CORPORATE OFFICE, THRISSUR

DEPARTMENT: INFORMATION TECHNOLOGY

Tender No: Tender/09/2026-27 Dated: 28.07.2026

Tender for Procurement, Implementation and Maintenance of Enterprise Data Privacy Governance & Compliance Platform (DPDP Act 2023 Aligned)

1. Introduction

Dhanlaxmi Bank Ltd invites proposals from eligible and qualified vendors for the supply, implementation and maintenance of Enterprise Data Privacy Governance & Compliance Platform aligned with DPDP Act 2023.

The **Digital Personal Data Protection (DPDP) Act, 2023** provides a comprehensive legal framework for the collection, processing, storage, protection and management of personal data in India. As a regulated entity under the supervision of the **Reserve Bank of India (RBI)**, **Dhanlaxmi Bank Ltd.** processes personal and sensitive personal data pertaining to customers, employees, vendors and other stakeholders through its extensive IT landscape, which includes core banking platforms and other interconnected applications

With the enactment of the **Digital Personal Data Protection (DPDP) Act, 2023** and the subsequent notification of the **DPDP Rules, 2025**, the Bank is required to adhere to an enhanced and more rigorous framework of personal data protection and privacy obligations. Considering the volume, diversity, sensitivity and complexity of personal data processed across the Bank's operations, it has become necessary to establish a centralized Data Privacy Management Platform to facilitate compliance with applicable regulatory requirements and strengthen the Bank's data protection governance framework.

2. Objectives of the Tender

The objective of this tender notice is to procure, implement and maintain an enterprise-grade, on-premises Data Privacy Governance & Compliance Platform that enables the Bank to comply with the DPDP Act, 2023 and related regulatory requirements in a consistent, auditable and scalable manner.

The proposed solution shall provide: end-to-end visibility of personal and sensitive personal data across the Bank's IT landscape; structured, lawful, and timely handling of Data Principal rights; enforcement of data retention, restriction and erasure (where legally permissible); and generation of regulator-ready evidence to support regulatory inspections, internal and external audits, and proceedings before the Data Protection Board of India.

3. Scope of Work

Bank desires to select a Vendor (OSD / Authorized Partner of OSD) for providing a comprehensive 'Enterprise Data Privacy Governance & Compliance Platform' in compliance with the DPDP Act, 2023, DPDP Rules 2025, and other applicable regulatory frameworks.

The Scope of Work is detailed in clauses 13 and 15 of this document. The Bank reserves the right to modify/change the scope of work at any phase of this procurement process. Any service forming part of the Project Scope not explicitly excluded shall form part of this tender notice and the Bidder is expected to provide the same at no additional cost to the Bank.

3.1 . Technical Requirements

The Vendor must size the solution based on the Bank's data volumes and projected growth, as part of the technical bid submission. The complete supply, implementation, maintenance, and support of the Enterprise Data Privacy Governance & Compliance Platform shall form part of the Bidder's scope.
The Bidder must design the solution with high availability and secure infrastructure in the Data Centre (DC) and Disaster Recovery (DR) site.

As part of the technical proposal, the Bidder must provide:

- List of compatible Operating Systems and Databases, along with licensing details
- Details of redundancy and security setup
- Application architecture diagram including infrastructure setup at DC and DR
- Implementation procedure / roadmap
- Server and infrastructure specifications for UAT and production environments

Enterprise License: The license for the solution shall be enterprise-wide and perpetual, covering all modules without any constraint on the number of branches or users for the Bank's domestic operations.

The proposed system must be capable of and compatible with Disaster Recovery implementation. The Bidder must describe the provisions for disaster recovery and demonstrate that the proposed solution facilitates seamless failover. The Bidder must submit the technical architecture relating to data replication between primary and secondary sites.

3.2 Implementation & Delivery

The Enterprise Data Privacy Governance & Compliance Platform must be implemented as per the project scope within 24 weeks from the date of placing the Purchase Order. The implementation shall be executed in two phases as follows:

S.No.	Implementation Phase	Duration
1	**PHASE 1 – Consent & Privacy Governance Platform** A. Cookie Management B. Notice Management C. Consent Lifecycle Management – Digital Self Journey (NTB) & Digital Assisted Journey (NTB) D. Data Principal Right Management / Grievance Redressal	Week 1 to Week 12 (12 Weeks)
2	**PHASE 2 – Consent & Privacy Governance Platform (Continued)** A. Consent Lifecycle Management – Physical Journey (NTB) & Legacy Customers (ETB) B. Data Protection Impact Assessment (DPIA) C. Data Processor Privacy Risk Assessment	Week 13 to Week 24 (12 Weeks)

	D. Governance and Compliance Dashboard E. Integration with NeGD Platform	

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned above.

