above-mentioned Bidder, and hereby undertake to perform the obligations as set out in the RFP in respect of such equipment and services.

We assure you that in the event of M/s not being able to fulfill its obligation in respect of the warranty terms for the hardware supplied, as defined in the RFP, (OEM Name) would continue to meet these warranty obligation either directly or through alternate arrangements 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)

Signature of the Bidder with company Seal

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

Signature of the Bidder with company Seal

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 21**.

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: _____

Signature of the Bidder with company Seal

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

Signature of the Bidder with company Seal

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 even after termination / expiry of contract.

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;

Signature of the Bidder with company Seal

- 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 End to End Design, Supply and Implementation of Data Privacy & On-premise Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025 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 **End to End Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025** 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

Signature of the Bidder with company Seal

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:-

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)

Signature of the Bidder with company Seal

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 ----- 2026 at -----

For and on behalf of ----- Bank.

sd/- -----

Annexure 12: Technical Evaluation Sheet

Bank will evaluate the technical proposals of all eligible Bidders based on the documents submitted for the below mentioned criteria:

Sl. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted For award of mark
1.	<u>Functional Coverage of proposed solution – DPDPA Scope of Work</u> The <u>proposed solution/platform</u> should have capabilities of all 11 modules with at least five module including 1,2 & 4 are mandatorily <u>implemented or under implementation</u> (The purchase order /Contract for under implementation must have been issued at least three month prior to the date of publishing of this RFP) in a single or separate project (Module. No. 1–11): 1. Consent Management 2. Cookie Consent Management 3. Record of Processing Activities (RoPA) 4. Data Discovery, Inventory, Classification & Data flow Mapping 5. Data Privacy Assessments 6. Data Principal Rights Management 7. Data Protection Impact Assessments (DPIA) 8. Privacy Notice Management 9. Data Breach Management 10. Compliance Monitoring, Reporting and Governance Dashboard 11. Third Party Risk Management.	Compliance Scoring (20 Marks): • Implementations>= 10 modules: 20 Marks • Implementations>= 8 and <10modules :16 Marks • Implementations>= 5 and <= 7 modules :12 Marks	20	The Bidder/OEM has to provide relevant purchase order/work order/engagement letter along with satisfactory reference letter/e-mail from the client confirming the details of the modules implemented or under implementation provided along with Name, Designation, Contact details.

2.	<u>Bidder /OEM Module wise implementation experience (Global/ India)</u> The Bidder/OEM must have <u>implemented or under implementation</u> of Modules 1 to 11 across BFSI or other enterprise environments during the last five(5) years as on the date of issuance of this RFP. The implementation must encompass regulatory compliance, operational and technology requirements relevant to the proposed solution.	Module-Wise Scoring (Max 20 Marks): 1. Consent Management – 3 Marks 2. Cookie Consent Management – 1 Marks 3. Record of Processing Activities (RoPA) – 3 Marks 4. Data Discovery, Inventory , Classification & Data Flow Mapping -2 Marks 5. Data Privacy Assessments -2 Marks 6. Data Principal Rights Management -3 Marks 7. Data Protection Impact Assessments (DPIA) -2 Marks 8. Privacy Notice Management -1 Marks 9. Data Breach Management-1 Marks 10. Compliance Monitoring, Reporting and Governance Dashboard -1 Marks 11. Third Party Risk Management. - 1 Marks	20	For each cited project:- Purchase Order / Work Order / Engagement Letter-Completion certificate / Reference letter / Client email reference- Client email from official ID with name, designation, contact number- Project brief mapping to modules.
3.	<u>Number of Implementation Experience (Global / India)</u> The Bidder /OEM must have Implementation experience of privacy and Data protection governance to ensure compliance of DPDPA/GDPR etc .The Project/ Engagement should have been <u>implemented or under implementation</u> in	Number of Project/Engagement implemented or Under Implementation (Project Count- Based Scoring Maximum :12 Marks) • Each Implementation :3 Marks • Each Under Implementation: 2 Marks	12	For each cited project:- Purchase Order / Work Order / Engagement Letter-Completion certificate / Reference letter / Client email reference- Client email from official ID with name, designation, contact number- Project brief mapping to modules.

Signature of the Bidder with company Seal

	BFSI / large enterprises (preferably ≥ 50 Lakhs Customer Base or equivalent complexity) before the date of issuance of this RFP.			
4.	<u>Project Team Capability</u> Competency of Professionals (Project Team Capability) Technical competency of professionals proposed for DPDP implementation in the Bank (Gap Assessment, Integration Implementation & OEM Support)	Team Competency Scoring (Max 8 Marks): A) Privacy Certifications Any of the Below (Max 3 Marks): (IAPP - CIPP/E, CIPP/US, CIPP/A, CIPP/C etc.), ISO/IEC 27701 (PIMS), ISC2 - Systems Security Certified Practitioner (SSCP), Certified Information Systems Security Professional (CISSP), Certified in Governance, Risk and Compliance (CGRC), Certified Secure Software Lifecycle Professional (CSSLP) etc.,) ISACA - Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Certified Data Privacy Solutions Engineer (CDPSE) or equivalent : I. $\geq 40\%$ team certified: 3 Marks II. $\geq 30\% < 40\%$ certified: 2 Marks III. Else : 0 Marks B) Integration &	8	Profile Details of proposed resources for Project Implementation - Certification proofs duly verified by the Bidder- Deployment plan & resource matrix- Undertaking on availability as per Bank schedule

		Engineering Skills (Max 2 Marks): Skilled in REST APIs, JSON/XML, modern web/mobile tech skilled I. $\geq 50\%$: 2 marks II. $\geq 40\% < 50\%$: 1 marks III. Else : 0 Marks C) Resources from OEM during Implementation (Max 3 Marks): I. $\geq 30\%$ out of total resource:3 marks II. $\geq 10\% < 30\%$ out of total resource:2 marks III. Else : 0 Marks		
5.	Bidder's Presentation	Points will be assigned by an internal committee as per Table A-1 1. Understanding of Scope & Bank Requirements 2. Relevant Experience & Case Studies 3. Functional and Technical features, capabilities, strength, richness of the proposed solution: 4. Technical Approach & Implementation Strategy: 5. Solution Architecture: 6. Governance & Compliance:	20	Presentation to be conducted as per the schedule provided by Bank.

6.	Technical Presentation cum Demo (On-Premises Demonstration)	Points will be assigned for proposed 11 Module by an internal committee as per Table B-1	20	Demo to be conducted as per the schedule provided by Bank.
Total Maximum Marks			100	

Note: The bidder should score minimum 70% of marks out of 100 marks for qualifying under Technical Evaluation. The bidders qualified under Technical Evaluation will be eligible for commercial opening.

Presentation of proposal:

Central Bank of India will schedule the presentations and intimate the time and locations to the bidders. Failure of a bidder to complete a scheduled presentation may result in the rejection of that Bidder's proposal.

