**Ref: RFP No. GEM/2026/B/7823086** **Date: 23/07/2026**

**REQUEST FOR PROPOSAL (RFP)**

**FOR**

**ENGAGEMENT OF VENDOR FOR SUPPLY, IMPLEMENTATION, INTEGRATION AND MANAGEMENT OF AN ENTERPRISE DATA PRIVACY GOVERNANCE & COMPLIANCE PLATFORM, INCLUDING SUPPLY AND INSTALLATION OF REQUIRED HARDWARE, FOR COMPLIANCE WITH DPDP ACT, 2023 AND DPDP RULES, 2025**

| | |
|---|---|
| RFP Reference No. | **GEM/2026/B/7823086** |
| RFP Issuance Date | **23/07/2026** |
| Last Date of request for Queries/ Clarifications | **27/07/2026 by 05:00 PM** |
| Date and time of Pre-Bid Meeting | **28/07/2026 at 03:00 PM** |
| Last Date for receipt of bids | **07/08/2026 at 03:00 PM** |
| Date and time of opening technical bids | **07/08/2026 at 03:30 PM** |

**Issued by:**

Indian Bank,

**Information Technology Department**,

4th Floor 66 Rajaji Salai, Chennai - 600001

Email: dpdpcell@indianbank.bank.in

Website: https://www.indianbank.bank.in

**Table of Contents**

**SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION**

| S. No | Particulars | Timeline |
|---|---|---|
| 1 | **Issuance Date of RFP**<br><br>(Date of RFP Issuance) | **23/07/2026** |
| 2 | **Last Date of request for Queries/ Clarifications**<br><br>(Last Date of receiving request for queries / clarifications before the Pre-bid Meeting) | **27/07/2026 by 05:00 PM** [to be submitted through GeM Portal or sent through email on email-id dpdpcell@indianbank.bank.in<br><br>Format for seeking clarification is enclosed as Annexure-XIII |
| 3 | **Pre–bid Meeting Date and Venue Details** | **28/07/2026 at 03:00 PM** through physical/virtual mode. Bidders willing to participate in pre-bid meeting need to submit their details at dpdpcell@indianbank.bank.in on or before 28/07/2026 01.00 PM.<br><br>Details of virtual/ physical pre-bid meetings would be communicated via e-mail to interested bidders separately. |
| 4 | **Last Date of Submission/ Closing Date in Online & Offline Mode**<br><br>(Last Date of Submission of RFP Response) | **07/08/2026 at 03:00 P.M**. for both online bid and offline document submissions.<br><br>For Offline submission of documents listed in Sl. No. 9 below, the sealed envelope shall be addressed to the Bank and to be delivered at the address below.<br><br>General Manager,<br>Information Technology Department, 4th Floor, Indian Bank Head Office,<br>66 – Rajaji Salai, Chennai 600001 |
| 5 | **Eligibility cum Technical Bid Opening Date** | **07/08/2026 at 03:30 PM** |
| 6 | **Date, time and venue of presentation & demo by the eligible** | Shall be intimated separately by the Bank through email. |

| | | |
|---|---|---|
| | **bidders** | |
| 7 | **Opening of Commercial Bids** | The commercial bids will be opened for those Bidders who qualify in both eligibility and technical evaluation.<br><br>The date for commercial bid opening would be communicated via e-mail to the technically eligible Bidders. |
| 8 | **Online Bid Submission Details** | This RFP will follow e-Procurement (e-Tendering) process and the same will be conducted through Government e-Market Place (GEM) portal.<br><br>The documents listed below in Sl. No 9 below only to be submitted in offline physical mode. |
| 9 | **Documents to be submitted physically by Bidders (offline Mode)** | 1. Bid Security (EMD) for Rs.1,00,00,000/- (Rupees One Crore only) to be submitted in the form of DD/ Fund transfer/ Bank Guarantee (issued by a nationalized/ scheduled commercial Bank (other than Indian Bank)) in favor of “Indian Bank” payable at Chennai. BG should be valid for 165 days from the last date for submission of the Bid (or) Fund transfer to be made in the account as detailed below:<br><br>Account No.: 743848138<br>Account Name: INDIAN BANK, H.O. TECHNOLOGY MANAGEMENT DEPARTMENT-II<br>IFSC Code: IDIB000H003<br>Branch: Harbor<br><br>2. Pre-Contract Integrity Pact (Please refer to ANNEXURE VI) |
| 10 | **RFP Coordinator** | 1. Shri. Vivek Kumar Singh<br>Assistant General Manager<br>Email: vivek.singh@indianbank.bank.in<br>Contact No: 9987175205<br><br>2. Smt. Sathiyapriya Somasundaram<br>Manager<br>Email: sathiyapriya.somasundaram@indianbank.bank.in<br>Contact No: 9600612882 |

**The RFP document can also be downloaded from:**

1. **Bank’s website:** https://www.indianbank.bank.in **and**
2. **Government e- Market Place (GeM) portal**

Any clarifications, modifications, or extensions of dates will be published only on the above-mentioned Bank website and GeM portal. A public notice will also be issued in newspapers to inform about the RFP publication.

I. Note: Indian Bank does not take responsibility of any offers damaged/lost in transit/delivered at incorrect address prior to its receipt at the Bank's designated office.

II. Bank will follow two bidding system Part-I (Technical Bid) of the bid contains compliance details of the eligibility and terms & conditions set in the RFP document (including annexures) for which quotation is called for. Bidders should enroll / register before participating through e-procurement portal (GeM). Bids have to be submitted online only through Government e- Market Place (GeM) portal along with physical submission of documents mentioned in Point No. 9 of Schedule [A] (Important Dates and Information on RFP Submission). Further Bidders must submit their commercial bid as per the format given in the RFP (as per Appendix II of Section-V) along with the technical bid on the e-procurement (GeM) portal. Technical bids submitted by all the bidders will be evaluated and only technically qualified bidders will be called for opening of commercial bids.

1. Bidders should enroll/ register before participating through Government e- Market Place (GeM) portal. All the documents in support of eligibility criteria etc. are also to be scanned and uploaded along with the tender documents. Any documents sent by any other mode will not be accepted.

2. Documents to be uploaded online duly signed by the Authorized Signatory under the seal of the bidder in every page. Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the bid will be liable for rejection.

3. The price quoted should be unconditional and should not contain any string attached thereto. Bid, which do not conform to our eligibility criteria and terms & conditions, will be liable for rejection.

III. The RFP document (and addendums, if any) needs to be signed and stamped by the Bidders and it must be submitted along with the Technical Bid. Further, compliance statement (as per Annexure-XVIII) duly signed by bidder also to be submitted along with Technical Bid.

IV. All times mentioned are as per Indian Standard Time (IST). The above dates and time are tentative and subject to change without any prior notice or intimation. If a holiday is declared on the dates mentioned above, the Bids shall be opened on the next working day at the same time specified unless communicated otherwise.

**This RFP is issued by:**

Shri. VISSA VENKATA RAMANA RAO
General Manager,
Information Technology Department,
4th Floor, Indian Bank Head Office,66, Rajaji Salai, Chennai 600001

## SCHEDULE [B] GLOSSARY OF TERMS

Following terms are used in the document interchangeably to mean:

1. Bank refers to 'Indian Bank (IB)' including its Branches, Administrative offices, processing centres/HUBS, cells and all other units and establishments etc. (excluding its overseas establishments, Subsidiaries / Joint Ventures and Regional Rural Banks)
2. Recipient, Respondent, Consultant, Consultancy firms, System Integrator / Technical partner / Technical Integrator, Bidder, Applicant means the respondent to the RFP document.
3. RFP means the "Request for Proposal" document.
4. Proposal, Bid means "Response to the RFP Document"
5. Tender means RFP response documents prepared by the Bidder and submitted to 'Indian Bank'
6. Selected bidder and the Bank shall be individually referred to as "party" and collectively as "parties".
7. The term "Bid" & "Quote/ Quotation" bears the same meaning in this RFP.
8. OEM refers to the entity that designs, develops, and manufactures the core hardware or software components proposed in response to this RFP.
9. Unless contrary to the context or meaning thereof, contract or agreement wherever appearing in this RFP shall mean the contract to be executed between the Bank and the successful bidder.

Other Terms and abbreviations**:**

| Sl. No. | Terms used in the RFP | Terms and abbreviations |
|---|---|---|
| 1 | API | Application Programming Interface |
| 2 | BAU | Business-as-Usual |
| 3 | BFSI | Banking, Financial Services and Insurance |
| 4 | CERT-In | Indian Computer Emergency Response Team |
| 5 | CSP | Cloud Service Provider |
| 6 | DC | Data Centre |
| 7 | DLP | Data Loss Prevention |
| 8 | DPBI | Data Protection Board of India |
| 9 | DPDP Act | Digital Personal Data Protection Act, 2023 |
| 10 | DPIA | Data Protection Impact Assessment |
| 11 | DPRM | Data Principal Rights Management |
| 12 | DR | Disaster Recovery |
| 13 | EMD | Earnest Money Deposit |
| 14 | GeM | Government e-Marketplace |
| 15 | GOI | Government of India |

| | | |
|---|---|---|
| 16 | GST | Goods and Services Tax |
| 17 | IAM | Identity and Access Management |
| 18 | IBA | Indian Banks' Association |
| 19 | IDS/IPS | Intrusion Detection System / Intrusion Prevention System |
| 20 | IPR | Intellectual Property Rights |
| 21 | ISO | International Organization for Standardization |
| 22 | IT | Information Technology |
| 23 | JSON | JavaScript Object Notation |
| 24 | KT | Knowledge Transfer |
| 25 | LLP | Limited Liability Partnership |
| 26 | NDA | Non-Disclosure Agreement |
| 27 | OEM | Original Equipment Manufacturer |
| 28 | PBG | Performance Bank Guarantee |
| 29 | PII | Personally Identifiable Information |
| 30 | POC | Proof of Concept |
| 31 | RACI | Responsible, Accountable, Consulted, Informed |
| 32 | RBAC | Role-Based Access Control |
| 33 | RBI | Reserve Bank of India |
| 34 | ROPA | Records of Processing Activities |
| 35 | SDK | Software Development Kit |
| 36 | SI | System Integrator |
| 37 | SIEM | Security Information and Event Management |
| 38 | SIT | System Integration Testing |
| 39 | SLA | Service Level Agreement |
| 40 | SOAR | Security Orchestration, Automation, and Response |
| 41 | SOD | Segregation of Duties |
| 42 | SOW | Scope of Work |
| 43 | TCO | Total Cost of Ownership |
| 44 | TPRM | Third Party Risk Management |
| 45 | UAT | User Acceptance Testing |
| 46 | UEBA | User and Entity Behaviour Analytics |
| 47 | WCS | Weighted Commercial Score |
| 48 | WTS | Weighted Technical Score |
| 49 | XML | Extensible Markup Language |
| 50 | AMC | Annual Maintenance Contract |
| 51 | ATS | Annual Technical Support |
| 52 | BOM / BoM | Bill of Materials |
| 53 | CBS | Core Banking System |

| | | |
|---|---|---|
| 54 | CRM | Customer Relationship Management |
| 55 | DPO | Data Protection Officer |
| 56 | DPR | Data Principal Request |
| 57 | GFR | General Financial Rules |
| 58 | HA | High Availability |
| 59 | HLD | High-Level Design |
| 60 | LLD | Low-Level Design |
| 61 | KYC | Know Your Customer |
| 62 | AML | Anti-Money Laundering |
| 63 | MAF | Manufacturer Authorization Form |
| 64 | MeitY | Ministry of Electronics and Information Technology |
| 65 | MIS | Management Information System |
| 66 | MSME | Micro, Small and Medium Enterprises |
| 67 | PAM | Privileged Access Management |
| 68 | RPO | Recovery Point Objective |
| 69 | RTO | Recovery Time Objective |
| 70 | SOP | Standard Operating Procedure |
| 71 | SSO | Single Sign-On |
| 72 | UPI | Unified Payments Interface |
| 73 | VAPT | Vulnerability Assessment and Penetration Testing |
| 74 | WAF | Web Application Firewall |
| 75 | AV | Anti-Virus |
| 76 | MFA | Multi-Factor Authentication |
| 77 | SDF | Significant Data Fiduciary |
| 78 | NIST | National Institute of Standards and Technology |
| 79 | LDAP | Lightweight Directory Access Protocol |
| 80 | SBOM | Software Bill of Materials |
| 81 | CBOM | Component Bill of Materials |