Penalty for Delay: In case individual phase-wise deadlines are not met, the Vendor shall pay penalty to Dhanlaxmi Bank Ltd at the rate of 0.5% of the particular phase implementation cost (inclusive of all taxes, duties, and levies) per week or part thereof, for late implementation beyond the due date, up to a maximum of 10%. If delay exceeds two weeks from the due date, Dhanlaxmi Bank Ltd reserves the right to cancel the entire order.

3.3 Training Requirements

1. As part of implementation, the bidder shall provide:
    a. Onsite Training at Bank Premises.
    b. Comprehensive training to all relevant stakeholders.
2. Functional & Technical Training to Key Stake holders (e.g. DPO Team, Technology & Security Team, Digital Team) - Duration - One Week
3. Functional - Train the Trainer -Duration - One Week (For User Group) Role-based user manuals and handbooks
4. Standard Operating Procedures (SOPs)
5. Training presentations (PPTs)
6. Documentation - User manual (Functional, Operational, Technical, FAQ, SOP, & Technical and Training material Softcopy).
7. Training shall cover consent management, DPIA, and data discovery modules

3.4 Support & Maintenance Requirements

1. Warranty period of minimum 12 months from go-live date
2. Annual Maintenance Contract (AMC) covering software updates, bug fixes and regulatory changes
3. 24x7 helpdesk support with ticketing system

3.5 Service Levels and Uptime Guarantee

The solution must achieve the following minimum service levels:

Parameter	Target SLA	Penalty for Breach
System Availability (Production)	99.5% per month	Proportionate deduction from ATS
Critical Incident Resolution (P1)	4 hours	Penalty as per SLA schedule
High Severity Incident Resolution (P2)	8 business hours	Penalty as per SLA schedule
Scheduled DR Drill Success	Twice annually	As per SLA schedule
Data Principal Rights Fulfilment TAT	As per DPDP Rules	Proportionate deduction

4. Eligibility Criteria

Bidder must satisfy the following eligibility criteria to qualify for participation in this tender

- Bidder must be a company registered in India under the Companies Act, 1956/2013.
- Bidder must be the OSD or an authorized partner/reseller of the OSD for the proposed solution.
- The Bidder must have successfully implemented a Consent & Privacy Governance Platform, comprising at a minimum the following four mandatory functionalities - (i) Consent Management, (ii) Records of Processing Activities (ROPA), (iii) Third-Party Risk Management, and (iv) Data Protection Impact Assessment (DPIA) - in at least two (2) BFSI entities in India during the preceding three (3) years.
- The bidder/vendor shall possess a valid ISO/IEC 27001 certification or an equivalent.
- Bidder must not be blacklisted/debarred by any Public Sector Bank, RBI, or any Government body in India.

- The Bidder must successfully clear the Bank's Vendor Risk Assessment and Due Diligence process, conducted in line with applicable regulatory guidelines;
- Submission of the bid shall constitute the Bidder's unconditional acceptance and consent to the Bank's Vendor Due Diligence and Risk Assessment process as a precondition of eligibility.

5. Submission Requirements

5.1 Technical Proposal

The Technical Bid response must include all information required to assess the technical proposal, covering:

- High-level service delivery roadmap and delivery schedule
- Program/Project Management methodology, processes, service management and governance structure
- Signed copies of the Vendor On-Boarding Evaluation Sheet, Detailed Due Diligence Report, and Risk Assessment Sheet, duly executed on the Bidder's official letterhead, signed by an authorised signatory.
- Integration methodology – Internal and External Third-party standards
- Technology considerations for SLAs, operational resilience, availability, business continuity, and observability
- Sample SLA reports/templates, deliverable reports, executive dashboards, and application performance monitoring
- Technology considerations for security, audit, and compliance requirements
- Details of ITSM and COBIT capabilities
- Resource deployment strategy including resource continuity, key roles, and governance structure
- Detailed steps on how to measure, track, monitor, and achieve service level KPIs and SLA parameters.

5.2 Commercial Proposal

Payment Terms

Payment shall be milestone-linked and subject to successful delivery, implementation, and operationalization of the solution in accordance with the Scope of Work, SLA, and acceptance criteria defined by the Bank.