Table A-1

Sl. No.	Presentation Agenda	Maximum Marks
1.	Understanding of Scope & Bank Requirements: Understanding of Bank context, objectives, target operating model, and current landscape awareness.	3
2.	Relevant Experience & Case Studies: Privacy automation at BFSI scale (preferably ≥ 50 Lakhs Customer Base or equivalent complexity); challenges, approach, outcomes, metrics, testimonials.	3
3.	Functional and Technical features, capabilities, strength, richness of the proposed solution: Completeness, maturity, scalability, security, and compliance capabilities of the proposed solution, including coverage of all functional requirements, integration capabilities, automation, reporting, and user experience	4
4.	Technical Approach & Implementation Strategy: Project plan, milestones, go-live plan, risk & mitigation strategy.	3
5.	Solution Architecture: On Prem (DC/DR/UAT/DEV) deployment architecture, workflow, Secure integration Layer (APIs & Connectors)	4

Signature of the Bidder with company Seal

6.	Governance & Compliance: DPDPA governance including consent & purpose limitation, rights handling, accountability, continuous monitoring, and regulatory alignment and updates.	3
	Maximum Marks for Presentation	20

Table B-1

The bidder/OEM shall provide a comprehensive module-wise demonstration of the proposed solution during the technical evaluation stage. The demo environment shall include at least 1,000 pre-loaded sample records/entries, wherever applicable, to adequately demonstrate the functionality, workflows, scalability, automation capabilities, dashboards, reports, and performance of the proposed solution.

The demonstration shall cover all proposed modules and key business/use cases relevant to the Bank's requirements under the Digital Personal Data Protection (DPDP) Act, 2023 and DPDP Rules, 2025. The bidder shall clearly demonstrate how the proposed solution enables compliance with the provisions of the DPDP Act, 2023, applicable Rules, MeitY guidelines/advisories, RBI regulatory expectations, and CERT-In directions, wherever applicable.

The bidder shall also highlight the unique features, differentiators, advanced capabilities, AI/ML-enabled features (if any), automation capabilities, and value-added functionalities of the proposed solution in comparison with other leading/top market solutions available in the industry.

Sl. No.	Module	Maximum Marks
1.	Consent Management	3
2.	Cookie Consent Management	1
3.	Record of Processing Activities (RoPA)	3
4.	Data Discovery, Inventory , Classification & Data Flow Mapping	2
5.	Data Privacy Assessments	2
6.	Data Principal Rights Management	3
7.	Data Protection Impact Assessments (DPIA)	2
8.	Privacy Notice Management	1
9.	Data Breach Management	1
10.	Compliance Monitoring, Reporting and Governance Dashboard	1
11.	Third Party Risk Management	1
	Maximum Marks for Demo	20

Bidders scoring 70% or more marks will be considered eligible in technical evaluation and shall be eligible for further process of evaluation

In case there is only one bidder having technical score of 70% or more, the Bank may, at its sole discretion, also consider to reduce the threshold of 70%.

Signature of the Bidder with company Seal

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Final Technical Score Summary

Section	Max Marks	Minimum Qualifying Marks	Marks Awarded
Functional Coverage of solution – DPDPA Scope of Work	20	10	
Module wise implementation experience	20	10	
Bidder/OEM Implementation Experience	12	6	
Competency of Professionals (Project Team Capability)	8	4	
Bidder's Presentation	20	10	
Technical Presentation cum Demo (On-Premises Demonstration)	20	10	
Total	100	*	

*The above section wise minimum marks are mandatory for qualification. However, the bidder must secure an aggregate technical score of minimum 70 out of 100 for qualification.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Signature of the Bidder with company Seal

Annexure 13: Bid Security (BG Format- for Earnest Money Deposit)

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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:

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)

Signature of the Bidder with company Seal

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

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

#	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:

Signature of the Bidder with company Seal

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,

**Data Protection Officer
Data Protection Cell,
RMD , Central Bank Of India
1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026 RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules

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

Signature of the Bidder with company Seal

Annexure 16: NPA UNDERTAKING

Performa of 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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026 RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules

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:

Annexure17: Land Border Sharing Undertaking Letter

(This undertaking should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026 RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025

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]"

Signature of the Bidder with company Seal

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. _____

Signature of the Bidder with company Seal

Annexure 18: Cover Letter

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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)

Signature of the Bidder with company Seal

Annexure 19: Escalation Matrix

Ref: Tender No - **GEM/2026/B/ 7977310 dated 31/08/2026**

Date: -

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point, Mumbai 400 021.

Sir,

Reg: RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025

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:

Signature of the Bidder with company Seal

Annexure 20: Query Format

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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)

Signature of the Bidder with company Seal

Annexure 21: Guidelines on Banning of Business Dealing

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

Signature of the Bidder with company Seal

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

Signature of the Bidder with company Seal

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 Data Protection Officer 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;

Signature of the Bidder with company Seal

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 Signature of the Bidder with company Seal

& 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 Signature of the Bidder with company Seal

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/ 7977310 dated 31/08/2026

Date: -

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sir,

**Reg:- RFP for Design, Supply and Implementation of Data Privacy & Consent
Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA)
2023 & DPDP Rules 2025**

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

Signature of the Bidder with company Seal

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, Hardware, Cryptographic Bill of Material Format]

Ref: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Date: -

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Reg:- RFP for Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025

Note – In case of multiple software , hardware and cryptography component, please provide the details of all software and cryptographic bill of material separately having following required data fields.

Format - Software Bill of Material (SBOM)

Sl No	Data Field	Description	Details to be furnished by Bidder
1	Component Name	The name of the software component or library included in the SBOM.	
2	Component Version	The version number or identifier of the software component.	
3	Component Description	A brief description or summary of the functionality and purpose of the software component.	
4	Component Supplier	The entity or organization that supplied the software component, such as a vendor, third-party supplier, or open- source project	
5	Component License	The license under which the software component is distributed, including details such as the license type, terms, and restrictions.	
6	Component Origin	The source or origin of the software component, such as whether it is proprietary, open-source, or obtained from a third-party vendor.	

Signature of the Bidder with company Seal

7	Component Dependencies	Any other software components or libraries that the current component depends on, including their names and versions.	
8	Vulnerabilities	Information about known security vulnerabilities or weaknesses associated with the software component, including severity ratings and references to security advisories or CVE identifiers	
9	Patch Status	The patch or update status of the software component, indicating whether any patches or updates are available to address known vulnerabilities or issues	
10	Release Date	The date when the software component was released or made available for use	
11	End-of-Life (EOL) Date	The date when support or maintenance for the software component is scheduled to end, indicating the end of its lifecycle	
12	Criticality	The criticality or importance of the software component to the overall functionality or security of the application, often categorized as critical, high, medium or low.	
13	Usage Restrictions	Any usage restrictions or limitations associated with the software component, such as export control restrictions or intellectual property rights	
14	Checksums or Hashes	Cryptographic checksums or hashes of the software component files to ensure integrity and authenticity	
15	Comments or Notes	Additional comments, notes, or annotations relevant to the software component or its inclusion in the SBOM	
16	Author of SBOM Data	The name of the entity that creates the SBOM data for this component.	
17	Timestamp	Record of the date and time of the SBOM data assembly	
18	Executable Property	Attributes indicating whether a component within an SBOM can be Executed.	
19	Archive Property	Characteristics denoting if a component within an SBOM is stored as an archive or compressed file	
20	Structured Property	Descriptors defining the organized format of data within a component listed in an SBOM.	