**Confidentiality:**

*This document is meant for the specific use by the Bidder/s to participate in the current tendering process. This document in its entirety is subject to Copyright Laws. Indian Bank expects the Bidders or any person acting on behalf of the Bidders strictly adhere to the instructions given in the document and maintain confidentiality of information.* ***The Bidder/s shall undertake that they shall hold the information received by them under the contract "in trust" and they shall maintain utmost confidentiality of such information. The Bidders have to agree and undertake that (a) They shall maintain and use the information only for the purpose of the contract as permitted by the Bank (b) To strictly allow disclosure of such information to its employees, agents and representatives on" need to know" basis only and to ensure confidentiality of such information disclosed to them****. The Bidders will be held responsible for any misuse of information contained in the document, and liable to be prosecuted by the Bank in the event that such a circumstance is brought to the notice of the Bank. By downloading the document, the interested parties are subject to confidentiality clauses.*

## SCHEDULE [C] DISCLAIMER

The information in this Request for Proposal ("RFP") document provided to bidders or applicants whether verbally or in documentary form by or on behalf of Indian Bank, is on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is made available. This RFP document is not an agreement, offer or an invitation by Indian Bank to enter into an agreement/contract in relation to the service but is meant for providing information to the applicants who intend to submit the bids (hereinafter individually and collectively referred to as "Bidder" or "Bidders" respectively). This RFP is designed with the purpose to assist the applicants/ Bidders to formulate their proposal and does not claim to provide all the information that may be required by the applicants/ Bidders.

Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP. Indian Bank and its directors, officers, employees, respondents, representatives, agents, and advisors make 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. The information contained in the RFP document is selective and is subject to updating, expansion, revision, and amendment. It does not purport to contain all the information that a Bidder require. Indian Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

The Bidders, by accepting this document, agree that any information contained herein may be superseded by any subsequent written information on the same subject made available to the recipient or any of their respective officers or published in the Bank's website. It is also understood and agreed by the Bidder/s that decision of the Bank regarding selection of the Bidder will be final and binding on all concerned. No correspondence in this regard, verbal or written, will be entertained. It shall be the duty and responsibility of the Bidders to ensure about their legal, statutory and regulatory eligibility and other competency, capability, expertise requisite for them to participate in this RFP process and to provide all the services and deliverables under the RFP to the Bank.

The applicant shall bear all its costs associated with or relating to the preparation and submission of its proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the Bank or any other costs incurred in connection with or relating to its proposal. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an applicant in preparation or submission of the proposal, regardless of the conduct or outcome of the selection process.

Indian Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Such change will be published on the Bank's Website and GEM Portal, and it will become part and parcel of RFP.

Indian Bank reserves the right to reject any or all the bids/proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Indian Bank shall be final, conclusive and binding on all the parties.

**SCHEDULE [D] GENERAL INFORMATION**

Indian Bank (hereinafter called the “Bank”) is floating Request for Proposal (RFP) for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance and compliance platform including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025.

Shortlisting of Bidders shall be done and informed after evaluation of the technical Bids submitted by the bidders participated in this RFP.

Bidders are hereby advised to carefully review and submit all relevant information in the same chronology under the relevant sections only, with their RFP responses.

Details of the objectives, scope of the services, eligibility and qualification criteria, data & documents required (if any) to be submitted along with RFP, criteria that would be adopted for evaluation of the responses for short listing and other information is contained in the RFP document.

The RFP document can be downloaded from GEM portal or from the Bank’s website www.indianbank.bank.in.

## SCHEDULE [E] OVERVIEW OF INDIAN BANK

**Indian Bank,** with Corporate Office in Chennai was established as part of the Swadeshi Movement on August 15, 1907.

Along with 13 other banks, the Bank was Nationalized on July 19, 1969. The Bank celebrated its centenary in August 2007. With effect from 1st April 2020, erstwhile Allahabad Bank merged into Indian Bank. The integration of CBS systems of both the banks was completed on 14.02.2021. Bank has established a rich legacy by providing quality financial services. It has passed through challenging times, successfully registered turnaround and emerged stronger than before. Given the ever-changing requirements, Bank fine-tuned its strategies and undertook several structural and operational changes and earned a coveted position in the Indian banking industry. Bank's foremost priority has been to serve the people and its nation.

The Bank has two subsidiaries viz., IndBank Merchant Banking Services Ltd and IndBank Global Support Services Ltd. (wholly owned subsidiary). Bank also has one joint venture namely Universal Sompo General Insurance Company Ltd.

The Bank has two sponsored Regional Rural Banks viz, Tamil Nadu Grama Bank; headquartered at Salem (Tamil Nadu) and Puduvai Bharathiar Grama Bank headquartered at Puducherry (UT of Puducherry).

The Bank has been pioneer in developing many digital products and received many awards on digital front.

Bank has been making profit continuously since 2002 and has been self-sustaining in terms of capital adequacy.

**VISION:**
"Delivering excellence in financial services through customer focus, employee engagement and sustainable growth"

**MISSION:**

- Bring the best of innovation and technology in our offerings
- Be responsive to the unique needs of every customer through all channels of choice
- To provide value to stakeholders
- Empower and engage our employees

As on 30th June 2026, the Bank's total Global Business reached Rs.15.29 Lakh Crore, comprising Deposits of Rs.8.44 Lakh Crore and Advances of Rs.6.85 Lakh Crore.

As on 30th June 2026 Bank has Pan-India network with 28,994 touch points including 6,007 Brick & Mortar branches including 3 DBUs + 1 IBU, 5,676 ATMs/BNAs and 17,314 Business Correspondents.

The Bank has expanded its footprint overseas with branches at Singapore, Colombo and Jaffna, besides a Foreign Currency Banking Unit in Colombo.

The Bank serves a customer base of 13.71 crore customers and has a workforce of 41,875 employees. Digital adoption continues to grow with 2.48 crore Mobile Banking users, 2.77 crore UPI users, 1.19 crore Internet Banking users, and 3.76 crore Debit Card users. The Bank also has 41,511 FASTag users and 27,922 POS users.

The Bank had always been a forerunner in offering digital products which provide hassle free, convenient, and safe transaction facilities to enhance customer experience, meeting their expectations as the country gears itself for riding on the digital wave. After the amalgamation, the Bank is poised to grow on both business and profitability fronts. The emphasis will be to leverage operational efficiencies, cost synergies and new opportunities in terms of Brand and reach to deliver enhanced customer experience. The focus will be on increasing the CASA share in deposits while looking at diversified growth in credit. Cost optimisation and increasing revenue with focus on fee income, improving recovery and containing NPAs will be levers to improve bottom line.

**Technology Environment**

Indian Bank has all its branches on Core Banking Solutions, has a range of customer centric and other solutions like full suite of Core Banking Solution, CRM, payment systems like IMPS, NEFT, RTGS, SWIFT, CTS, etc., alternate delivery channels viz., ATM, e-Kiosk, Internet Banking, Mobile Banking, e-payment of Taxes, Utility Bill, Ticket, Donation, etc., SMS alerts and Corporate Net Banking. Bank has launched an integrated mobile app having various functionalities with biometric / face id login.

Bank has also implemented solution for digital onboarding, both for liability and asset products. Bank is also in the process of setting up an Enterprise Data Lakehouse which will help them with single source of truth, powerful dashboards and data driven insights with advanced analytics including AI / ML and AI capabilities, to support their digital driven business growth.

As a part of enhancing customer experience, Bank has also launched an AI-Chatbot ADYA, that is currently available on Bank’s website and Mobile Banking App as an additional interface for answering customer queries and lead generation. Bank has launched Digital Banking Omni Channel Application “IndSMART” (Mobile Banking/Internet Banking) and established a Digital Lending Platform for catering to digital servicing of loans across Retail, Agri and MSME business streams. Bank's Information Systems and Security processes are certified with ISO27001:2022 standard and is among very few Banks certified worldwide.

Bank is having their DC, NDC, NDR and DR at below mentioned locations.

Data Center - Chennai
Near Data Center - Chennai
Near Disaster Recovery Site - Mumbai
Disaster recovery Site - Mumbai

**For further details, please visit Bank’s website [www.indianbank.bank.in](http://www.indianbank.bank.in)**

## SECTION – I
## REQUEST FOR PROPOSAL (RFP)

Indian Bank is a Public Sector Bank, headquartered at Chennai. The Bank has Pan-India network with 28,994 touch points including 6,007 Brick & Mortar branches including 3 DBUs + 1 IBU, 5,676 ATMs/BNAs and 17,314 Business Correspondents.

The Bank serves a customer base of 13.71 crore customers and has a workforce of 41,875 employees. Digital adoption continues to grow with 2.48 crore Mobile Banking users, 2.77 crore UPI users, 1.19 crore Internet Banking users, and 3.76 crore Debit Card users. The Bank also has 41,511 FASTag users and 27,922 POS users.

As on 30th June 2026, the Bank's total Global Business reached Rs.15.29 Lakh Crore, comprising Deposits of Rs.8.44 Lakh Crore and Advances of Rs.6.85 Lakh Crore.

Bank's Information Systems and Security processes are certified with ISO27001:2022 standard and is among very few Banks certified worldwide. It has overseas branches in Colombo, Singapore and Jaffna including a Foreign Currency Banking Unit at Colombo and an offshore banking unit in Gift City. Post-merger with Allahabad Bank, Indian Bank is the seventh largest bank in the country.

The Bank is interested in identifying vendor for supply, installation, implementation, integration, commissioning and maintenance of hardware, software and services for Enterprise Data Privacy Governance & Compliance Platform to comply with DPDP Act, 2023 and DPDP Rules, 2025. The Enterprise Data Privacy Governance & Compliance Platform must be implemented On-premise and should comply with Scope, Technical Specifications as specified in various sections of this RFP.

Bank will follow two bidding systems. Part-I of the bid contains Eligibility and Technical compliance details and Part-II of the bid contains Commercials of the specifications for which quotation is called for. The Bidders should enroll/ register before participating in bidding through GEM Portal. **Except for the documents required to be submitted in physical form to the Bank, Bids have to be submitted online only through GeM portal**. The bidders also need to submit necessary documents physically through offline mode to the address mentioned in the RFP.

Interested-eligible bidders may submit their quotation for providing Enterprise Data Privacy Governance & Compliance Platform as specified in Part-I as per the following procedure:

1. Bidders should apply through GeM Portal. All the documents in support of eligibility criteria etc. are also to be scanned and uploaded along with the tender documents. Bid Documents submitted/sent by any other mode will not be accepted.