A. License Cost (Milestone Linked)

Milestone	% of License Cost	Conditions
Milestone 1	30%	Delivery of license keys, installation in Bank's DC/DR environment
Milestone 2	30%	Completion of configuration, successful SIT with CBS integration
Milestone 3	20%	Successful Go-Live of Phase 1, sign-off by IT, Business, IS and Compliance teams
Milestone 4	20%	Successful Go-Live of Phase 2, final validation of all modules in production

B. Implementation & Integration Cost (OTC)

Milestone	% of Impl. Cost	Conditions
Phase 1 Go-Live	30%	Go-Live sign-off of Phase 1 scope
Phase 2 Go-Live	40%	Integration with legacy systems (ETB), DPIA, Vendor Risk, Governance Dashboard

Final Sign-off	20%	Final Go-Live closure, all integrations complete, documentation submitted
Retention (3-month post Go-Live)	10%	SLA compliance achieved; no Severity-1 issues pending

C. Annual Technical Support (ATS)

ATS shall be payable quarterly in arrears, subject to submission of quarterly service reports and SLA compliance certification. Any SLA breach shall result in proportionate deduction. ATS shall not be payable in advance under any circumstances.

Onsite Support & Training Charges

Payable quarterly in arrears, proportionate to actual attendance and subject to deductions for SLA breaches. Training charges shall be released upon completion of all scheduled sessions and submission of a training completion report duly signed by the Bank's Project Manager.

6. Additional Requirements

The price payable to the Bidder shall be inclusive of any modifications, changes or upgrades to the application and other software required to comply with any statutory or regulatory requirements during the subsistence of the contract. Version upgrades not necessitating a technology refresh or architectural change shall fall within this scope.

7. Audit Rights

All Bidder records pertaining to matters covered in this tender shall be made available to auditors and inspecting officials of Dhanlaxmi Bank Ltd, the Reserve Bank of India and any other regulatory authority, at any time during normal business hours, as often as the Bank deems necessary. The Bidder must provide the Bank access to monitoring and performance measurement systems and must remedy all discrepancies observed by auditors at no additional cost to the Bank.

8. Escrow Mechanism

The Bank and the successful Bidder shall appoint an escrow agent for the deposit of source code of the software product. The Bank and the Bidder shall enter into a tripartite escrow agreement. All costs for the Escrow arrangement shall be borne by the Bidder.

9. Evaluation Criteria

A two-bid system is adopted for selection of the Service Provider:

- Stage 1 – Eligibility Evaluation
- Stage 2 – Technical Evaluation followed by Commercial Evaluation

9.1 Stage 1 – Eligibility Evaluation

The Eligibility Criterion is specified in Section 4 of this document. Only Bidders meeting the eligibility criteria shall have their Technical Proposals evaluated.

9.2 Stage 2 – Technical and Commercial Evaluation

- **Technical Evaluation**

Proposals will be evaluated based on technical compliance, functional capabilities, vendor experience and implementation approach.

- **Commercial Evaluation**

Technically qualified vendors will be evaluated on commercial terms. The evaluation will consider:

- Total cost of ownership (TCO) over 5 years
- Value for money and cost-benefit analysis
- Payment terms and conditions
- AMC cost structure and escalation terms

10. Terms & Conditions

This tender notice is not a contract offer. Receipt of a proposal neither commits Dhanlaxmi Bank Ltd to award a contract to any vendor, nor limits the Bank's rights to negotiate with any vendors in the Bank's best interest.

- The Bank reserves the right to accept or reject any or all proposals, or any part thereof, without penalty and without assigning any reason.
- The Bank may conduct product demonstrations and proof-of-concept (POC) before the final selection.
- The Bank reserves the right to request additional information necessary to assure the vendor's ability and qualification to perform the contract.
- For any ambiguity, omissions, or unclear content in the tender, the vendors must raise pre-bid queries within the timeline mentioned.
- Vendors must maintain confidentiality of all information shared during the tender process.