21	Unique Identifier	A unique identifier is a distinct code assigned to each software component,	
----	-------------------	---	--

Format - Cryptographic Bill of Material

Cryptographic Asset Type	Element	Description	Details to be furnished by Bidder
Algorithms	Name	The name of the cryptographic algorithm or asset. For example, "AES-128-GCM" refers to the AES algorithm with a 128-bit key in Galois/Counter Mode (GCM).	
	Asset Type	Specifies the type of cryptographic asset. For algorithms, the asset type is "algorithm"	
	Primitive	Describes the cryptographic primitive. For "SHA512withRSA", the primitive is "signature" as it's used for digital signing.	
	Mode	The operational mode used by the algorithm. For example "gcm" refers to Galois/Counter Mode used with AES encryption	
	Crypto Functions	The cryptographic functions supported by the asset. For example, the functions in the case of "AES-128-GCM" are key generation, encryption, decryption, and authentication tag generation.	
	Classical security level	The classical security level represents the strength of the cryptographic asset in terms of its resistance to attacks using classical (non-quantum) methods. For AES-128, it's 128 bits.	
	OID	The Object Identifier (OID) is a globally unique identifier used to refer to the algorithm. It helps in distinguishing algorithms across different systems. For example, "2.16.840.1.101.3.4.1.6" for AES128-CM, "1.2.840.1.13549.1.1.13" for SHA512 with RSA.	
	List	List the cryptographic algorithms employed by the quantum device or	

Signature of the Bidder with company Seal

		system, allowing for an assessment of its security capabilities, especially in the context of post-quantum encryption standards.	
Keys	Name	The name of the key, which is a unique identifier for the key used in cryptographic operations	
	Asset Type	Defines the type of cryptographic asset. For keys, the asset type is typically "key".	
	Id	A unique identifier for the key such as a key ID or reference number.	
	State	The state of the key, such as whether it is active, revoked or expired	
	Size	The size of the key, typically measured in bits. For example, a 128-bit key or a 2048-bit RSA key	
	Creation Date	The date when the key was created.	
	Activation Date	The date when the key became operational or was first used.	
Protocols	Name	The name of the cryptographic protocol, such as TLS, IPsec, SSH, etc.	
	Asset Type	Defines the type of cryptographic asset. In this case, it would be a "protocol".	
	Version	The version of the protocol used, such as TLS 1.2, TLS 1.3, etc	
	Cipher Suites	The set of cryptographic algorithms and parameters supported by the protocol for tasks like encryption, key exchange and integrity checking.	
	OID	The (OID) associated with the protocol, identifying its unique specifications.	
Certificates	Name	The name of the certificate, typically referring to its subject or the entity it represents (e.g., a website)	
	Asset Type	Defines the type of cryptographic asset. For certificates, the asset type	

		is "certificate"	
	Subject Name	This refers to the Distinguished Name (DN) of the entity that the certificate represents. It typically contains information about the organization, domain name	
	Issuer Name	The issuer is the Certificate Authority (CA) that issued and signed the certificate. This field contains the DN of the CA that verified and issued the certificate.	
	Not Valid Before	This specifies the date and time from which the certificate is valid.	
	Not Valid After	This specifies the expiration date and time of the certificate. The certificate becomes invalid after this timestamp.	
	Signature Algorithm Reference	This refers to the cryptographic algorithm used to sign the certificate. It provides a reference to the algorithm and its OID (Object Identifier).	
	Subject Public Key Reference	This points to the public key used by the subject (the entity being identified in the certificate). It provides a reference to the key's details, including the algorithm.	
	Certificate Format	Specifies the format of the certificate. Common formats include X.509, which is the most widely used format for certificates.	
	Certificate Extension	This refers to the file extension associated with the certificate. It is commonly .crt for certificates in the X.509 format.	

Format - Hardware Bill of Material

Sl No	Element	Description	Details to be furnished by Bidder
1	Product Name	The common or marketing name of the hardware item.	
2	Product Version	The specific iteration or release number of the product.	
3	Product Details	Key specifications and features that describe the hardware	

Signature of the Bidder with company Seal

4	Warranty/AMC	Information regarding the product's guarantee and any annual maintenance contract.	
5	Manufacturer Name	The name of the company responsible for producing the hardware.	
6	Manufacturer Location	The geographical address of the product's manufacturer.	
7	Manufacturing Date	The specific date when the product was produced.	
8	Supplier Information	Details about the company that provided or sold the product.	
9	Supplier Location	The geographical address of the product's supplier.	
10	Model Number	A specific alphanumeric identifier for a particular product design.	
11	Serial Number	A unique identifier assigned to each individual unit of a product for tracking.	
12	Technical Specification	Detailed technical characteristics and performance parameters of the component (e.g., voltage, frequency, capacity).	
13	Supplier Information	The name and contact details of the company that supplied the component to the manufacturer of the larger product.	
14	Supplier Location	The geographic location (city, country) of the direct supplier of the component.	
15	Technology Node	For integrated circuits, this refers to the semiconductor manufacturing process technology (e.g., 7nm, 14nm), indicating its feature size and generation.	
16	Compliance	Declarations or certifications indicating adherence to relevant industry standards, regulations, or environmental directives	

Signature of the Bidder with company Seal

		(e.g., RoHS, CE).	
17	Power supply	Details about the component's power requirements, such as voltage, current, and wattage.	
18	License Information	Any associated intellectual property licenses or usage terms, particularly relevant for firmware or embedded software within the component.	
19	Test Result	Information about the component's performance during quality assurance or functional testing, indicating its operational status.	
20	Sub-component	This refers to the recursive nature of an `; if a component itself contains further distinct hardware parts, those would also be listed with similar detailed attributes.	

The bidder must submit only such document as assurance regarding the accuracy, completeness and timelines of SBOM, HBOM, CBOM & AIBOM.

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

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?		

Signature of the Bidder with company Seal

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

Signature of the Bidder with company Seal

Annexure 25: Bidder's Particulars on Company Letter Head:

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Subject: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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:

Signature of the Bidder with company Seal

Annexure 26: List of Hardware and Software Components:

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Format 7.12- Infrastructure for the Solution

a. Instance or Server details:

Bidder must submit the required details for each layer in solution/platform covering all layers but not limited to WEB, APP, DB in the following format:

Application name	Application instance / Module name	Env	Application tier	Physical Server / Virtual instance	H/w Platform (x86 or other please specify)	Cluster Type (Active-Active/ Active Passive)	No. of Physical cores	No. of Virtual Cores	Memory in (GB)	Operating system with version	Database with version	Database type (Server based / User based / Core based, etc.)	Runtime Components (Example - .NET Framework, Oracle's JRE/Java, OpenJDK etc)	Third party's libraries/software/API/SDK	MiddleWare Components (Example-JBOSS EAP,TOMCAT, WEBLOGIC,WEBSFHERE etc)	Usable Storage capacity (GB)	Load balancer type (Application based / Appliance based /NA)

Signature of the Bidder with company Seal

Application name	Application instance / Module name	Env	Application tier	Physical Server / Virtual instance	H/w Platform (x86 or other please specify)	Cluster Type (Active-Active/ Active Passive)	No. of Physical cores	No. of Virtual Cores	Memory in (GB)	Operating system with version	Database with version	Database type (Server based / User based / Core based, etc.)	Runtime Components (Example - .NET Framework, Oracle's JRE/Java, OpenJDK etc)	Third party's libraries/software/API/SDK	MiddleWare Components (Example-JBOSS EAP,TOMCAT, WEBLOGIC,WEBSFHERE etc)	Usable Storage capacity (GB)	Load balancer type (Application based / Appliance based /NA)

b. Link Requirement:

Link reference	From	To	Primary / Secondary link	Purpose	Type of link	Bandwidth (in Mbps)
Link1						
Link2						
Link3						

Signature of the Bidder with company Seal

(Application OEM to add)

Note:

1. Considering the integration that may be required with on-premises deployment (existing applications)
2. **Bidder to enclose the benchmarking report of their application done by any reputed agencies to substantiate their infrastructure.**
3. **All requisite software licenses including middleware / application / tool licenses should be offered as part of the solution.**
4. The licenses may be delivered in paper form or electronic form.

c. Any Other

Any other information that could not be captured in "Infra details" or "Bandwidth requirement" to be included in this table

SL.No.	Description	Purpose	Qty

Signature of the Bidder with company Seal

SL.No.	Description	Purpose	Qty

Authorised Signatory:

Name and Designation:

Office Seal with date

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Signature of the Bidder with company Seal

Annexure 27: Letter for Refund of EMD

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

To,

**Data Protection Officer
Data Protection Cell,
RMD , Central Bank Of India
1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

We (Company Name) had participated in the Request for Proposal (RFP) bearing reference no. **Bid Number: GEM/2026/B/ 7977310 dated 31/08/2026** for **Design, Supply and Implementation of Data Privacy & Consent Management Solution/Tools as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025** 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:

Signature of the Bidder with company Seal



Design, Supply and Implementation of Data Privacy & Consent
Management Solution/Tools as per Digital Personal Data
Protection Act (DPDPA) 2023 & DPDP Rules 2025

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Signature of the Bidder with company Seal

Annexure 28: Format for Submission of Client References by Bidder.