   **Technical Glitch on GeM Portal**: In case of any technical glitch encountered on the Government e-Marketplace (GeM) portal during bid submission, the bidder must obtain and submit a written confirmation from GeM authorities certifying the occurrence of such technical issues. The Bank at its discretion may extend the bid submission not exceeding two weeks. Unless such written confirmation is provided, the Bank will not consider the issue as a technical glitch. No extension of bid submission timelines will be granted on account of unconfirmed technical glitches.

2. **Part-I** contains eligibility and technical compliance details of the specifications for which Bid is called for. No column shall be left blank or altered.

3. **Part-II** – Commercial along with price break up details to be submitted separately along with the bid documentation (open bidding process). After technical evaluation, intimation will be given to all qualifying bidders about the date and time of opening of commercial bids.

4. **Part-I** (Technical Bid) & **Part-II** (Commercial bid) to be uploaded online duly signed by the Authorized Signatory under the seal of the company in every page. The bidders also need to submit necessary documents physically through offline mode to the address mentioned in the RFP (under SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION, point 9). Any correction should be authenticated by the same signatory. If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the quotations will be liable for rejection. The price quoted in the Commercial bid should be unconditional and should not contain any strings attached thereto. The bids which do not conform to our specifications will be liable for rejection and offers with a higher configuration will not attract any special consideration in deciding the vendor.

5. Bank has the right to accept or reject any quotation/cancel the e-tender at its sole discretion, at any point, without assigning any reason thereof. Also, Bank has the discretion for amendment / alteration / extension before the last date of receipt of bid.

**MAKE IN INDIA**

This RFP is further governed by Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion order number P-45021/ 2/2017-B.E.-II dated 15th June 2017 for the Public Procurement (Preference to Make in India), Order 2017, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 28th May 2018, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 29th May 2019, revision order no DPIIT Order No. P-45021/2/2017-PP(BE-II) dated June 04, 2020 and subsequent revision order no. P-45021/2/2017-PP (B.E.-II) dated 16th Sept 2020 and subsequent revision Order No. No. P-45021/2/2017-PP (BE-ll)-Part (4) Vol. II dated 19/07/2024 and its amendment (if any).

Bank will follow the above orders and guidelines on Public Procurement (Preference to Make in India) and basis of allotment will be done in terms of the same.

1. Definitions: For the purpose of this RFP

    1. ’Local content’ means the amount of value added in India which shall, unless otherwise prescribed by the nodal ministry, be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.

    2. ‘Class-I local supplier’ means a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%, as defined under this Order.

    3. ‘Class-II local supplier’ means a supplier or service provider, whose goods, services or works offered for procurement, has local content more than 20% but less than 50%, as defined under this Order.

4. 'Non - Local supplier' means a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%, as defined under this Order.

5. 'L1' means the lowest tender or lowest bid or the lowest quotation received in a RFP, bidding process or other procurement solicitation as adjudged in the evaluation process as per the RFP or other procurement solicitation.

6. 'Margin of purchase preference' means the maximum extent to which the price quoted by a "Class-I local supplier' may be above the L1 for the purpose of purchase preference.

2. Eligibility of 'Class-I local supplier'/ 'Class-II local supplier'/ 'Non-local suppliers' for different types of procurement

a. In procurement of all goods, services or works in respect of which the Nodal Ministry/Department has communicated that there is sufficient local capacity and local competition, only 'Class-I local supplier', as defined under the Order, shall be eligible to bid irrespective of purchase value.

b. In procurement of all goods, services or works, not covered by sub-para ii(a) above, and with estimated value of purchases less than Rs.200 Crore, in accordance with Rule 161(iv) of GFR, 2017, Global tender enquiry shall not be issued except with the approval of competent authority as designated by Department of Expenditure. Only 'Class-I local supplier' and 'Class-II local supplier', as defined under the Order, shall be eligible to bid in procurements undertaken by procuring entities, except when Global tender enquiry has been issued. In global tender enquiries, 'Non-local suppliers' shall also be eligible to bid along with 'Class-I local suppliers' and 'Class-II local suppliers'

3. Purchase Preference

a. 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 bank in the manner specified here under.

b. In the procurements of goods or works which are covered by para ii(b) above and which are divisible in nature, the 'Class-I local supplier shall get purchase preference over 'Class-II local supplier', as per following procedure:

   i. In case there is sufficient local capacity and competition for the item to be procured, as noted by the nodal ministry, only class I local suppliers shall be eligible to bid. As such, the multiple suppliers who would be awarded the contract, should be all and only 'Class-I local suppliers'

   ii. In other cases, 'Class II local suppliers' may also participate in the bidding process along with 'Class-I local suppliers' as per provisions of this Order.

   iii. If 'Class-I local suppliers' qualify for award of contract for at least 50% of the tendered quantity, the contract will be awarded to all the qualified bidders as per the award criteria stipulated in the bid document. However, in case 'Class-I local suppliers' do not qualify for award for contract for at least 50% of the tendered quantity, purchase preference will be given to the 'Class-I local suppliers' over 'Class-II local suppliers' provided that their quoted rate falls within 20% margin of purchase preference of the highest quoted considered for award of contract so as to ensure that the 'Class-I local suppliers' taken in totality are considered for award of contract for at least 50% of the tendered quantity.

iv. First purchase preference will be given to the lowest quoting 'Class-I local suppliers', whose quoted rates fall within 20% margin of purchase preference, subject to its meeting the prescribed criteria for award of contract as also the constraint of maximum quantity that can be sourced from any single supplier. If the lowest quoting 'Class-I local suppliers', does not qualify for purchase preference because of aforesaid constraints or does not accept the offered quantity, an opportunity may be given to next higher 'Class-I local suppliers', falling within 20% margin of purchase preference, and so on.

v. To avoid any ambiguity during bid evaluation process, Bank may stipulate its own RFP/tender specific criteria for award of contract amongst different bidders including the procedure for purchase preference to 'Class-I local suppliers' within the broad policy guidelines stipulated in sub-paras above.

vi. Make In India purchase preference would not be applicable where evaluation is based inter-alia on non-price criteria e.g., QCBS or FBS in Services and Works.

4. Margin of Purchase Preference: The margin of purchase preference shall be 20%.

5. Verification of Local Content:

a. If nodal ministry is satisfied and communicates to bank that Indian suppliers of an item are not allowed to participate and /or compete in procurement by any foreign government, it may, if it deems appropriate, restrict or exclude bidders from that country from eligibility for procurement of that item as per advise of nodal ministry.

For the Purpose of above, a Supplier or bidder shall be considered to be from a country if (i) the entity is incorporated in that country, or ii) a majority of its shareholding or effective control of the entity is exercised from that country; or (iii) more than 50% of the value of the item being Supplied has been added in that country. Indian suppliers shall mean those entities which meet any of these tests with respect to India." Declaration to be submitted by bidder as per Annexure-X.

Bank will also provide benefits to Micro and Small Enterprises (MSEs) as per the guidelines of public procurement policy issued by Government of India. The bidders to submit declaration for claiming MSE Benefits as per Annexure-VIII.

**STARTUP**

Bank will also provide relaxation to startups as defined in the RFP document. For claiming the same, the Bidder must submit its valid startup certificate.

1. Applicable for Indian Bidders only as defined in gazette notification no. D.L-33004/99 dated 11.04.2018 of Ministry of Commerce and Industry and as amended from time to time.

2. As mentioned in Section-II of O.M. No.F.20/2/2014-PPD(Pt.) dated 20.09.2016 of Procurement Policy Division, Department of Expenditure, Ministry of Finance on Prior turnover and prior experience, relaxations may be applicable for all Startups [whether Micro & Small Enterprises (MSEs) or otherwise] subject to meeting of the quality and technical specifications specified in RFP document.

3. Further, the Startups are also exempted from submission of EMDs.

4. For availing the relaxations, bidder is required to submit requisite certificate towards Startup enterprise registration issued by Department of Industrial Policy and Promotion, Ministry of Commerce and the certificate should be certified by the Chartered Accountant (not being an employee or a director or not having any interest in the bidder's company/firm) and notary public with legible stamp. These relaxations do not dilute compliance with technical, security, and regulatory requirements specified in the RFP.

5. Startup purchase preference would not be applicable where evaluation is based inter-alia on non-price criteria e.g., QCBS or FBS in Services and Works.

**RESTRICTION OF BIDDERS FROM COUNTRIES SHARING LAND BORDERS WITH INDIA:**

As per Ministry of Finance, Department of Expenditure, Public Procurement Division's office memorandum F.No.6/18/2019-PPD dated 23.07.2020, regarding insertion of Rule 144 (xi) in the General Financial Rules (GFR) 2017 and all subsequent amendments in GFR, Manual for procurement of goods 2022 and manual for procurement of consultancy and other services 2022, any bidder from a country which shares a land border with India will be eligible to bid either as a single entity or as a member of a JV / Consortium with others, in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) only if the bidder is registered with the Competent Authority. The Competent Authority for registration will be the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT). Political & Security clearance from the Ministries of External and Home Affairs respectively will be mandatory.

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

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

However, as per the office memorandum F.No.18/37/2020-PPD dated 08/02/2021 issued by the ministry,

A Bidder is permitted to procure raw material, components, subassemblies etc. from the vendors from countries which shares a land border with India. Such vendors will not be required to be registered with the competent authority, as it is not regarded as "sub-contracting".

However, in case a Bidder has proposed to supply finished goods procured directly/indirectly from the vendors from the countries sharing land border with India, such vendor will be required to be registered with the competent authority.

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

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

1. An entity incorporated, established or registered in such a country; or
2. A subsidiary of an entity incorporated, established or registered in such a country; or
3. An entity substantially controlled through entities incorporated, established or registered in such a country; or
4. An entity whose beneficial owner is situated in such a country; or
5. An Indian (or other) agent of such an entity; or
6. A natural person who is a citizen of such a country; or
7. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

"Beneficial owner" will be as under:

i. In case of a company or Limited Liability Partnership (LLP), the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means.

    a. Explanation "Controlling ownership interest" means ownership of, or entitlement to, more than twenty-five per cent of shares or capital or profits of the company;

    b. "Control" shall include the right to appoint the majority of the directors or to control the management or policy decisions, including by virtue of their shareholding or management rights or share-holders agreements or voting agreements.

ii. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

iii. 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 juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

v. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

Please note that

1. The cost of preparing the bids, including visit / visits to the Bank is not reimbursable.

2. The Bank is not bound to accept any of the bids submitted and the bank has the right to reject any/all bid/s or cancel the tender at any point without assigning any reason thereof.

3. All pages of the Bid document, Clarifications/Amendments if any should be sealed and signed by the Authorized Signatory and to be uploaded with technical bid. A certificate to the effect that the Authorized Signatory has authority to bind the company should also be attached along with the technical bid.

4. The Authority/Bank shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP, Bidding Documents or the Bidding Process, including any error or mistake therein or in any information or data given by the Authority.

5. Bidder should notify the Bank of any error, fault, omission, or discrepancy found in this RFP document but not later than Last Date of request for Queries/ Clarifications specified in this RFP or in any subsequent amendments.

6. Nothing in this Agreement shall obligate either Party to enter into any further Agreements.

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

**Note:** Due to the complexity, single ownership and integration required with multiple applications of the bank, the tender will not be split and will be awarded to the single bidder only. Either the OEM (Principal) or authorized partner/bidder on behalf of the OEM may participate, but not both. If both submit bids then only the bid from the OEM (Principal) will be considered, and the partner's bid will be rejected.