11. Submission Process

Proposals must be submitted via secure email clearly marked as: **Tender for Procurement Enterprise Data Privacy Governance & Compliance Platform** [Tender Reference Number]

Activity	**Date**
Bank's Address for Communication	IT Department, 1st Floor, Corporate Office Dhanlaxmi Bank Ltd, Punkunnam, Thrissur, Kerala - 680002
E-mail for Submission of Tender and Clarifications.	hoits@dhanbank.co.in
Tender Release	28-07-2026
Last Date for Clarifications	31-07-2026
Last Date for Proposal Submission	06-08-2026

12. General Terms & Conditions

- The scope outlined in this document is indicative and subject to revision.
- Any delay or non-performance shall attract applicable penalties, as per contract terms.
- The successful Bidder must sign the Bank's SLA and NDA before commencement of work. No payment shall be released prior to the execution of these documents.
- The Bidder shall comply with all applicable laws, rules, regulations, and guidelines including the DPDP Act, 2023, DPDP Rules, 2025, RBI guidelines, and other applicable regulatory frameworks, throughout the contract period.
- The Bidder shall treat all information obtained from the Bank during this tender process and the subsequent contract as strictly confidential. The Bidder shall not disclose any such information to any third party without the prior written consent of the Bank. This obligation shall survive the termination of the contract
- The Bank reserves the right to terminate the contract for convenience by giving 30 days written notice. The Bank may also terminate the contract with immediate effect in the event of breach of contract terms, fraud, insolvency, or failure to meet critical SLAs.
- The Bidder shall indemnify and hold harmless Dhanlaxmi Bank Ltd, its directors, officers, employees, and agents from and against any claims, damages, losses, costs, and expenses arising out of or in connection with the Bidder's performance under the contract, including infringement of intellectual property rights.
- Except as specifically agreed, all intellectual property rights in and to the software shall remain with the Bidder or its licensors. The Bank shall be granted a non-exclusive, non-transferable, perpetual license to use the software for its business operations. The Bidder shall ensure that the software does not infringe any third-party intellectual property rights.
- The total liability of the Bidder under this contract shall not exceed the total fees paid or payable under the contract. Neither party shall be liable for indirect, incidental, consequential, or punitive damages.
- The Bidder must comply with all of the Bank's information security policies and procedures, RBI guidelines on IT security, and applicable industry standards (ISO 27001, OWASP, etc.). The Bank shall have the right to conduct periodic information security audits of the Bidder's systems and processes.

- The bidder shall submit the duly completed Vendor On-Boarding Evaluation Sheet, Detailed Due Diligence Report, and Risk Assessment Sheet, as provided in Annexure - 1, on its official letterhead, duly signed by an authorised signatory
- The proposals would be subjected to the technical and commercial qualification process as per Bank's policy.

Dhanlaxmi Bank Ltd reserves the right to reject any or all tenders without assigning any reason thereof. The decision of Bank will be final and binding.

For any clarifications or inquiries, please contact:

Contact Details	Binesh Kurup B Senior Manager IT Department Mob: 9539007448	Remya DPO -In Charge DPGD Mob:9539003634

13. Project Scope

The Scope of Work encompasses the supply, implementation, customization, integration, training, and maintenance of the Enterprise Data Privacy Governance & Compliance Platform (DPDP Act 2023 Aligned). The detailed scope of work is mentioned below:

The scope of work shall include the following:

- **Software Supply:** On-premises licensing of the Consent & Privacy Governance Platform.
- **Implementation Services:** Installation, configuration, customization, and integration with the Bank's existing systems.
- **Support & Maintenance:** Comprehensive support and maintenance services for a period of five (5) years.

Bank invites responses to this tender for the following module

13.1 Consent & Privacy Governance Platform

- Data Discovery and Data Classification
- Data Inventory and Data Mapping
- Data Retention and Deletion
- Data Protection Impact Assessment

- Privacy Incident and Breach Management
- Consent and Privacy Notice Management
- Data Principal Rights Management
- Third-Party Risk Management (TPRM)
- Cookie Management
- Notice Management
- Consent Life Cycle Management
- Data Processor Privacy Risk Management
- Governance and Compliance Dashboard

13.2 Integration Requirements

- Core Banking System (CBS) – bidirectional integration for customer data and consent propagation
- CRM System – for customer communications and consent status updates
- Internet Banking & Mobile Banking Platforms
- HR System – for employee data and consent
- NeGD (National e-Governance Division) Platform for government integration
- LDAP/Active Directory for authentication and authorization
- SIEM/ITSM tools for incident management integration

13.3 Training Requirements

- Administrator training for IT/IS teams
- End-user training for business teams (Compliance, Legal, Operations, Customer Service)
- DPO/CISO training on platform capabilities and regulatory reporting
- Training materials, user manuals, SOPs, and knowledge base documents

All training must be completed before Go-Live of the respective phase.