To,

Data Protection Officer
Data Protection Cell,
RMD , Central Bank Of India
1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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

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

* Platform Implementation / Platform Setup / Facility Management etc

**Delivery/ Installation/ Implementation/ Designing/ Development/ Maintenance / maintenance etc

referenced Project must be no earlier than five (5) years from the Bid Submission Date

The documentary proof of the client reference is enclosed.

Yours faithfully,

Signature of Authorized Signatory: Name of Signatory: Designation: Seal of Company:	Date: Place:
--	-------------------------------

Signature of the Bidder with company Seal

Annexure 29: 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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

We hereby undertake to comply with the regulations of Digital Personal Data Protection Act (DPDPA 2023), Digital Personal Data Protection Rules 2025 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.

The obligations contained in this undertaking shall survive even after the expiry or termination of the Contract and shall continue for so long as the Bidder possesses or has access to the Bank's Confidential Information or Personal Data

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Signature of the Bidder with company Seal

Annexure 30: Undertaking for 5 Years Roadmap:

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

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

We, _____ hereby confirm that as a bidder and the product provider, would Design, Supply, Install, Manage and Maintenance of **Data Privacy & Consent Management Tool as per Digital Personal Data Protection Act (DPDPA) 2023 & DPDP Rules 2025**. We also commit to support the proposed **Data Privacy & Consent Management Solution/Tools** 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 31: 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,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Bidder Name:

This is to certify that the RFP bearing reference no. **Bid Number: GEM/2026/B/.....**

**..... 2026 for Design, Supply and Implementation of Data Privacy & Consent
Management Tool as per Digital Personal Data Protection Act (DPDPA) 2023 &
DPDP Rules 2025** 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:

Signature of the Bidder with company Seal

Annexure 32: Proposed Team Profile:

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Sl NO.	Name of the Role (Product Owner/ Solution Architect etc)	Name of the Resource	Experience in Years	Education Qualification (Btech/ Mtech etc)	Certifications	Expertise / Skill set	Remarks/ Comments

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

Signature of the Bidder with company Seal

Annexure 33: Volumetrics

Below Indicative details are provided for the sizing of the proposed solution. However, Actual count may increase or decrease over the period and detail will be provided with the successful bidder for implementation of the proposed solution may change at the time of initiation. Bidder should factor additional 10% provisioning for each year of the proposed solution including hardware infrastructure & Licenses as per below indicative volumetrics during the contract period. The volumetric information provided by the Bank is indicative and intended solely for bid preparation. Actual volumes may vary during implementation.

Sr No	Item	Count (Approx)
1	No of Branches	4606
2	No of Region	90
3	No of Zone	14
4	No of BC Outlets	13890
5	No of BC Max Centres	30
6	Total ATMs	3820
8	No of Application	150
9	No of Mobile Application	12
10	No of Database	541
11	No of End Points / Computers in the Bank	40000
12	No of Customers*	85000000
13	No of Internal and External Application API Integration	743

*Sizing to be done for Approx 10 Crore customers

Annexure 34 Declaration of Source Code Audit

(To be submitted by Bidders on their letter head)

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

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 35: Technical/functional Specifications

(To be submitted with technical bid on the letter head of the bidder)

Support of following in the Proposed application Non-compliance to any of the specification shall entail rejection of the bidder

S No	Module	Description	Compliance (Yes/No)
1	Consent Governance	The solution should have ability to support configurable parameters (e.g. Country or Business Unit) to store consents with any data aligned with your business needs	
2	Consent Governance	The solution should have ability to support a comprehensive universal consent compliance audit trail	
3	Consent Governance	The solution should have ability to track all changes of consent by date and ID	
4	Consent Governance	The solution should have ability to support filtering on the reporting dashboard	
5	Consent Governance	The solution should have ability to locate the user and review his or her consents through API commands	
6	Consent Governance	The solution should have ability to support the ability to bulk import consents	
7	Consent Governance	The solution should have ability to support a Form JS that automatically captures and stores consent from forms	
8	Consent Governance	The solution should have ability to flexible Consent API's for universal consent and preference management	
9	Consent Governance	The solution should have ability to support consumer authentication through email verification for a Preference Center	
10	Consent Governance	The solution should have ability to support configuring fields on the Preference Center like branding and logo customization	
11	Consent Governance	The solution should have capability to bifurcate / isolate consents of multiple BU's / internal ORG's / Units into separate dashboard without allowing visibility to each other consents.	
12	Consent Governance	The platform should have capability to host webhooks for advance integration with other applications to collect / read consents using API methods.	
13	Consent Governance	The system should support end-to-end consent lifecycle including collection, renewal, expiry, and revocation tracking with audit trails.	
14	Consent Governance	The system should enable tagging of each consent to specific purposes and personal data identifiers as defined	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
		by the organization's data processing structure.	
15	Consent Governance	The system should auto-generate consent notices in all 22 official Indian languages as per Schedule 8 of the Constitution.	
16	Consent Governance	The system should create immutable consent artefacts as per MeitY's Electronic Consent Framework.	
17	Consent Governance	The system should store granular, timestamped, and purpose-specific consent artifacts for each data principal and should be retrievable through APIs.	
18	Consent Governance	The system should allow mapping of consents to specific business processes to ensure contextual granularity.	
19	Consent Governance	The system should automatically manage expiry of consents based on legal or business- defined retention timelines.	
20	Consent Governance	The system should be able to issue downloadable consent receipts to data principals with purpose and timestamp references.	
21	Consent Governance	The system should maintain a versioned history of consents granted for each business process and revoked over time.	
22	Consent Governance	The system should provide an authenticated interface where data principals can view and manage their consents.	
23	Consent Governance	The system should offer real-time analytics on consent status segmented by purpose, language, geography, etc.	
24	Consent Governance	The solution should have ability to support a wide variety of collection points. i.e Branches, BC points, digital journeys etc.	
25	Consent Governance	The solution should have ability to track data principal consent by purpose of processing and subgroups/topics of processing purposes. Verifiable Parental Consent: For children (under 18) or disabled persons, obtain verifiable parental/guardian consent before processing, using methods like DigiLocker. No Tracking/Profiling of Children: Behavioral monitoring, targeted advertising, or profiling of children is prohibited.	
26	Consent Governance	The solution should have ability to support configurable parameters in Universal Consent API	
27	Cookie Manager	The solution should have ability to allow Bank to configure cookie categories and cookie category descriptions	
28	Cookie Manager	The solution should have ability to allow Bank to configure text and links on the cookie banner	