**SECTION-II**

**INSTRUCTIONS TO BIDDERS**

**1. Introduction**

The Bidder is expected to examine all instructions, forms, terms and specifications given in the Bidding Documents. If any element of doubt arises, the same should be clarified from the Bank before submitting the bid. Failure to furnish all information required by the Bidding Documents may result in the rejection of its bid and will be at the Bidder's own risk. Bank will not be responsible for the same.

**2. Pre-Bid Meeting**

a. A pre-bid meeting is scheduled to be held through physical mode (offline) / Video Conference / Web-ex as per the schedule mentioned in section SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION**.** Bidder's designated representatives (maximum two persons) may attend the pre-bid meeting.

b. The purpose of the meeting will be to clarify the doubts raised by the probable bidders.

c. Bidder is requested to submit any queries/clarifications to the Bank to the following email id on or before the schedule mentioned in section SCHEDULE [A]: IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION. Bidder can submit their queries in GeM portal or send their queries to the email address - dpdpcell@indianbank.bank.in. Queries must include clear and concise question(s) referencing the specific section/clause of the RFP document. Bidder is advised not to include sensitive information in their queries.

d. Bidder needs to note that the query should be strictly sent in the excel sheet and as per the Annexure XIII.

**3. Amendment of bidding documents**

a. At any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification(s) requested by a prospective Bidder, may modify / cancel / extend / amend the Bidding Document by modification(s) / amendment(s).

b. All prospective bidders will be communicated of the details of amendments and clarifications. Signed copy of the amended document should form part of the Technical Bid. The amendments if any, will be published in Bank website www.indianbank.bank.in and in the GeM Portal and will form part of the Bidding document.

c. The bid submitted cannot be withdrawn / modified after the last date for submission of the bids unless specifically permitted in writing by the Bank.

**4. Technical Bid**

The Bidder shall furnish as part of its technical bid, documents establishing the bidder's eligibility to bid and its qualifications to perform the Contract.

The documentary evidence of the Bidder's eligibility to bid and qualifications to perform the Contract if its bid is accepted, shall establish to the Bank's satisfaction that, the Bidder has the financial and technical capability necessary to perform the Contract and that, the Bidder meets the qualification requirements.

**Note:** Incomplete submissions or bids not accompanied by the above documents will be rejected without further notice.

**5. Commercial Bid**

a. The Bank will open commercial bids after technical bid evaluation and a notice will be given to the technically qualified bidders.

b. The calling for quote does not confer any right on the bidder for being awarded any purchase order.

c. The price submitted by Bidders in GeM portal will be treated as the final offer of that bidder and bid will be evaluated accordingly.

d. The Bidder is requested to quote in Indian Rupee (INR). Bids in currencies other than INR would not be considered. The prices quoted by the Bidder shall be inclusive of all taxes, duties, levies etc. including GST.

e. There will be no price escalation during the contract period. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected

**6. Clarification of Bids**

During evaluation of the bids, the Bank may, at its discretion, seek clarification from the Bidder/s. The request for clarification and the response shall be in writing by email to dpdpcell@indianbank.bank.in and no change in the substance of the bid shall be sought, offered, or permitted.

The Bidder shall make his/her own interpretation of any and all information provided in the Bidding Document. The Bank shall not be responsible for the accuracy or completeness of such information and/or interpretation. Although certain information is provided in the Bidding Document, however, bidder shall be responsible for obtaining and verifying all necessary data and information, as required by him. The Bank reserves the right to accept or reject any/ all tender in whole or in part without assigning any reason whatsoever. The Bank shall not be bound to accept the lowest tender and reserves the right to accept any or more tenders in part. Decision of Bank in this regard shall be final.

**7. Bid Security (Earnest Money Deposit)**

The Bidder should submit at the time of online submission of Bid, as part of its bid, a bid security / EMD in the form of DD/ Fund transfer/ Bank Guarantee issued by a Scheduled Commercial Bank located in India (other than Indian Bank), in the form provided in the Bidding Documents (Annexure - XVII) for a sum of Rs.1,00,00,000/- (Rupees One Crore only) valid for 165 days from the last date for submission of Bid. Bank may seek extension of Bank Guarantee, if required. Relaxation if any, extended by GOI/ competent authorities for furnishing the EMD shall be passed on to the bidders. In case of fund transfer, bid security amount is to be remitted to following account:

Account No.: 743848138
Account Name: INDIAN BANK, H.O. TECHNOLOGY MANAGEMENT DEPARTMENT-II
IFSC Code: IDIB000H003
Branch: Harbour

Note: Bidders must include their bid reference number in the transaction remarks for easy identification.

Unsuccessful Bidders' Bid Security will be discharged or returned within 30 days from the date of bid evaluation completion. The successful Bidder's Bid Security will be discharged upon the Bidder signing the Contract and furnishing the performance security.

The bid security may be forfeited if:

a. Bidder withdraws or modifies its bid during the period of bid validity.
b. Successful Bidder fails to sign the Contract or fails to furnish performance security within the specified time from the date of issue of purchase order.
c. Successful Bidder fails to submit the compliance statement Annexure-XVIII within the stipulated time.

**8. Evaluation Criteria**

The bids will be evaluated in three stages:

- Stage 1 – Eligibility cum general evaluation
- Stage 2 – Technical evaluation
- Stage 3 – Commercial evaluation

Bid evaluation methodology that Indian Bank is adopting is given below:

a) 70:30 Techno-Commercial scoring model will be used for the evaluation. The total marks scored by the eligible bidders as determined by the Bank under Technical Requirements will be given 70% weightage and shall be called Weighted Technical Score (WTS). The Total Weighted Commercial Cost will be given 30% weightage and shall be called Weighted Commercial Score (WCS).

b) Scoring in the Technical Evaluation: The Bidders, who comply with Bank's eligibility criteria, mandatory technical specifications and other terms and clauses of the RFP document as explained in the bid document, will be shortlisted for technical evaluation. The bidders are expected to submit sufficient supporting details along with all documentary evidence records in their technical bid for enabling the Bank for objective evaluation and scoring in the Technical Requirements. The Bidders themselves will not fill-in any score in Technical Requirements. Evaluation and scoring process will also involve independent verification by the Bank of the details submitted in the Bid Document, including third party validations if required.

c) After scrutiny of the Technical Bid document and supporting documents, and responses to various Technical Evaluation points, scoring of marks will be done therein against bids of shortlisted bidders as explained above. The total marks in the Matrix scored by the bidder will be called Technical Score.

d) The marks obtained in Technical Evaluation will be given a weightage of 70% which will be termed as "***Weighted Technical Score***" (WTS) and shall be arrived at as under:

**Weighted Technical Score (WTS): (T/T1) * 70**

T: Technical score of the respective bidder

T1: Highest technical score of all qualified bidders

The total marks of **100** as per technical evaluation criteria will be scaled down to 70 marks as furnished below.

***For Example:*** If there are two bidders "A" and "B" who score 85 and 100 marks respectively, their "WTS" would be as under:

Bidder "A" = 85 / 100 x 70 = 59.5 marks, Bidder "B" = 100 / 100 x 70 = 70 marks

e) If sufficient numbers of bidders do not qualify the cut off score of 50 marks, Bank at its sole discretion may reduce the cut off score. Bank reserves the right to accept or reject any technical bid without assigning any reason thereof. Decision of the Bank in this regard shall be final and binding on the bidders.

f) Total marks for technical evaluation will be converted to 100 and weight will be assigned as mentioned in the evaluation method. Technical marks of the respective Bidders will be updated in GeM portal before opening of the commercial bid.

g) In the second phase of evaluation, the Commercial Bids of those bidders, whose technical bids have been short-listed and who have qualified in technical evaluation as explained above after scoring of Techno Evaluation, will be opened. After opening of Commercial Bids, commercial evaluation & verification of the commercial bids will be done by the Bank.

h) For the final evaluation, total cost of ownership (TCO) quoted by the bidder will be given 30% weightage using the formula given below as part of Techno-Commercial Evaluation Process:

**Weighted Commercial Score (WCS): (L1/C) * 30**

L1: Lowest price of all qualified bidders

C: Commercial bid of the respective bidder

Extending the example given above, in case Bidders, Bidder "A" and "B" for example quote TCO as Rs. 2,10,000 and Rs.2,00,000 respectively, then the WCS in their case would be calculated as under:

Bidder "A" = 2,00,000 / 2,10,000 x 30 = 28.57 marks

Bidder "B" = 2,00,000 / 2,00,000 x 30 = 30.00 marks

i) The total of Technical and Commercial Scores of each bidder will become basis of final ranking of bidders. Bidder whose combined weighted Technical & weighted Commercial Scores is highest will be ranked as "H1 Bidder" and bidders with second & third highest final scores will be ranked as "H2" and "H3" and so on and so forth.

**Total Score H1 = (T / T1) * 70 + (L1 / C) * 30**

**In above examples, the Total Score after Techno-Commercial evaluation (H1) of Bidders "A" and "B" will be as under:**

| Bidder | Weighted Technical Score | Weighted Commercial Score | Total Score | Rank |
|---|---|---|---|---|
| **A** | 59.5 | 28.57 | 88.07 | **H2** |
| **B** | 70 | 30 | 100 | **H1** |

j) All bids shall be evaluated by an Evaluation Committee set up for this purpose by the Bank. The evaluation shall be on the basis of technical competence and the price quoted. The re-evaluation requests will not be entertained any time once scores are finalized.

**Eligibility Criteria**

Bank is looking for eligible bidders for selecting a Vendor for the supply, installation, implementation, integration, commissioning and maintenance of hardware, software and services for Enterprise Data Privacy Governance & Compliance Platform to comply with the Digital Personal Data Protection Act, 2023 and its Rules 2025. Only those Bidders who fulfil the following criteria are eligible to respond to the RFP. Offers received from Bidders who do not fulfil any of the following eligibility criteria are liable for rejection.

Bidder shall be the single point of contact and solely responsible for the supply, installation, implementation, integration, commissioning and maintenance for the entire project. The bidder will be solely responsible for ensuring adherence to the Service Levels, terms & condition and Service Quality for each of the deliverables executed.