13.4 Documentation Requirements

- As-built architecture documentation
- Installation and configuration guide
- Operations and maintenance manual
- Disaster Recovery runbook

- Security architecture document
- Data flow diagrams and system integration specifications

13.5 Regulatory & Legal Compliance Obligation

- The bidder shall design, configure, deploy, and support the solution in full compliance with the Digital Personal Data Protection Act, 2023, applicable Rules and Guidelines issued by MeitY, RBI Master Directions, CERT-In advisories, and the Bank's internal IT, Information Security, and Data Privacy policies applicable as on the date of go-live and during the contract period.
- Any regulatory non-compliance, supervisory observation, or adverse audit finding attributable to deficiencies in the solution, its configuration, or implementation shall constitute a material breach of this SOW.

13.6 Acceptance & Go-Live Criteria

Final acceptance shall be subject to successful completion of: - Functional and User Acceptance Testing (UAT) - Security, vulnerability, and performance testing - Validation of consent enforcement across all configured use cases - Closure of all critical and high-severity defects - Submission of complete as-built documentation, configuration artefacts, and audit logs.

Go-live shall not be deemed successful until written acceptance is issued by the Bank.

13.7 Audit, Inspection & Regulatory Support

The Implementing Partner shall provide all information, logs, system access, documentation, and clarifications required during internal audits, statutory audits, RBI inspections, CERT-In reviews, or DPDP-related regulatory inquiries, at no additional cost during the contract period. The bidder shall coordinate and ensure closure of all internal and external audit observations. No additional cost shall be borne by the Bank for audit observation closure.

14. Other Terms

1. The Bank shall provide virtualized compute and storage infrastructure. The Bidder shall provide hardware sizing and shall not factor hardware costs.
2. The Bank shall provide operating system and database software licenses. The Bidder shall not factor these licenses.

3. The Bank shall provide virtualized Infrastructure, Load Balancer, Server OS (Linux/Windows), and Database (Oracle/MS SQL) licenses. The Bidder shall use only Bank-provided OS and DB licenses and factor all other required software licenses.
4. The solution shall support High Availability architecture:
   (a) Active-Active or Active-Passive within a single site (DC or DR)
   (b) Active-Passive across DC and DR
5. The proposed solution shall be deployed on premises with RBAC, SSO Integration, encryption, logging, and SIEM integration.
6. The Bidder shall coordinate with the Bank's for implementation, go-live, and ongoing support.
7. The Bidder shall be responsible for end-to-end management, operations, and support of the platform throughout the contract period.
8. One-click generation of regulator-ready evidence pack including consent logs, DPIA references, rights request logs, breach reports, SLA performance and audit trail.

15. Additional Scope of Work

15.1 Testing and Validation

The bidder shall:

1. Prepare comprehensive test plans and test cases and capture all testing artefacts, including evidence, and share the same with the Bank.
2. Conduct performance and load testing to ensure the solution can sustainably handle the Bank's current and projected workloads.
3. Test all integrations with critical applications, including but not limited to:
   - Version control systems
   - Build systems
   - Issue and ticketing tools
4. Collaborate with business teams to execute User Acceptance Testing (UAT) for all integrations and releases.
5. Coordinate with the Bank's appointed consultant(s), where applicable, throughout the testing lifecycle.

15.2 Reporting and Metrics

The bidder shall:

1. Establish reporting mechanisms to track Key Performance Indicators (KPIs) and security metrics.
2. Generate, review, and distribute reports to relevant stakeholders at agreed frequencies.

15.3 Security Requirements

The solution shall:

1. Support standard authentication mechanisms including Active Directory (AD) and SAML.
2. Support different authentication mechanisms for different user populations.
3. Ensure all connections and data transmissions to on-premises applications occur over encrypted channels.

15.4 Compliance and Governance

The bidder shall:

1. Ensure the solution aligns with all applicable Indian regulatory and statutory requirements, including the Digital Personal Data Protection Act, 2023.
2. Define and implement a governance model covering ownership, escalation, and accountability.

15.5 Expected Implementation Deliverables

The bidder shall deliver, at a minimum:

1. Complete implementation documentation including configurations, versioning, and customizations.
2. Documented pre-requisites, assumptions, dependencies, risks, and mitigation strategies.
3. Approved Project Management Plan.
4. Meeting briefings, presentations, and MOMs.
5. Periodic Status Reports (Weekly / Monthly / Quarterly).
6. Test Strategy and Test Plans.
7. Test cases for Development, UAT, and Production environments.
8. Uptime and availability reports.
9. Application rollback and migration plan to ensure service continuity.