S No	Module	Description	Compliance (Yes/No)
29	Cookie Manager	The solution should have ability to have the ability to create a customized cookie banner for each scanned website	
30	Cookie Manager	The solution should have ability to record cookie consent of Bank website visitors	
31	Cookie Manager	The solution should have ability to offer a robust reporting suite so a user can view cookie consent rates down to a category level by domain	
32	Cookie Manager	The solution should have ability to configure "consent" to be? For example, "opt out of all" or "opt out of one or more", etc.	
33	Cookie Manager	The solution should have ability to support different cookie consent compliance types/models for Bank to choose from	
34	Cookie Manager	The solution should have ability to support cookie policy versioning to ask users for re-consent	
35	Cookie Manager	The solution should have ability to configure cookie category opt-out verbiage to encourage options	
36	Cookie Manager	The solution should have ability to auto-blocking of tags / tracking technologies	
37	Cookie Manager	The solution should have ability to digesting a UUID of choice to store consent	
38	Cookie Manager	The solution should have ability to remember the cookie choices stored in the browser once the user returns	
39	Cookie Manager	The solution should have ability to provide a description of use for each of the third-party cookies and other website data collection technologies identified in the scan	
40	Cookie Manager	The solution should have ability to support the ability to configure monthly scanning frequency for websites	
41	Cookie Manager	The solution should have the capability to automate and perform a full scan of all of Bank's website domains	
42	Cookie Manager	The solution should have ability to identify all cookies and other website data collection instances in use on each website that are not disclosed in the published Cookie Policy for that website	
43	Cookie Manager	The solution should have ability to have a reporting dashboard and allow you to export compliance reports	
44	Cookie Manager	The solution should have ability to allow filtering on the reporting dashboard	
45	Cookie Manager	The solution should have ability to block unwanted cookies	

S No	Module	Description	Compliance (Yes/No)
46	Cookie Manager	The solution should have ability to have the capability to auto-detect the website visitor's preferred language	
47	Cookie Manager	The solution should have ability to have dynamic IP detection to support different compliance types depending on where the website visitor is coming	
48	Cookie Manager	The solution should have ability to support Consent API's for cookie consents	
49	Cookie Manager	Auto-categorization of cookies into essential, functional, analytics, marketing and performance.	
50	Cookie Manager	Auto-blocking of cookies, including 3rd party scripts and tags, based on consent provided by the user.	
51	Cookie Manager	Customizable banner template.	
52	Cookie Manager	Auto-translation of cookie banner content into 22 languages as mandated by the DPDP Act.	
53	Cookie Manager	The solution should have ability to have dynamic language detection to support banner and preference centre localization	
54	Cookie Manager	The solution should have ability to perform 1st party and 3rd party cookie management	
55	Cookie Manager	The solution should have ability to identify all cookies and other website data collection technologies that are being used on our websites	
56	Data Discovery	Solution should support built-in detectors for personal and sensitive data elements	
57	Data Discovery	Solution should support sensitive data discovery supported On-prem /IaaS / SaaS Datastores	
58	Data Discovery	The solution should have ability to use other proximate data to increase confidence of correct matching	
59	Data Discovery	The solution should have ability to train/configure the tool to identify PII data specific to Bank environment	
60	Data Discovery	The solution should have ability to configure a PII entity definition using a regex model	
61	Data Discovery	Does the solution use machine learning to identify trainable PII	
62	Data Discovery	The solution should have ability to scan / OCR images and identify out-of-the-box PII information as specified above	
63	Data Discovery	The solution should have ability to provision of a confidence level for matched PII data	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
64	Data Discovery	Ability to initiate scanning manually or scheduled scans from within a UI	
65	Data Discovery	Ability to amend new findings from subsequent scans to primary scan output automatically.	
66	Data Discovery	Ability to pause the scans as per Bank requirement	
67	Data Discovery	Ability to drill down into a particular data store to initiate scanning of a particular subset of the data store	
68	Data Discovery	Ability to include/exclude particular file types from scanning	
69	Data Discovery	Ability to specify what PII should be included in any particular scan	
70	Data Discovery	Ability to initiate re-scans based upon modified date timestamps	
71	Data Discovery	Ability to identify ROT data (redundant, obsolete, trivial data in digital information that has little or no business value to the organization but is still stored.	
72	Data Discovery	Solution should allow Bank to identify and quarantine files from unstructured data systems based on file metadata (dates, file type, etc.) or classification data to reduce exposure to risky files being accessible to unintended users.	
73	Data Discovery	Solution should be capable to identify risk involved in Bank data system and data elements discovered after discovery scans.	
74	Data Discovery	The Solution must have native support for one or more of the following single sign-on (SSO) protocols SAML or OpenID Connect.	
75	Data Discovery	The solution should have ability to allow defining custom Data Element detections.	
76	Data Discovery	The solution should have proximity be configured for higher detection efficacy	
77	Data Discovery	List the languages supported for sensitive data discovery.	
78	Data Discovery	The solution should ensure support for data elements from multiple countries. List supported countries for following data elements: Addresses, Names, Govt IDs.	
79	Data Discovery	The solution should provide built-in Dictionaries	
80	Data	Is sensitive data discovery supported for Structured data	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Discovery	stores	
81	Data Discovery	The solution should have ability to automatically classify the contents of each column of a database and tag the table with required labels on structured databases	
82	Data Discovery	The solution should have ability to identify when a column of data has multiple data element types in it (e.g., a name and an address)	
83	Data Discovery	The solution should have ability to perform sensitive data discovery supported in unstructured text (blob/clob) of database tables	
84	Data Discovery	The solution should allow to specify which databases, schemas, and tables to scan and classify	
85	Data Discovery	The solution should allow classification metadata gathered from content discovery scans to be pushed to an external data catalog. List supported data catalogs.	
86	Data Discovery	The solution should have ability to scan multiple file formats i.e pdf, word, excel, csv, json, image files, compressed files, avro, parque etc.	
87	Data Discovery	The solution should have ability for detection of sensitive data elements in images. List formats supported.	
88	Data Discovery	The solution should have ability for detection of sensitive data elements in archive/compressed files? List formats supported.	
89	Data Discovery	The solution should have ability to scan nested records in big data formats (e.g., JSON)? And provide location information of detections?	
90	Data Discovery	The solution should have ability to support multiple languages for document classification. List supported languages.	
91	Data Discovery	The solution should have ability to centralized reporting with support for filters to find documents with sensitive data by location, datastore, owner, etc	
92	Data Discovery	The solution should have ability to list metadata available for each document. Folder path, create/modify times, owner, others	
93	Data Discovery	The solution should allow to define scans targeting specific datastores and specific data elements	
94	Data Discovery	The solution should allow on-demand scans of datastores	
95	Data	The solution should allow periodic scheduled scans	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Discovery		
96	Data Discovery	The solution should allow single file analysis to be performed without any requirement of data store	
97	Data Discovery	The solution should allow to view detections from past scan jobs	
98	Data Discovery	The solution should provide unique and total data element counts in unstructured data	
99	Data Discovery	The solution should allow Bank to easily export SDI data in PDF or CSV format	
100	Data Discovery	The solution should provide a centralized dashboard to view data insights and risk across data stores.	
101	Data Discovery	The solution should provide contextual drill down capabilities based on context	
102	Data Discovery	The solution should support integration with Microsoft Information Protection (MIP) for applying additional file metadata as custom tags to documents	
103	Data Discovery	The solution should be able to override current labels on documents with new classification labels	
104	Data Discovery	The solution should provide statistics on how many documents were labelled, when, for audit purposes	
105	Data Discovery	The solution should support risk scoring of data	
106	Data Discovery	The solution should allow the admin to adjust the importance of different risk factors	
107	Data Discovery	The solution should determine top risk hotspots by datastores, by locations, by owners etc	
108	Data Discovery	The solution should have ability to identify obsolete files and documents based on defined criteria. For e.g. find all the HR documents which are older than 3 years OR find all the documents older than 5 years having PII & Sensitive data).	
109	Data Discovery	The solution should have ability to identify files from based on file metadata (dates, file type, etc.) or classification data (e.g. data elements, content profiles, etc.) to quarantine for further review or action	
110	Data Discovery	The solution should have ability to display all contextual info related to files in a single pane of glass.	
111	Data Discovery	The system should scan all kinds of databases to detect and classify Indian personal data fields including names,	