The Bidder needs to comply with all the eligibility criteria mentioned below to be evaluated in Eligibility bid evaluation phase. Non-compliance to any of these criteria would result in outright rejection of the Bidder's proposal.:

| Bidder Criteria | | |
|---|---|---|
| **S.No.** | **Eligibility Criteria** | **Support Document** |
| 1. | The bidder must be a registered Company (Public / Private) / PSU / PSE / Partnership Firm / LLP in India and has been in operation in India for at least 5 years as on date of publishing RFP. | Self-attested copy of Certificate of Incorporation issued by Registrar of Companies and full address of the registered office along with copies of Memorandum and Articles of Association/ Partnership Deed to be submitted along with GST registration certificate. |

| | | |
|---|---|---|
| 2. | The average annual turnover of the Bidder should be Rs.75 crore or above in last three fiscal years (2023-24, 2024-25 & 2025-26). This must be the individual company turnover (the company which is bidding) and not that of any group of companies.<br><br>Relaxation only for MSE/ Start-up:<br>The average annual turnover of the MSE/Start-up Bidder should be Rs.50 crore or above in last three fiscal years (2023-24, 2024-25 & 2025-26). | Certificate is to be provided by the chartered accountant/ statutory auditor, as per Annexure- XV.<br><br>Self-attested Copies of audited financial statements, duly certified by auditor along with the auditor's report to be enclosed.<br><br>In case of MSE, self-attested copy of Udyam Registration certificate/valid MSE certificate issued by the Ministry of Micro, Small and Medium Enterprises, Government of India also to be submitted |
| 3. | The net worth of the Bidder firm should be positive in last three fiscal years (2023-24, 2024-25 & 2025-26).<br>and<br>should not have eroded by more than 30% (thirty percent) in the last three fiscal years 2023-24, 2024-25 & 2025-26.. | Certificate is to be provided by the chartered accountant/ statutory auditor, as per Annexure- XV.<br><br>Self-attested Copies of audited financial statements duly certified by auditor along with the auditor's report to be enclosed. |
| 4. | The Bidder should have experience in supplying, implementation, integration, installation, maintenance and support of Enterprise Data Privacy & Governance Solutionduring the last 3 years till the date of release of this RFP for at least one organization in the BFSI sector / Government / PSU in India (The experience must be in the capacity of a solution implementer. Experience limited to consultancy, advisory, assessment, gap analysis, audit, or similar services shall not be considered as qualifying implementation eligibility). This must include at least the modules below:<br>1 Consent Management<br>2 Data Discovery and Classification. | The Bidder should submit documentary proof of supplying, implementation, integration, installation, maintenance, and support by providing copy of Purchase order / Contract, and work-in-progress / completion status email from client.<br>If the submitted documents do not contain sufficient details regarding the implementation, the bidder shall furnish a Credential Letter from the client on the client's official letterhead. The Credential Letter must clearly specify the scope of work, contract value, project duration, and project completion status (where applicable). The letter shall be duly signed and stamped by the client's authorized representative. Submissions not supported by the required details or a valid Credential Letter may not be considered for evaluation. |
| 5. | The bidder shall be the OEM / System Integrator / Certified or authorized agent / reseller / partner for supply of Licenses and solution implementation and maintenance support under warranty/ AMC of the proposed solution. No consortium is allowed for the scope of the RFP. | Manufacturer Authorization Form (MAF) from all the proposed OEMs needs to be submitted as the Annexure V |

| | | |
|---|---|---|
| | The bidder needs to submit the MAF from the OEM proposed components of enterprise data privacy governance & compliance platform (as mentioned in section 3 of this RFP) and the related hardware components. | |
| 6. | The bidder shall have a valid partnership with the proposed OEM as on the date of issuance of the RFP, for supply, implementation, warranty, and maintenance support of the proposed solution and related hardware. The bidder shall ensure continuation / formalization of such arrangement for minimum three (3) years from the date of go-live Order, if selected. | Proof of valid OEM partnership / authorization / reseller / channel partner certificate or agreement, along with OEM confirmation letter for continuation of the arrangement for minimum three (3) years from the date of go-live. |
| | **OEM Criteria** | |
| 8. | The proposed enterprise data privacy governance & compliance platform by OEM must have been implemented in at least one organization in the BFSI sector / Government / PSU in India within the last five (5) years as on the date of RFP release.<br>This must include at least the below modules:<br>1. Consent Management<br>2. Data Discovery and Classification<br><br>The Bank reserves the right to assess equivalence of functionalities provided under different nomenclatures. | The bidder should submit documentary proof of by providing copy of Purchase order/ Contract with Completion Certificate<br>or<br>Credential letter on client letter head providing all the details duly signed and stamped from client. |
| 9. | The hardware OEM must have successfully supplied and implemented the hardware infrastructure in any organization within the BFSI, Government, or Public Sector Undertaking (PSU) sectors in India within the last five (5) years as on the date of this RFP release.<br>Note: The hardware components need not be specific to privacy solutions. For the purpose of eligibility, the bidder may submit experience of similar hardware implementations by OEM. | The bidder should submit documentary proof by providing a copy of Purchase Order / Contract along with Completion Certificate<br>or<br>Credential letter on client letterhead providing all the details, duly signed and stamped by the client.<br><br>And<br>The OEM should submit the detailed hardware specification and sizing in the format prescribed in ANNEXURE-XXVI Proposed Hardware Description Details, duly filled and signed by the authorized signatory. |
| 10. | The proposed OEM of the enterprise data privacy governance & compliance platform must have a fully operational development | Bidder needs to submit the full details of Name, Address / Telephone Numbers |

| | | |
|---|---|---|
| | and support center in India for at least one (1) year prior to the RFP release date. | with escalation matrix and GST Number on OEM's letter head. |
| **Bidder - OEM Criteria** | | |
| 11. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017.<br>(or)<br>The Bidder and proposed OEM is from such a country and has been registered with the Competent Authority i.e., the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade, as stated under Annexure to the said Office Memorandum / Order and to submit the proof of registration herewith. | Undertaking as per Annexure-IX to be submitted by bidder as well as proposed OEM. |
| 12. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform to provide information that any of its subsidiaries or associate or holding company or companies having common director/s or companies in the same group of promoters/ management or partnership firms/ LLPs having common partners has not participated in the bid process. | Self-certified letter signed by authorized official of the Bidder and OEM on Company's letter head to be submitted. |
| 13. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform should not have been debarred/ blacklisted for corrupt and fraudulent practices by the Govt. of India / State Governments / Regulatory Agencies / PSU/other institutions at the time of submission of bid. | A Self-Declaration to be furnished by the Bidder and proposed OEM on the Company's letter head for the same as per Annexure-II. |
| 14. | Bidder and proposed OEM of the enterprise data privacy governance & compliance platform should not be insolvent, in receivership, Bankrupt, or being wound up. | Self-Declaration on Bidder's and proposed OEM's Letterhead signed by the respective authorized signatory. |

Note:

1. Attested photocopies of all relevant documents / certificates should be submitted as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. The Bank reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of the Bank in this regard shall be final, conclusive and binding upon the Bidder.

2. Either the Bidder on behalf of the Principal/ OEM or the Principal/ OEM themselves can participate in the bid, but both cannot bid simultaneously for the same solution. Any such participation shall result in the OEM's bid to be considered, other bids to be rejected.

3. A Bidder representing one OEM for enterprise data privacy governance & compliance platform cannot represent another OEM for the same solution. Any such participation shall result in rejection of both bids. However, multiple Bidders may bid with the same OEM as solution.

4. If any OEM's product/solution is proposed in this RFP, such OEM shall not participate for or be associated with any other OEM's product for the same solution.

5. The proposed enterprise data privacy governance & compliance platform, including all underlying hardware specified in the eligibility criteria, must comprehensively support the Bank in complying with the Digital Personal Data Protection (DPDP) Act, 2023, and the DPDP Rules, 2025. The solution and hardware must adhere to all applicable directions, guidelines, and advisories issued by the Government of India and relevant regulatory bodies, including MeitY (Ministry of Electronics and Information Technology), DPBI (Data Protection Board of India), RBI (Reserve Bank of India), and CERT-In (Indian Computer Emergency Response Team), as prevailing on the date of this RFP and as amended or enacted during the contract period. Furthermore, the entire ecosystem must strictly align with the Bank's internal policies, security frameworks, and operational guidelines.

6. The proposed solution must be of an equivalent or more advanced version than what has been successfully deployed by the bidder in other organization, and the deployment of any legacy or earlier versions of the software/hardware shall not be permitted.

7. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.

8. 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.

9. In the event that the Bidder fails to perform its contractual obligations, the OEM shall assume complete responsibility for providing the end-to-end solution, including technology, personnel, financial, and infrastructural support, at no additional cost to the Bank.

10. The proposed software solution must be sourced entirely from a single OEM. A hybrid or mixed architecture involving components from multiple software OEMs to meet the functional requirements will not be accepted.

**General Evaluation Criteria**

1. The Bank will examine the bid to determine that it is complete in all aspects, duly authenticated by the bidder and fulfilling the requirements stated in the bid document.

2. The bank may waive any minor informality, non-conformity, or irregularity in a bid which does not constitute a material deviation.

3. Prior to the detailed evaluation, the bank will determine the substantial responsiveness of bid documents. The quote shall conform to all the terms and conditions of the bid documents without material deviations.

4. Documents submitted with redacted or masked client name, client email ID, assignment start/end dates, or any information required to verify authenticity will not be considered for eligibility verification and will also not be considered for scoring under the Technical Evaluation Criteria.

5. Bidder to note that client email should be from official email IDs only containing their name, designation and contact number.

**Technical Evaluation Criteria**

The Bidder has been found to satisfy all the qualification criteria and presented proof as mentioned in Eligibility Criteria. The software offered should meet all the technical specifications as stipulated in the bid.

The technical bid submitted by the Bidder will be evaluated only if they fulfil the eligibility criteria.

Further, the Bidder is required to comply with all Mandatory requirements defined in the Appendix I of this RFP. Compliance with these requirements shall serve as the initial screening criterion. Any deviation from or non-compliance with a Mandatory requirement may result in disqualification from the RFP process. The Bank reserves the right to validate such compliance during the Presentation and Product Demo including Bidder’s response during Interaction (Q & A Session) and supporting evidence provided by the Bidder.

The technical bid evaluation will be done on a total score of 100. The technical evaluation will be based on the evaluation matrix consisting of the following parameters.

Bidders must secure a minimum overall technical score of 50 to be declared technically qualified.

Bank at its sole discretion, reserves the right to cancel and go for re-tendering process and the decision of the Bank in this regard shall be final.

If only one bidder qualifies, Bank, at its discretion, may choose to open the commercial bid of the only bidder who qualifies. Bank may at its discretion also reject the proposal if any of the Bidders have provided wrong information in technical / functional specifications.

During the period of evaluation, bidders may be asked to provide more details and explanations about information provided in the proposals. Bidders should respond to such requests within the time limit indicated in the letter / email seeking clarification/ explanation.

The evaluation of technical proposals, will be based on the following:

| Sl. No. | Evaluation Criteria | Scoring Criteria | Proof for Marks Allocation | Max Marks |
|---|---|---|---|---|
| 1 | **Bidder Experience:**<br>The Bidder (SI / OEM Partner) should have experience of providing Enterprise Data Privacy Governance & Compliance Platform / DPDP / GDPR tool implementation services during the last eight (8) years in an organization.<br><br>The experience shall specifically include implementation and/or deployment of enterprise data privacy governance & compliance platform covering relevant modules for at least 2 modules:<br>i. Consent and Preference Management<br>ii. Cookie Consent<br>iii. Privacy Notice Management<br>iv. Data Principal Rights Management<br>v. Personal Data Breach Management<br>vi. Data Discovery, Classification and Lineage<br>vii. Data Protection Impact Assessment<br>viii. Records of Processing Activities<br>ix. Third Party Risk Management | **Project Count-Based Scoring (Max 15 Marks):-**<br>• >5 implementations: 15 Marks<br>• 3-5 implementations: 9 Marks<br>• <3 implementations: 6 Marks | Copy of Purchase Order / Contract / Work Order<br><br>AND<br>Go-Live Certificate / Completion Certificate / Closure Sign-off document (for completed projects)<br><br>OR<br><br>Client confirmation / credential letter indicating project execution status (for ongoing projects) The bidder shall clearly indicate module coverage in the submitted documents or provide supporting client certification. | **15** |