10. Setup and maintenance of three environments – Development/UAT and Production (DC&DR)
11. Updated requirement documents.
12. High-Level Design (HLD) and Low-Level Design (LLD) documents.
13. Bug tracker and Lessons Learned Register, reviewed at each project phase.
14. Closure of VA/PT, IS Audit, and other audit observations prior to go-live.
15. Technical Architecture Manual (TAM).
16. Technical Operations Manual (TOM).
17. SOPs for day-to-day operations with monitoring checklists.

15.6 Other Functional and Technical Requirements

The proposed solution shall:

1. Support multilingual capabilities as per Schedule 8 of the Indian Constitution.
2. Provide version control for consent forms with complete audit history.
3. Maintain immutable audit trails for all consent activities.
4. Support real-time synchronization of consent data across systems.
5. Enable hierarchical and granular consent management.
6. Maintain a centralized consent repository.
7. Provide end-user dashboards for viewing and downloading consent history.
8. Support granular consent preferences and self-service revocation.
9. Provide real-time consent analytics and automated renewal workflows.
10. Support high volume, low latency operations.
11. Provide secure deletion, masking, and anonymization.
12. Integrate with Bank ITSM tools.
13. Support escrow of source code at no cost.
14. Support DC/DR High Availability architecture and DR drills.
15. Support physical, assisted, offline, and third-party consent capture.
16. Support high-availability architectures (Active-Active / Active-Passive).

Annexure - 1

(To be printed in Company Letter Head)

Vendor Onboarding Evaluation Sheet - Detailed Due Diligence & Risk Assessment

Sl. No.	Parameters	Response
1.	Vendor Name	
2.	Vendor Full Address	
3.	Constitution of Service Provider	
4.	Details of Authorized person responsible to conduct Business of the service provider	
5.	Contact Numbers	
6.	Contact email ID	
7.	Service Description	
8.	Brief description on analysis of financial soundness and ability to meet service commitments to the Bank.	
9.	Staff Strength, their Qualification and Experience relating to the nature/scope of work	
10.	Please furnish the length of association with other Banks.	

	Parameters	Yes	No	N/A	Response / Explanations & References to Attachments if any
11.	Does the vendor have sufficient Infrastructure available to provide the services to Bank	☐	☐	☐	
12.	Does the vendor possess enough past experience for the service provided	☐	☐	☐	
13.	Does the vendor conduct Employee Back Ground verification	☐	☐	☐	
14.	Does the vendor provides similar services to other Bank's.	☐	☐	☐	
15.	Does the vendor follow adequate Risk Management practices	☐	☐	☐	

Sl. No.	Control Requirement	Vendor Response			Response / Explanations & References to Attachments if any
		Yes	No	N/A	
1	Has the bidder/vendor been in continuous operation for more than two (2) years as of the date of submission of the bid	☐	☐	☐	
2	Does the bidder/vendor maintain documented policies and procedures governing the delivery of the proposed services	☐	☐	☐	
3	Is the bidder/vendor a duly registered corporate entity and compliant with all applicable local laws and regulatory requirements.	☐	☐	☐	
4	Are there any ongoing or pending litigation proceedings, regulatory investigations, insolvency or bankruptcy proceedings against the bidder/vendor or any of its directors, key management personnel, or promoters.	☐	☐	☐	
5	Will 100% of the Bank's data, including production data, logs, backups, metadata, and master databases, be stored, hosted, processed, and transmitted strictly within the geographical boundaries of India.	☐	☐	☐	
6	Is the bidder/vendor willing to disclose the exact physical address and geographical region of the Primary and Recovery Data Centres where the Bank's data will be stored, hosted, processed, or backed up.	☐	☐	☐	
7	Does the bidder/vendor implement a documented logical segregation architecture to ensure that the Bank's data is securely isolated from the data of other clients.	☐	☐	☐	
8	Does the bidder/vendor implement end-to-end encryption for the Bank's data using strong, industry-standard encryption protocols. Please specify the encryption algorithms and protocols used for data at Rest/Transit.	☐	☐	☐	
9	Does the bidder/vendor maintain valid and current independent third-party security certifications, attestations, or compliance reports relevant to the proposed services. Please provide copies of the following,	☐	☐	☐	