S No	Module	Description	Compliance (Yes/No)
		Aadhaar Card, PAN Card, Passport, Voter ID Card, Driving License, NREGA Job Card, Proof of Address (If not included in OVD): Utility Bills (Electricity, Water, Telephone) - typically < 2-3 months old, Bank Account Statement/Passbook, Rent Agreement/Sale Deed, Residence Visa copies (duly attested), E-Aadhaar or via authorized digital, as per AMFI, PAN card of the entity, proof of address, and documents of the Karta/Authorized Signatory	
112	Data Discovery	Ability to identify key government identifiers: PII/SPI, Aadhaar number, PAN card, driving license, Banking information, Credit card, India Rupay Card number, Indian Virtual payment address, Credit score, Bank routing number, SWIFT/BIC number, Bank a/c number (savings, loan, demat, etc)	
113	Data Discovery	Ability to identify duplicate/near duplicate files/documents	
114	Data Discovery	Solution should be able to identify similar files (data duplication) or documents having exactly similar or nearly similar content.	
115	Data Discovery	Solution should be hosted within Indian geography considering data localization requirements from various regulatory bodies i.e. RBI, CERT-IN, DPDPA, NCIIPC etc	
116	Data Discovery	The system should be capable of scanning unstructured data such as PDFs, Photos, PPTs to identify and categorise PII.	
117	Data Discovery	The system should accurately identify historical versions of Indian-specific identifiers such as Aadhaar, PAN, Voter ID, Driving License belonging to all Indian states	
118	Data Discovery	The system should create a persistent and searchable inventory of discovered personal data across systems.	
119	Data Discovery	The system should support discovery across on-premises, cloud, and hybrid environments.	
120	Data Discovery	The system should enable linking discovered fields to Business processes (products) where relevant.	
121	Data Discovery	The system should alert when new sensitive PII is added to a previously scanned source.	
122	Data Discovery	The system should show data flow and transformation paths across systems for compliance traceability.	
123	Data Mapping	The solution should have ability to support data mapping initiatives, including mapping and analyzing assets and	

S No	Module	Description	Compliance (Yes/No)
		processing activities	
124	Data Mapping	The solution should have ability to support different data elements that apply to specific data principals, such as internal employees, external customers, vendors, etc	
125	Data Mapping	The solution should have ability to import pre-defined assets, processing activities, and data elements through a standard interface or bulk import	
126	Data Mapping	The solution should have ability to pre-defined questionnaires to analyze current and new data mapping initiatives	
127	Data Mapping	The solution should have ability to automatically update our data inventory when an assessment has been completed on an asset or processing activity	
128	Data Mapping	The solution should have ability to possess the ability to map all types of applications (On-Prem, Cloud, SaaS, etc.)	
129	Data Mapping	The solution should have ability to automated data mapping visualizations such as heat maps, data flows and data lineage from Process records.	
130	Data Mapping	The solution should have ability to automate RoPA/GDPR Article 30 reporting capability/DPDPA guideline	
131	Data Mapping	The solution should have ability for a scheduled re-assessment of data mapping activities	
132	Data Mapping	The solution should have ability to define different data elements to associate with each processing activity	
133	Data Mapping	The solution should have ability to store information concerning all of the above, such as classifying attributes for each asset and processing activity	
134	Data Mapping	The solution should have ability for central dashboard with sorting and filtering capabilities	
135	Data Principal Rights Management	The solution should have ability to receive, process, and record a Data principal Access Requests (DSAR) as required by global privacy regulations (e.g. DPDPA, GDPR etc.)	
136	Data Principal Rights Management	The solution should have ability to support front-end secure web portal accessible from a BANK website(s) that allows a user (i.e. data principal) to initiate a request using a form.	
137	Data Principal Rights	The solution should have ability to embed intake form within the Bank website	