| | | | | |
|---|---|---|---|---|
| **2** | **OEM Experience:**<br>The OEM shall demonstrate proposed enterprise data privacy governance & compliance platform / DPDP / GDPR tool having maturity, stability, and successful usage in organization.<br>The enterprise data privacy governance & compliance platform includes following modules:<br>i. Consent and Preference Management<br>ii. Cookie Consent<br>iii. Privacy Notice Management<br>iv. Data Principal Rights Management<br>v. Personal Data Breach Management<br>vi. Data Discovery, Classification and Lineage<br>vii. Data Protection Impact Assessment<br>viii. Records of Processing Activities<br>ix. Third Party Risk Management | **Module-wise Implementation Experience (Max 20 Marks):**<br>I. Consent and Preference Management – 3 Marks<br>II. Cookie Consent – 1 Mark<br>III. Privacy Notice Management – 1 Mark<br>IV. Data Principal Rights Management – 3 Marks<br>V. Personal Data Breach Management – 3 Marks<br>VI. Data Discovery, Classification and Lineage – 3 Marks<br>VII. Data Protection Impact Assessment (DPIA) – 2 Marks<br>VIII. Records of Processing Activities (ROPA) – 2 Marks<br>IX. Third Party Risk Management – 2 Marks | Proof to be submitted:<br><br>Copy of Purchase Order / Contract / Work Order<br><br>AND<br><br>Go-Live Certificate / Completion Certificate / Closure Sign-off document.<br><br>OR<br><br>Client confirmation / credential letter clearly indicating project execution status and scope of implementation.<br><br>The bidder shall ensure that the submitted documents clearly indicate the scope of work and coverage of privacy modules. In case the module coverage is not explicitly mentioned, the bidder shall provide supporting client certification. | **20** |
| **3** | **Hardware OEM Implementation Experience:**<br>The proposed hardware OEM must have successfully supplied and implemented | **Implementation count based scoring:**<br>• >5 implementations: 10 Marks | Documentary proof of Order / Contract / Work Order / Purchase Order and Go-Live / Completion / Closure | **10** |

| | | | | |
|---|---|---|---|---|
| | hardware infrastructure in any organization within the BFSI, Government, or Public Sector Undertaking (PSU) sectors in India within the last five (5) years as on the date of this RFP release.<br><br>Note: The proposed hardware components need not be specific to privacy solutions. For the purpose of bid, the bidder may submit experience of similar hardware implementations by OEM | • 3-5 implementations: 5 Marks<br>• <3 implementations: 3 Marks | Sign-off / Project completion certificate. | |
| **4** | Competency of Professionals (Project Team Capability) | **Team Competency Scoring (Max 10 Marks):**<br><br>A. Techno-Functional Privacy Skills (Max 6 Marks)<br>≥40% proposed resources certified – 6 Marks<br>≥20% and <40% proposed resources certified – 3 Marks<br><br>B. Integration & Engineering Skills (Max 4 Marks)<br>≥60% proposed resources skilled in REST APIs, JSON/XML, modern web/mobile technologies – 4 Marks<br>≥40% and <60% skilled – 2 Marks | Undertaking from the bidder on its letterhead, CVs of proposed resources, certification proofs, resource deployment plan and skill matrix in Annexure - XXV | **10** |
| **5** | Presentation and Product Demo including Bidder's response during Interaction (Q & A Session) | Bidders will be evaluated on their technical presentation and product demonstration, which must reflect a comprehensive | In-Person Technical Presentation | 45 |

| | | | | |
|---|---|---|---|---|
| | | understanding of the Bank's requirements. The evaluation will assess how closely the proposed solution and implementation roadmap align with the core objectives outlined in this RFP, specifically considering the following parameters:<br>i. In-depth understanding of the Bank's Technical and Functional requirements mentioned in the scope of work. – Maximum of 7.5 Marks<br>ii. Implementation Plan (Technical Architecture) and Proposed Team Structure for Implementation (Details of Experience & Background) – Maximum of 7.5 Marks<br>iii. Level of Compliance, Data Privacy & Security – Maximum of 15 Marks<br>iv. Solution Architecture & Business Continuity – Maximum of 7.5 Marks<br>v. Product features along with the Project | | |

| | | | | |
|---|---|---|---|---|
| | | Roadmap – Maximum of 7.5 Marks | | |
| | | | **Total** | **100** |

**Technical Evaluation**Technically qualified bidders alone will be intimated for opening of commercial bids to identify L1 bidder and the evaluation will consider the following factors:

a) The Bill of Material must be attached in Technical Bid as well as Commercial Bid. The format will be identical for both Technical Bid and Commercial Bid, except that the technical bid should not contain any price information (with Prices masked). Technical bid without price masked Bill of Materials will be liable for rejection. Any deviations from the Bill of Material / non-submission of prices in the commercial bid as per the format shall make the bid liable for rejection.

b) The optimized TCO (Total Cost of Ownership) identified in the commercial bid would be the basis of the entire outflow of the Bank for undertaking the scope of work. In case there is a variation between figure and words, the value mentioned in words will be considered.

**Presentation and Product Demo:**

Indian Bank 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.

**Note:**

1 The highest technical bidder may not automatically qualify for becoming successful bidder and for award of contract by the bank.

2 The Successful Bidder shall be the first ranked Bidder (having the highest combined score). The final decision on the successful bidder will be taken by the bank. The implementation of the project will commence upon acceptance of purchase order by the successful bidder.

3 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.

4 The bank will calculate the scores up to two decimal points only. If the third decimal point is greater than 0.005, then the same shall be scaled up else, it shall be scaled down to arrive at two decimal points.

5 The scores of the bidders based on technical evaluation will be shared / communicated to the bidders before the opening of the commercial bids.

6 Indian Bank 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

7 Documents submitted with redacted or masked client name, client email ID, assignment start/end dates, or any information required to verify authenticity will not be considered for eligibility verification and will also not be considered for scoring under the Technical Evaluation Criteria.

**Commercial Evaluation**

1 Technically qualified Bidders alone will be intimated, and their commercial bids will be opened, through which Bank will identify successful Bidder for awarding contract.
2 In the commercial bid, the bidder will be required to quote the cost as mentioned in the commercial bid format (Appendix II of Section V).
3 The bidder has to submit price break up as per commercial bid format duly signed by the authorized signatory.
4 Bank reserves the right to correct any arithmetical errors furnished in the Commercial Bid. If any such errors are noticed, it will be rectified on the following basis:
   - Bank may waive off any minor infirmity or non-conformity or irregularity in a bid, which does not constitute a material deviation at its own discretion.
   - If there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price shall be corrected accordingly. However, price quoted by bidder in GeM system will prevail over the price breakup submitted.
   - If there is discrepancy in the total arrived at (addition, subtraction, multiplication, division and carryover of amount from one page to another), correct total will be arrived by the Bank and the same will prevail over the total furnished by the bidder.
   - If there is a discrepancy between words and figures, the rate/ amount in words shall prevail, unless the amount expressed in words is related to an arithmetical error in which case, the amount in figures will prevail, subject to the above two provisions.

**Proposal Process Management**

- The Bank reserves the right to accept or reject any or all proposals received in response to the RFP without assigning any reasons thereof. Also, the Bank reserves rights to revise the RFP, to request one or more re-submissions or clarifications from one or more Bidders, or to cancel the process in part or whole without assigning any reasons.
- Additionally, Bank reserves the right to alter the requirements, in part or whole, during the RFP process, and without re-issuing the RFP. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the RFP, subsequent presentations, demos, and any other meetings during the process.

**Liabilities of the Bank**

This RFP is not an offer by Bank, but an invitation for Bidder responses. No contractual obligation on behalf of Bank whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officials of Bank and the Bidder.

**Bid and Proposal Ownership**

The Bid submitted and all supporting documentation/ templates are the sole property of Indian Bank and should NOT be redistributed, either in full or in part thereof, without the prior written consent of Bank. Violation of this would be a breach of trust and may, inter-alia causes the Bidder to be irrevocably disqualified. The proposal and all supporting documentation submitted by the Bidder shall become the property of Indian Bank and will not be returned.

## Bid Pricing Information

By submitting a signed bid, the Bidder certifies that the Bidder has arrived at the prices in its bid without agreement with any other Bidder of this RFP for the purpose of restricting competition. The prices in the bid have not been disclosed and will not be disclosed to any other Bidder of this RFP. No attempt by the Bidder, to induce any other Bidder to submit or not to submit a bid for restricting competition, has occurred.

**SECTION – III**

## CONDITIONS OF CONTRACT

### 1. Scope Overview

### 1.1 Objective & Scope

The objective of this activity is to enable enterprise data privacy governance & compliance platform in the Indian Bank's environment. The technological requirements, which include all the modules covered under this RFP for the bank to comply with the Digital Personal Data Protection (DPDP) Act, 2023 and Digital Personal Data Protection Rules 2025, while establishing scalable, auditable, and enterprise-grade privacy governance capabilities across people, processes, and technology.

The selected bidder shall supply, install, integrate, implement, harden, test, commission, and maintain all hardware, software, operating systems, databases, middleware, storage, and supporting components required for successful deployment of the proposed solution across DC, DR, Development and UAT environments.

The scope of work shall include the following:

a) **Hardware Deployment:**
End-to-end supply, installation, configuration, hardening, and support of all hardware required for implementing all the solutions specified in this RFP.
(Refer to Section 1.7 - Technical requirements)

b) **Software Deployment:**
End-to-end supply, installation, configuration, hardening, and support of all software required along with necessary licenses for implementing all the solutions specified in this RFP.
(Refer to section 1.6 - Software Deployment)

c) **Implementation Services:**
Installation, configuration, customization, and integration with the Bank's existing systems.
(Refer to section 1.6 - Software Deployment)

d) **Training and Documentation:**
Role-based training for Bank users, along with complete documentation.
(Refer to section 1.11 - Training & Knowledge Transfer, 1.5 - Key Outcomes / Deliverables across the modules and 4.4 - Documentation)

e) **Support & Maintenance:**
Comprehensive support and maintenance services for a period of 3 years post go-live, with an extension of another Two (2) years.
(Refer to section 3.2 – Post Go-live support)

The Bank invites responses to this RFP for the following modules to ensure compliance with the Digital Personal Data Protection Act 2023 and its Rules:

**Modules**

1 Consent and Preference Management
2 Cookie Consent
3 Privacy Notice Management
4 Data Principal Rights Management

5 Personal Data Breach Management
6 Data Discovery, Classification and Lineage
7 Data Protection Impact Assessment
8 Records of Processing Activities
9 Third Party Risk Management

### 1.2 Current Landscape

1 The Bank operates a large and heterogeneous application ecosystem covering customer-facing channels, transactional systems, lending platforms, KYC/AML/fraud systems, statutory/government systems, HR and internal administration platforms, risk/audit/compliance systems, document repositories, IT security tools, and analytics/MIS environments.

2 For implementation and integration purposes, the Bank's current landscape has been classified into the following application buckets: Customer Digital Channels; Core Banking & Transaction Processing; Lending, Credit & Collections; KYC, AML & Fraud Systems; Government, Subsidy & Statutory Reporting Systems; HR, Staff & Internal Administration; Risk, Audit, Compliance & Vigilance; Document, Content & Repository Systems; IT Security & Infrastructure Tools; and Analytics, MIS & Dashboards.

3 The bidder shall consider the above current landscape, application bucket coverage, and module priority while proposing the solution architecture, integration strategy, implementation plan, infrastructure sizing, and support model.

4 The Bank has executed a Perpetual Unlimited License Agreement (PULA) with Oracle, covering a comprehensive suite of database and middleware components. Usage of the below product / component for integration with non-Oracle databases or platforms is not covered under Bank's PULA.