Sl. No.	Control Requirement	Vendor Response			Response / Explanations & References to Attachments if any
		Yes	No	N/A	
	wherever applicable (ISO/IEC 27001:2022, SOC 2 Type II)				
10	Does the bidder/vendor conduct regular Vulnerability Assessment and Penetration Testing (VAPT) of the proposed application, APIs, and supporting infrastructure. Please provide the Executive Summary of the latest VAPT report, conducted within the preceding twelve (12) months, including the scope, assessment date, key findings, and current status of identified vulnerabilities.	☐	☐	☐	
11	Does the bidder/vendor enforce Multi-Factor Authentication (MFA) and strict Role-Based Access Controls (RBAC) across all environments that host, access, process, or support the Bank's application and infrastructure.	☐	☐	☐	
12	Does the bidder/vendor maintain and follow a documented patch and vulnerability management policy covering the timely identification, assessment, prioritisation, testing, and deployment of security patches and updates. Please specify the committed remediation timelines for security vulnerabilities based on severity, particularly for Critical and High-severity vulnerabilities, from the date of identification or disclosure.	☐	☐	☐	
13	Does the bidder/vendor maintain a documented and regularly reviewed Software Development Life Cycle (SDLC) policy incorporating secure software development practices and formal change management requirements. Please specify the SDLC methodology/framework followed and the frequency of review and update of the SDLC policy.	☐	☐	☐	
14	Does the bidder/vendor maintain and implement secure coding standards and practices, provide periodic security awareness and secure coding training to developers, conduct formal code reviews, perform automated security testing, and	☐	☐	☐	

Sl. No.	Control Requirement	Vendor Response			Response / Explanations & References to Attachments if any
		Yes	No	N/A	
	remediate identified vulnerabilities prior to production release. Please provide details/evidences.				
15	Does the bidder/vendor maintain documented Service Level Agreements (SLAs), a current Software Bill of Materials (SBOM), and formal software supply chain security controls to manage service performance, software component vulnerabilities, and risks associated with third-party and open-source software.	☐	☐	☐	
16	Does the bidder/vendor incorporate threat modelling into the application design and development process using a defined methodology, with identified threats documented, assessed, prioritised, remediated, and periodically reviewed.	☐	☐	☐	
17	Does the bidder/vendor maintain a documented process to identify, monitor, track, and manage End-of-Support (EOS) and End-of-Life (EOL) software, hardware, and third-party components, including the timely remediation, upgrade, replacement, or retirement of unsupported components.	☐	☐	☐	
18	Does the bidder/vendor conduct formal Disaster Recovery (DR) and Business Continuity drills at least annually to validate the effectiveness of its recovery and continuity arrangements.	☐	☐	☐	
19	Has the bidder/vendor defined and documented the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the proposed system/service.	☐	☐	☐	
20	Has the bidder/vendor experienced any significant cybersecurity incident, data breach, or security compromise during the last three (3) years.	☐	☐	☐	
21	Does the bidder/vendor maintain a documented incident response and breach notification process to ensure the Bank is notified immediately, in accordance with applicable regulatory requirements and RBI expectations for prompt reporting, in	☐	☐	☐	

Sl. No.	Control Requirement	Vendor Response			Response / Explanations & References to Attachments if any
		Yes	No	N/A	
	the event of a confirmed data breach, ransomware attack, or other significant cybersecurity incident.				
22	Is the bidder/vendor financially sound and capable of fulfilling its financial, operational, and contractual obligations throughout the proposed contract period.	☐	☐	☐	
23	Does the bidder/vendor engage or rely on any third-party sub-contractors, service providers, or other fourth parties for the delivery of any core or critical component of the proposed services.	☐	☐	☐	
24	Does the bidder/vendor unconditionally agree to include provisions in the final Master Service Agreement (MSA) and Service Level Agreement (SLA) granting the Bank's internal and external auditors, as well as the Reserve Bank of India (RBI), the right to audit and inspect the bidder/vendor's premises, systems, processes, records, and applicable controls, whether physically or remotely, as required by applicable regulatory and contractual requirements.	☐	☐	☐	
25	Will the bidder/vendor provide audited financial statements, including the Balance Sheet and Profit and Loss Account/Statement of Profit and Loss, for the last three (3) consecutive financial years.	☐	☐	☐	

Place:

Date: Signature with Seal