S No	Module	Description	Compliance (Yes/No)
	Management		
138	Data Principal Rights Management	The solution should have ability to customize web form support the capability for data principals to upload attachments to support and assist in verifying their identity	
139	Data Principal Rights Management	The solution should have ability for BANK employee to submit a request on behalf of a data principal when the request is received over the phone or via a form submitted in-person/mail.	
140	Data Principal Rights Management	The solution should have ability to facilitate a two-step process where the data principal must first submit the request and then separately confirm that they want their personal information deleted.	
141	Data Principal Rights Management	The solution should have ability for secure portal where data principal can login and see the status of their submitted request(s)	
142	Data Principal Rights Management	The solution should have ability to conduct two-way communication with the data principal within the secure portal (ask questions, confirm receipt of the request, notice of a delay in responding etc.).	
143	Data Principal Rights Management	The solution should have ability to have a central dashboard to show all received DSARs in an easy to manage queue	
144	Data Principal Rights Management	The solution should have ability to allow for designated reviewers and/or approvers based on certain conditions.	
145	Data Principal Rights Management	The solution should have ability to allow for administrative (i.e. global) access to view, edit all requests, workflow settings, etc.	
146	Data Principal Rights Management	The solution should have ability to allow for automatic assigning capabilities and re-assigning as needed for each DSAR ticket	
147	Data Principal Rights Management	The solution should have ability to have customizable workflows to process all received DSARs	
148	Data	The solution should have ability to assign sub-tasks within	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Principal Rights Management	a request	
149	Data Principal Rights Management	The solution should have ability to help BANK organization monitor the time remaining for each DSAR	
150	Data Principal Rights Management	The solution should have ability to provide alerts & reminders to designated internal parties when approaching the regulatory due date.	
151	Data Principal Rights Management	The solution should have ability of choosing to extend the data principal's request	
152	Data Principal Rights Management	The solution should have ability to support secure, direct communications with the data principal concerning their request	
153	Data Principal Rights Management	The solution should have ability to automatically highlight, and extract PD detected within objects & files belonging to the data principal	
154	Data Principal Rights Management	The solution should have ability to have reporting capabilities on DSR request types, owners, date, etc..	
155	Data Principal Rights Management	The solution should have ability to provide dashboard and on-demand reporting with key performance indicators (e.g. avg time to respond, etc.).	
156	Data Principal Rights Management	The solution should have ability to offer selective deletion and global deletion options for the user to select when making a request.	
157	Data Principal Rights Management	The solution should have ability to support masking/deleting of sensitive information before sharing the report with data principal	
158	Data Principal Rights	The solution should have ability to have pre-defined templates to use for communicating with a data principal concerning their request type	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Management		
159	Data Principal Rights Management	The solution should have ability to offer these templates in different languages	
160	Data Principal Rights Management	The solution should have ability to have the ability to fully automate selective DSR workflows without user intervention	
161	Data Principal Rights Management	The solution should have ability to offer an appeal option to data principals if the submitted report is not up to satisfaction by the data principal	
162	Data Principal Rights Management	The system should manage Data Principal Requests for access, correction, deletion, nomination, and grievance redressal in compliance with DPDP.	
163	Data Principal Rights Management	The system should coordinate with internal and third-party processors to fulfill requests across distributed systems.	
164	Data Principal Rights Management	The system should provide real-time dashboards to monitor SLA timelines and status of each data principal request.	
165	Data Principal Rights Management	The system should track processor-level acknowledgment and actions for deletion/correction as per requests.	
166	Data Principal Rights Management	The system should auto-send acknowledgments to data principals upon receipt of their request.	
167	Data Principal Rights Management	The system should support generation of pre-approved, customizable responses for DPAR fulfillment.	
168	Data Principal Rights Management	The system should maintain tamper-proof logs of actions taken, responses shared, and processors contacted.	
169	Data	The system should log and display reasons if any request is	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Principal Rights Management	rejected or partially fulfilled, as mandated under DPDP.	
170	Data Principal Rights Management	The system should allow tracing back consent context when a deletion request is received for accurate fulfillment.	
171	Data Principal Rights Management	The system should support escalations to internal grievance officers and auto-escalation to DPB when SLA is breached.	
172	Data Principal Rights Management	The system should generate export-ready formats for reports and notifications to the Data Protection Board (DPB).	
173	Data Principal Rights Management	The solution should have ability to support multiple languages for the customizable web forms	
174	Data Protection Impact Assessment	The system should offer a guided questionnaire-based DPIA flow that assesses risk based on data type, processing, and harm likelihood.	
175	Data Protection Impact Assessment	The system must provide tagging of business process while configuring DPIA	
176	Data Protection Impact Assessment	The system should automatically recommend DPIA for high-risk purposes involving sensitive personal data or profiling.	
177	Data Protection Impact Assessment	The system should calculate residual risk after mitigation steps have been defined within the DPIA.	
178	Data Protection Impact Assessment	The system should support role-based reviews, comments, and approvals of DPIAs within organizations.	
179	Data Protection Impact	The system should allow tracing back of DPIAs linked to a consented activity to validate risk assessments.	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Assessment		
180	Data Protection Impact Assessment	The system should allow linking PIIs, processors and purposes while creating an assessment	
181	Data Protection Impact Assessment	The system should allow upload of supporting documentation such as architecture diagrams, policies, and contracts.	
182	Data Protection Impact Assessment	The system should provide metrics such as time to complete, top risk domains, and mitigation effectiveness.	
183	Data Protection Impact Assessment	The system should be capable of exporting DPIA reports for submission to the DPB or auditors if requested.	
184	Data Protection Impact Assessment	The system should allow for periodic re-assessment of DPIAs based on changes in processing or legislation.	
185	Privacy notice & policy management	The solution should have ability to allow Bank to manage the process of creating, managing, and publishing policies and notices across websites and applications	
186	Privacy notice & policy management	The solution should have ability to maintain version history and notify users when changes are made to policies	
187	Privacy notice & policy management	The solution should have ability to have pre-defined template library of policies and notices	
188	Privacy notice & policy management	The solution should have ability to allow Bank to import and maintain existing policies directly within the solution	
189	Third Party Risk Management	The solution should have ability to allow for the assessment of third-party solutions (vendors and service providers)	
190	Third Party Risk	The solution should have ability to maintain a database of vendors to simplify the risk management process	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Management		
191	Third Party Risk Management	The solution should have ability to allow vendors to access the application using a self-service portal	
192	Third Party Risk Management	The solution should have ability to have pre-defined vendor assessment questionnaire templates that can be customized	
193	Third Party Risk Management	The solution should have ability to allow BANK to import existing vendor assessment questionnaire templates	
194	Third Party Risk Management	The solution should have ability to offer a vendor risk rating system that provides baseline privacy and security risk ratings for common vendors	
195	Third Party Risk Management	Create an audit trail with your data processors to ensure compliance as per consent updation/revocation by data principal.	
196	Third Party Risk Management	Ability to Raise Deletion requests to Processors	
197	Third Party Risk Management	Route deletion requests from Data Principal Rights Management to processor (Manual and auto)	
198	Third Party Risk Management	Ability for Data Processors to acknowledge, upload proofs and comply with deletion requests	
199	Third Party Risk Management	Create, assign Third party risk assessments to vendors and manage the lifecycle.	
200	Third Party Risk Management	The system should allow mapping of each processor to purposes they serve and PII types they handle.	
201	Third Party Risk Management	The system should visually represent processor PII Purpose Deletion flow in an interactive mindmap.	
202	Third Party Risk Management	The system should track deletion acknowledgments and timelines as committed by processors in contracts.	
203	Third Party Risk Management	The system should flag non-compliance with contractual clauses related to data breach, retention, deletion, etc.	

S No	Module	Description	Compliance (Yes/No)
204	Third Party Risk Management	The system should support management of multiple contracts and addendums per processor with version control.	
205	Third Party Risk Management	The system should offer dashboards showing active obligations, upcoming renewals, and expiring contracts.	
206	Third Party Risk Management	The system should trigger alerts if processor fails to meet SLA for data deletion, access, or breach reporting.	
207	Third Party Risk Management	The system should extract key metadata such as retention periods, breach clauses, and jurisdictions from contracts.	
208	Third Party Risk Management	The system should maintain and display authorized contact details for each processor for escalation workflows.	
209	Third Party Risk Management	The system should show how a processor's data activities relate to consents received and their expiry timelines.	
210	Third Party Risk Management	The system should integrate with DSAR, DPIA, and Breach modules to fetch processor-linked activity and risks.	
211	Third Party Risk Management	The system should monitor contract renewal dates and notify internal stakeholders for review or renegotiation.	
212	Assessments	The solution should have pre-built questionnaire templates that specifically map against legal requirements in privacy regulations, such as the EU GDPR, DPDPA etc	
213	Assessments	The solution should have ability to import existing pre-built questionnaires	
214	Assessments	The solution should have ability for built-in workflows to manage the beginning-to-end process of sending and approving the questionnaire	
215	Assessments	The solution should have ability to support unlimited assessments to be executed based on BANK requirements	
216	Assessments	The solution should have ability to version management capabilities and built-in audit trails for templates and completed assessments	
217	Assessments	The solution should have ability to support multiple response types	
218	Assessments	The solution should have ability to track the status of an	

S No	Module	Description	Compliance (Yes/No)
		assessment and assignment of items	
219	Assessments	The solution should have ability to create custom questionnaires directly in the UI of the application	
220	Assessments	Solution have the ability to pre-populate a new assessment based on the previous assessment	
221	Assessments	The solution should have ability to support assessments with conditional logic (context-aware questionnaires dependent on respondent's answers to apply risk ratings, severity, skip logic capabilities, workflows)	
222	Assessments	The solution should have ability to allow multiple respondents to collaborate on a single questionnaire	
223	Assessments	The solution should have ability to trigger additional assessments as needed	
224	Assessments	The solution should have ability to for built-in risk management lifecycle	
225	Assessments	The solution should have ability to support customizable risk scoring	
226	Assessments	The solution should have ability to visually view risks in a heat map and allow flexible risk configuration, such as risk severity and risk likelihood labels	
227	Assessments	The solution should have ability to add comments on a per-question basis while reviewing the completed questionnaire	
228	Assessments	The solution should have ability to upload attachments in a questionnaire	
229	Assessments	The solution should have ability for performing assessment on a scheduled basis	
230	Assessments	The solution should have ability to have a central dashboard with sorting/filtering capabilities	
231	Assessments	The solution should have ability to export assessment templates	
232	Assessments	The solution should have ability to easily export assessment data in PDF or CSV format	
233	Assessments	The solution should have ability to have a rich set of open API's for assessments	
234	Automated Compliance Tool kit	The system must in the digital journey, automatically identify and classify personal data fields, including Indian-specific identifiers such as Aadhaar, PAN, Voter ID, and Passport etc, into sensitive and non-sensitive categories.	
235	Automated	The system should flag and restrict use of pre-checked	