**Oracle PULA Components Licensed by the Bank**

| S. No | Product / Component Description |
|---|---|
| 1 | Oracle Database Enterprise Edition |
| 2 | Real Application Cluster (RAC) |
| 3 | Diagnostic Pack |
| 4 | Tuning Pack |
| 5 | DB Vault |
| 6 | Data Masking and Sub setting |
| 7 | Advance Security (ASO) |
| 8 | WebLogic Suite |
| 9 | Partitioning |
| 10 | Database life cycle Management |
| 11 | Golden Gate (GG*)* |

*Supports CDC from Oracle to Oracle Data bases only.

Bidder may leverage bank's existing licenses under Oracle PULA to meet the technical and functional requirements of the data Lakehouse solution. In such case, the bidder must ensure seamless integration and compatibility of the existing licenses with the proposed solution. Bidder is responsible

for providing all the required additional tools and related support for fulfilling the scope of the project and the same shall be included in the Commercial Bid (Appendix II).
If the proposed application is based on some other Database / System software not covered in PULA of the bank, then the bidder has to provide the same with cost of such product and related support & maintenance cost built within the overall commercials bid.

### 1.3 Indicative Sizing Inputs for enterprise data privacy governance & compliance platform

The indicative sizing for the proposed enterprise data privacy governance & compliance platform is derived considering the Bank's large and heterogeneous application ecosystem spanning customer channels, core banking and transaction systems, lending platforms, KYC/AML/fraud systems, statutory and government interfaces, HR and internal administration platforms, risk and compliance systems, document repositories, IT security tools, and analytics environments.

The proposed solution shall support the Bank in meeting its data privacy and regulatory compliance obligations and shall be sized appropriately to cater to the volumes indicated below. The solution must enable integration with the Bank's ecosystem of applications, including customer digital channels, core banking systems, lending and collections applications, KYC/AML platforms, government and regulatory systems, internal administrative systems, risk and compliance solutions, document repositories, cybersecurity tools, and analytics platforms, thereby ensuring enterprise-wide privacy governance, traceability, and compliance management.

The architecture will be modular and scalable, supporting high-volume transaction processing, consent lifecycle management, and data principal rights handling across multiple systems.

| Details | Numbers (approximate) |
|---|---|
| Number of Data Principal | ~13Cr+ |
| Total Application Count | ~350+ |
| End Point Devices | ~50,000 |

1 From an infrastructure standpoint, the solution will be supported by appropriately sized compute, storage, and security components (including encryption and key management mechanisms), provisioned with adequate capacity headroom and deployed in a highly available configuration across DC and DR environments.

2 The above sizing is indicative and will be finalized during the detailed design phase in consultation with the Bank, based on actual data landscape, integration scope, application onboarding priority, and operational considerations.

### 1.4 Key Overall Business and Functional Requirements across the modules (as applicable)

The bidder shall be responsible for end-to-end supply, installation, configuration, hardening, and support of all hardware and system software required for the proposed solutions. The bidder shall clearly define ownership, warranty, support, patching, replacement, and lifecycle responsibility for each supplied component.

The bidder shall design and implement the solution across, at a minimum, Data Center (DC), Disaster Recovery (DR), Development and UAT environments. The bidder shall provide environment-wise architecture, sizing, synchronization approach, deployment dependencies, and operational control measures.

The bidder shall independently size the infrastructure required for the proposed solution based on expected users, transaction volumes, application footprint, integrations, discovery/classification scan loads, reporting workloads, storage requirements, log retention, and projected growth over the contract period.

The bidder shall ensure that capacity utilization of all supplied hardware across all environments does not exceed 70% under normal operating conditions. Any latency introduced during implementation or operations shall be measured against agreed performance baselines and shall not exceed thresholds mutually agreed between the Bank and the Bidder.

| **Performance Metric** | **Description** | **Thresholds** |
|---|---|---|
| Uptime / Availability | Percentage of time the tool is accessible to users | ≥ 99.9% uptime |
| Page Load Time | Time taken to load key screens such as dashboard, workflow forms, assessment pages | < 10 seconds for standard pages |
| System Response Time | Time taken for the system to respond after user action, e.g., submit, save, approve | < 10 seconds for normal actions |
| Bulk Upload / Import Success Rate | Success rate for importing data inventories, processing activities, users, vendors, or assets | ≥ 95% successful uploads |
| API Response Time | Time taken for integration calls for the platform to respond | <7 seconds per API call |
| Report Generation Time | Time taken to generate dashboards, compliance reports, RoPA exports, DSR status reports | < 1 minute for standard reports |

Any exceedance shall require immediate remediation by the bidder at no additional cost to the Bank.

1. The solution shall ensure continued compliance with the DPDP Act, related Rules, and all applicable directions/advisories issued by MeitY, DPBI, RBI, and CERT-In, as prevailing on date and as amended during the contract period, along with adherence to the Bank's policies and guidelines

2. The bidder shall be responsible for end-to-end supply, installation, configuration, hardening, and support of all hardware and system software required for the proposed solutions. The bidder shall clearly define ownership, warranty, support, patching, replacement, and lifecycle responsibility for each supplied component.

3. The bidder shall design and implement the solution across, at a minimum, Data Center (DC), Disaster Recovery (DR), Development and UAT environments. The bidder shall provide

environment-wise architectThe solution shall be deployed on an on-premises model within the Bank's Data Centre (DC) and Disaster Recovery (DR) environments.

4. The bidder shall be responsible for installation, configuration, and deployment of the solution.

5. The Service Provider shall include all required software licensing, annual technical support, maintenance, documentation, and contracted on site/off site resources.

6. The solution shall integrate with Bank-designated systems and platforms relevant to in-scope modules. The scope shall typically include systems such as Core Banking System (CBS), Digital Channels (Internet Banking, Mobile Banking, UPI, DLP), ATM, Customer Relationship Management (CRM), Data Lake, Call Centre Systems, Treasury Systems, Inhouse Applications and third-party fintech applications identified during the gap assessment. However, the integration scope shall not be limited to the listed systems, and the bidder shall support integration with any additional systems as identified during the course of implementation~~,~~ using secure APIs/connectors, and shall preserve data security, availability, and operational continuity.

7. The bidder shall support a repeatable integration onboarding approach suitable for enterprise scale, including standardized onboarding artefacts, mapping, testing/certification approach, and rollback planning.

8. The bidder shall support the Bank in establishing and operationalizing a model for the solution across all in-scope modules, aligned to Bank functions and processing activities.

9. The solution shall support definition and assignment of granular roles and responsibilities (RACI) with role-based access controls (RBAC) and segregation of duties (SOD).

10. The solution shall support risk scoring and risk tiering models where applicable.

11. The solution shall support with Dashboards and reporting capabilities.

12. The solution shall support Bank-defined escalation paths and approvals, including time-bound escalations for SLA breaches and exception handling.

13. The solution shall enable evidence-based responses to audits, supervisory reviews, and regulatory inquiries through standardized exports, consistent logs, and regulator-ready reporting.

14. The solution shall demonstrate capacity to sustain expected and peak transaction volumes without performance degradation, including during integration onboarding and controlled releases.

15. Bidder shall support in migration to DR site during scheduled/unscheduled DR drills and Switch Bank from DR to DC Site

### 1.5 Key Outcomes / Deliverables across the modules (as applicable)

1 Environment-wise hardware architecture and Bill of Materials, including server, storage, operating system, database, middleware, virtualization, backup, and redundancy details.

2 Hardware installation and commissioning evidence for all environments.

3 OEM warranty/support documents, lifecycle support declarations, and replacement/escalation matrix.

4 Performance validation evidence for supplied hardware including CPU, memory, storage, throughput, and failover behaviour.

5 High-Level Design (HLD) and Low-Level Design (LLD) covering architecture, components, and module-specific workflows.

6 Configuration Evidence for implemented modules (configured components, admin consoles, rules/workflows/templates as applicable).

7 Integration Specifications & Interface Documentation (APIs/SDKs/webhooks/connectors), including mapping, error handling, and security approach for Bank-designated systems.

8 Dashboards & Standard Reports for operational and compliance monitoring (including but not limited to module posture/status/coverage/ageing/SLAs/exceptions) with export in Bank-approved formats.

9 Tamper-evident / Immutable Audit Logs configuration and sample extracts covering key events (administrative changes, workflow actions, exports, lifecycle events) suitable for audit/forensics.

10 Testing Artefacts and Execution Evidence (UAT) includes functional and negative scenarios relevant to each module, plus evidence verification.

11 Performance validation evidence for Bank-defined workloads where applicable (e.g., scan throughput, API latency, workflow throughput, propagation windows).

12 Operational runbooks for BAU operations (administration, monitoring, exception handling, evidence extraction, troubleshooting).

13 Training, Knowledge Transfer & BAU/Handover Pack (training materials, KT sessions, hyper care and steady-state transition documentation).

## 1.6 Software Deployment

### 1.6.1 Consent and Preference Management

#### 1.6.1.1 Detailed Requirements

**Scope**

a. The bidder shall provide an enterprise Consent & Preference Management capability for the Bank.
b. The capability shall enforce purpose limitation and maintain audit-ready proof for all consent actions.
c. The solution shall ensure continued compliance with the DPDP Act, applicable Rules, and all directions, advisories, and guidelines issued by MeitY, DPBI, RBI, CERT-In, and other applicable authorities, as prevailing on date and as amended during the contract period.

d. The solution shall support interoperability with DPBI-registered Consent Managers and any other consent ecosystem as mandated by regulatory authorities.
e. The solution shall expose consent records, notice versions, acknowledgements, withdrawal status, and related artefacts in machine-readable formats through secure APIs, in Bank-approved schemas.
f. The bidder shall support migration/export/import of consent records, notice acknowledgements, audit trails, and artefacts in the event of change of consent manager, replacement of the solution, or regulatory portability requirements, without loss of integrity, version history, or evidence traceability.

**Coverage**

a. The capability shall support customer journeys across Bank digital and non-digital channels (self-service and assisted).
b. The capability shall support customers, employees/candidates, and vendors/contractors using Bank-approved identity anchors.
c. The capability shall support extended relationships where applicable (nominee/authorized signatory/representative).
d. The capability shall support enterprise-wide coverage across all Bank channels including but not limited to Internet Banking, Mobile Banking, Branch operations, Call Center operations, Salesforce CRM systems, marketing platforms, and downstream applications.
e. Data Lake has been identified as a future-state requirement and is planned for inclusion in the next 2-year roadmap phase.

**Consent Model**

a. Consent shall be captured at purpose and sub-purpose level.
b. The solution shall support lawful basis tagging for processing not based on explicit consent.
c. The solution shall prohibit pre-ticked options and bundled consent for unrelated purposes.

**Identifiers**

a. Customer consent shall be anchored to CIF and/or other identifiers (e.g., email/phone/account number) as approved by the Bank.
b. The bidder shall implement a single canonical consent payload/data model across applications.
c. The canonical model shall include purpose/sub-purpose IDs, data categories, lawful basis tag, version/validity, timestamp, channel/source, authentication reference, and integrity fields.

**Consent Lifecycle**

a. The solution shall support, capture, validate, update, renew/revalidate, expire, and withdraw of consent.
b. Withdrawal shall be available via self-service and assisted channels and shall be as easy as it was given.
c. Withdrawal of one purpose shall not revoke other purposes unless explicitly requested or required by law/Bank policy.
d. The solution shall support renewal schedules and expiry rules configured by the Bank.

e. The solution shall notify renewal/expiry events via Bank-approved channels and retain delivery/outcome evidence.
f. The solution shall support digitization of offline consent captured through physical forms or assisted channels, including storage of consent artefacts and audit trail of digitization.
g. The solution shall support cohort-based bulk re-notification, re-confirmation, and re-consent campaigns where consent is absent, expired, invalid, withdrawn, not demonstrably compliant, or where a material change in purpose, sub-purpose, lawful basis, consent text, notice version, or Bank policy requires renewed consent. The solution shall retain delivery, acknowledgement, response, and remediation evidence in Bank-approved formats.