Signature of the Bidder with company Seal

S No	Module	Description	Compliance (Yes/No)
	Compliance Tool kit	consent boxes in any consent collection UI, as per DPDP compliance.	
236	Automated Compliance Tool kit	The system must automatically generate Records of Processing Activities (RoPA) by mapping personal data fields to their corresponding processing purposes.	
237	Automated Compliance Tool kit	The system must generate DPDPA-compliant consent notices, mapping each personal data field to the appropriate processing purpose and legal basis.	
238	Automated Compliance Tool kit	The system must assign a DPDPA compliance score to each assessed digital journey and highlight the reasons contributing to the score.	
239	Automated Compliance Tool kit	The system must support purpose dictionary creation by mapping the business process with obligations from RBI, SEBI, and IRDAI.	
240	Automated Compliance Tool kit	The system must support generation of detailed DPDPA compliance reports with downloadable formats for internal and regulatory audits.	
241	Breach	The solution should have ability to report incidents and potential data breaches via UI, self-service portal or API	
242	Breach	The solution should have ability to have detailed, built-in audit trails to support Bank to report on actions taken inside your proposed solution	
243	Breach	The solution should have ability to support automatic email notifications and workflows throughout the lifecycle of the incident	
244	Breach	The solution should have ability to customizable, automated workflows with assignable sub-tasks for each documented incident	
245	Breach	The solution should have ability to have native API integration capabilities with other applications, such as ServiceNow, JIRA	
246	Breach	The solution should have the ability to allow both internal and external facing audiences to report a suspected incident through an easy-to-use self-service portal	
247	Breach	The solution should support API based integration with other third-party solutions for incident management	
248	Breach	The system should support intake of breach incidents via UI and API for centralized tracking.	
249	Breach	The workflow of breach should align the requirement as per Rules of the DPDP Act.	

S No	Module	Description	Compliance (Yes/No)
250	Breach	The system should categorize incidents based on type (PII breach, processor breach, unauthorized access, etc.).	
251	Breach	The system should allow mapping of affected PII fields, processing purposes, and processors involved in the breach.	
252	Breach	The system should maintain a time-stamped event log for each incident from detection to resolution.	
253	Breach	The system should support assigning breach resolution tasks to internal compliance, legal, and IT teams.	
254	Breach	The system should have workflows to reach out to processors responsible for the breach and collect remediation responses.	
255	Breach	The system should generate regulator-ready breach notices aligned with DPDP draft rules for the Data Protection Board.	
256	Breach	The system should generate template-based notifications for affected data principals in case of material harm.	
257	Breach	The system should support identification of closed cohort of data principals possible to send the notifications to the affected Data Principals only.	
258	Breach	The system should auto-calculate breach severity based on volume, type of PII, sensitivity, and potential harm.	
259	Breach	The system should link breaches back to relevant DPIAs and consents impacted for impact traceability.	
260	Breach	The system should provide visual representation of Breach PII Processor Consent impact in a mind map format.	
261	Breach	The system should track breach response and notification timelines to ensure regulatory compliance within 72 hours.	
262	Breach	The system should maintain an audit trail for every action taken in breach management.	

Authorized Signatory
Office Seal

Name and Designation

Place:

Date:

Signature of the Bidder with company Seal

Annexure 36 Format for Credential Letter (For Bidder)

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Dear Sir ,

*(In case the below mentioned line items are supplied in different organisations separately
in different Purchase Orders, more than one Credential Letter have to be submitted)*

It is certified that the *(Choose appropriate Line Item/s)* _____ have Supplied &
implemented the following Components *(Line Items)*-

1. Gap Assessment, Solution Architecture and Implementation Planning.
2. Infrastructure and Hardware Supply & Configuration
3. Implementation of Data Privacy and Consent Management Solution
 1. Consent Management
 2. Cookie Consent Management
 3. Record of Processing Activities (RoPA)
 4. Data Discovery, Inventory, Classification and Data flow Mapping
 5. Data Privacy Assessments
 6. Data Principal Rights Management
 7. Data Protection Impact Assessments (DPIA)
 8. Privacy Notice Management
 9. Data and Privacy Breach Management
 10. Compliance Monitoring, Reporting and Governance Dashboard
 11. Third Party Risk Management

in our Scheduled Commercial Bank / BFSI /NBFC / PSU *(Select One)* in India on Date
_____.

This letter should not be treated as recommendation and M/s *(Company Name)*
_____ does not own any responsibility on the decisions taken based on this
Credential letter.

Yours faithfully,

Signature with Company Stamp

Designation:

Company Name:

Contact Number:

Signature of the Bidder with company Seal

Annexure 37 Format for Credential Letter (For OEM)

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.1**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Dear Sir ,

*(In case the below mentioned line items are supplied in different organisations separately
in different Purchase Orders, more than one Credential Letter have to be submitted)*

It is certified that the (OEM Company Name) _____ device had been
supplied & implemented (Choose appropriate Line Item/s)-

1. Gap Assessment, Solution Architecture and Implementation Planning

2. Infrastructure and Hardware Supply & Configuration

3. Implementation of Data Privacy and Consent Management Solution

1. Consent Management
2. Cookie Consent Management
3. Record of Processing Activities (RoPA)
4. Data Discovery, Inventory, Classification and Data flow Mapping
5. Data Privacy Assessments
6. Data Principal Rights Management
7. Data Protection Impact Assessments (DPIA)
8. Privacy Notice Management
9. Data and Privacy Breach Management
10. Compliance Monitoring, Reporting and Governance Dashboard
11. Third Party Risk Management

in our Scheduled Commercial Bank / BFSI /NBFC / PSU (Select One) in India on Date
_____.

This letter should not be treated as recommendation and M/s (Company Name)
_____ does not own any responsibility on the decisions taken based on this
Credential letter.

Yours faithfully,

Signature with Company Stamp

Designation:

Company Name:

Contact Number

Signature of the Bidder with company Seal

Annexure 38 Undertaking for Infrastructure Sizing and Capacity Planning

(On Bidder's Letterhead)

Date: _____

To,

Data Protection Officer

Data Protection Cell,

RMD , Central Bank Of India

**1st Floor, Bajaj Bhavan, Barrister Rajni Patel Marg, Nariman Point,
Mumbai 400 021.**

Sub: Tender No. GEM/2026/B/ 7977310 dated 31/08/2026

Dear Sir ,

We hereby undertake that the proposed solution infrastructure, including servers, storage, database, middleware, operating systems, and all related components, has been appropriately sized based on the volumetric requirements specified in Annexure 33 of the RFP.

We further confirm that the proposed sizing is adequate to support the required transaction volumes, data growth, concurrent users, integrations, reporting requirements, and all solution functionalities throughout the contract period. The infrastructure has been designed to ensure that utilization of critical resources, including CPU, memory, storage, and network capacity, does not exceed 70% at any point of time.

We also confirm that the Production environments at DC and DR shall be deployed in a High Availability configuration with no single point of failure. Any additional hardware, software, licenses, or infrastructure components required to meet the performance, availability, scalability, and service level requirements of the RFP shall be provided by us at no additional cost to the Bank.

We acknowledge that any shortfall in infrastructure sizing identified during implementation or the contract period shall be rectified by us through provisioning of additional capacity, licenses, or components at our own cost, without impacting project timelines, performance, or contractual obligations.

Yours faithfully,

Signature with Company Stamp

Designation:

Company Name:

Contact Number

*****End of Document*****

Signature of the Bidder with company Seal