**Enforcement and Stop-Processing**

a. The solution shall ensure that processing dependent on withdrawn, expired, or invalid consent is automatically blocked/restricted without manual intervention.
b. All in-scope applications/pipelines shall validate consent via centralized APIs/SDKs.
c. Any bypass attempt shall generate alerts and immutable audit records.

**Consent State Transmission and Fail-safe**

a. The solution shall ensure real-time propagation of consent updates across integrated systems within a Bank-defined SLA, and the bidder shall propose and adhere to such propagation timelines.
b. The solution shall support both real-time pathways and batch pathways for consent state transmission within Bank-approved compliance windows, where applicable.
c. In scenarios where consent validation is temporarily unavailable, the solution should provide configurable controls to restrict or defer processing, unless explicitly permitted under approved policy exceptions with appropriate logging.

**Third-party Sharing**

a. Consent validation shall be enforced before sharing personal data with third parties in scope.
b. The solution shall support logging of third-party sharing and retain evidence of withdrawal notifications where required by contract/Bank policy.

**Language and Accessibility**

a. Consent journeys shall support English and Eighth Schedule languages, with controlled translation parity.
b. Consent UX shall not use dark patterns; withdrawal shall not be harder than grant. Solution must provide a withdrawal mechanism that matches the simplicity of original consent capture journey.
c. The solution shall support verifiable parental/guardian consent for minors where required.

d. The solution shall support explicit policy controls to prohibit behaviour monitoring, targeted advertising, profiling, or any equivalent tracking activity in relation to minors and any other restricted categories as defined by applicable law, regulatory guidance, or Bank policy.

**Security and Session Controls**

a. The solution shall comply with Bank security standards. (authentication, authorization, encryption, key management etc.).
b. Step-up authentication shall apply for high-impact actions (withdrawals with consequence, preference changes, artefact downloads).
c. Sessions shall follow Bank timeout and session invalidation policies.

**Evidence and Audit**

a. The solution shall support generation of a consolidated, tamper-evident, non-repudiable evidence artefact for each consent event or lifecycle state change, suitable for legal, audit, and regulatory purposes, in Bank-approved human-readable and machine-readable formats.
b. Evidence shall include at minimum: timestamp, policy/version reference, categories selected, channel/context, and a reference identifier.

**Reporting, Monitoring, and Dashboard**

a. The solution shall provide dashboards for monitoring consent-related activities including consent grants, withdrawals, renewals, and expiries.
b. The solution shall support channel-wise analytics of consent capture across digital and non-digital channels.
c. The solution shall support purpose-wise coverage reporting and identification of gaps in consent coverage.

**Regulatory Updates**

a. The bidder shall provide periodic regulatory updates, product enhancements, and compliance patches required to ensure continued alignment with evolving DPDP regulatory requirements.

#### 1.6.1.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply in addition to the module-specific requirements.

**Legacy Consent Remediation**

a. The solution shall support re-collection or re-confirmation, or migration of legacy consents where existing consents are not demonstrably DPDP compliant.
b. The solution shall support co-hosting and audit-ready reporting of remediation outcomes.

#### 1.6.1.3 Deliverables / Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

a. Configured purpose taxonomy and consent templates.
b. Audit-ready consent logs and consent receipts/artefacts

### 1.6.2 Cookie Consent

#### 1.6.2.1 Detailed Requirements

**Scope**

a. The solution shall manage consent for tracking technologies on Bank web properties and mobile apps, including cookies, tags, scripts, SDKs, pixels, and telemetry
b. The solution shall support both first-party and third-party trackers.

**Consent Model**

a. The solution shall support category-based choices at minimum: Essential, Functional, Performance, Analytics, Marketing.
b. Non-essential trackers shall be blocked by default until explicit consent is captured for the applicable category
c. Essential category definition shall be Bank-controlled.

**Banner and Preference Center**

a. The solution shall display a cookie banner on first visit and when consent expires or is invalidated.
b. The banner shall provide Accept All and Reject All with equal ease and comparable prominence.
c. The solution shall provide a persistent preference center link to update/withdraw cookie preferences at any time.
d. Preference changes shall take effect on the next eligible page load / API call / app event / request and prevent further placement of blocked trackers.

**Discovery and Inventory**

a. The solution shall discover and inventory trackers on Bank web properties through automated scanning (domains/subdomains/pages as configured).
b. The solution shall detect tracker changes over time and highlight deltas (new/removed/changed).

**Categorization and Overrides**

a. The solution shall auto-categorize discovered trackers into Bank-defined categories.
b. The solution shall allow controlled overrides (re-categorize/approve/block) with RBAC and full audit logs.

**Mobile App Trackers**

a. The solution shall support mobile tracking discovery using Bank-approved methods (SDK inventory, dependency/config review, telemetry/network review).
b. Mobile trackers shall be mapped to the same consent categories and enforcement rules as web.

**Cookie Policy**

a. The solution shall generate/maintain a Cookie Policy page.
b. Cookie Policy shall include at minimum: categories, purposes, duration/expiry, third-party recipients, and user controls.

**Expiry and Re-consent**

a. Cookie consent shall expire as per Bank policy.
b. On expiry, the banner shall reappear, and non-essential tracking shall remain blocked until consent is renewed.

**Evidence and Audit**

a. The solution shall generate tamper-evident records for cookie consent actions and changes.
b. Evidence shall include at minimum: timestamp, policy/version reference, categories selected, channel/context, and a reference identifier.
c. Evidence and logs shall be exportable in Bank-approved formats.
d. The solution shall maintain version history of cookie banners, preference center configurations, and cookie policies.
e. The solution shall enable reconstruction of the exact content, categories, configuration, and user interface presented to the user at the time of consent for audit and legal purposes.

**Language and UX Controls**

a. Banner and preference center shall support English and Eighth Schedule languages (translation governed by Bank).
b. The UX shall not use dark patterns; reject/withdraw shall not be harder than accept.

#### 1.6.2.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply in addition to the module-specific requirements.

**Governance and Control**

a. Bank admins shall be able to configure categories, banner templates, text, languages, and default blocking rules.
b. The solution shall support maker–checker approvals for policy/template changes where required by Bank governance.

**Monitoring**

a. The solution shall provide dashboards for consent posture, tracker inventory status, scan health, and exceptions.
b. The solution shall support alerts for newly detected trackers and unauthorized/uncategorized trackers.

#### 1.6.2.3 Deliverables / Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

a. Configured banner + preference center + prior blocking rules.
b. Configured web scanning + tracker/third party inventory + categorization/ override workflow.
c. Configured mobile tracker discovery approach and mapping to categories.
d. Cookie Policy page aligned to live inventory + exportable evidence records.

### 1.6.3 Privacy Notice Management

#### 1.6.3.1 Detailed Requirements

**Notice Authoring and Rendering**

a. The solution shall support notice templates that can be rendered by product, journey, purpose, population, and locale.
b. Notices shall be rendered via embed methods suitable for Bank channels (web/mobile).
c. The solution shall support layered privacy notices, including short notices with links to detailed notices, based on context, stage of user journey, and sensitivity of data being processed.

**Mandatory Notice Content**

a. Notices shall include at minimum: purpose(s), data categories, retention reference, lawful basis (where applicable), withdrawal instructions, grievance/contact details, and recipient categories where applicable.
b. Notice text shall be Bank-configurable.

**Versioning**

a. The solution shall store the exact notice version presented and acknowledged.
b. The solution shall bind the acknowledged notice version to the related consent record(s) where consent is captured.
c. The solution shall maintain version history with effective date, retirement date, approver, and change rationale.
d. Historical versions shall remain retrievable for audit and dispute resolution.

**Acknowledgement and Receipts**

a. The solution shall capture acknowledgement with identity reference, notice ID/version, timestamp, channel, locale, and session/transaction reference.
b. The solution shall generate acknowledgement artefacts/receipts in Bank-approved formats.
c. Receipts shall include at minimum: notice version, timestamp, channel, locale, and withdrawal guidance.
d. The solution shall capture whether the privacy notice has been viewed prior to acknowledgement and maintain such records for audit purposes.

e. The solution shall automatically trigger re-presentation of updated privacy notices where a Data Principal has previously consented based on an outdated notice version and shall require acknowledgement prior to further processing where applicable.

**Publishing**

a. Notice authoring and publishing shall be controlled with RBAC.
b. The solution shall support maker–checker approval and scheduled go-live.
c. The solution shall maintain complete logs of authoring, approval, publish, and rollback actions.

**Language**

a. Notices shall support English and Eighth Schedule languages.
b. Translation governance shall ensure parity of meaning across languages (Bank-controlled).
c. Notices shall not use deceptive/dark patterns.

**APIs / SDKs**

a. The solution shall expose APIs/SDKs to fetch the latest effective notice by product/ journey/ purpose/ language.
b. The solution shall expose APIs to post acknowledgement and retrieve acknowledgement/ receipt artefacts.

**Evidence and Audit**

a. The solution shall maintain tamper-evident logs for notice versioning, publishing, acknowledgements, and receipt exports.
b. Evidence shall be exportable in Bank-approved formats.

#### 1.6.3.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply in addition to the module-specific requirements.

**Governance and Operational Controls**

a. Bank admins shall be able to govern templates, languages, publication workflow, and approval thresholds.
b. The solution shall provide dashboards for notice coverage, active versions, acknowledgements, and exceptions.

#### 1.6.3.3 Deliverables / Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

a. Configured notice templates + rendering for Bank channels.
b. Configured versioning repository.
c. Configured acknowledgement capture + receipts/artefacts + exportable evidence.

### 1.6.4 Data Principal Rights Management

#### 1.6.4.1 Detailed Requirements

**Scope**

a. The bidder shall operationalize an enterprise-grade Data Principal Rights Management capability to enable the Bank to receive, authenticate, process, fulfil, and close Data Principal rights requests in compliance with the Digital Personal Data Protection (DPDP) Act, applicable DPDP Rules, and the Bank's internal policies.
b. The DPRM capability shall support end-to-end lifecycle management of data principal rights requests, including intake, identity verification, validation, fulfilment, communication, grievance handling, and closure, with complete traceability and immutable auditability across all stages. The solution shall enable demonstrable accountability, transparency, and regulator-ready evidence for all Data Principal rights handling activities.
c. The solution shall enable Data Principals to exercise their rights including access, correction, completion, update, erasure, grievance redressal, and nomination, in accordance with applicable data protection regulations, with end-to-end workflow support, traceability, and auditability. The request intake and modification interfaces shall clearly capture and display the request type to ensure appropriate validation, processing, and tracking across the request lifecycle.

**Request Handling:**

a. The solution shall enable Data Principals to exercise all statutory rights under the DPDP Act, including but not limited to:
    - Right to access personal data
    - Right to correction, update, and erasure of personal data, subject to applicable lawful retention obligations
    - Right to grievance redressal
    - Right to nominate an individual to exercise rights in the event of death or incapacity

b. The solution shall provide a secure, user-friendly interface enabling Data Principals to:
    - View active and historical consents
    - Submit and track rights requests
    - Download response artefacts and request status updates
    - Manage nomination lifecycle activities including capture, validation, modification, revocation, and execution

c. The solution shall ensure clear, transparent, and timely communication with Data Principals across the entire request lifecycle.

**Workflow and SLA Management**

a. The solution shall enable workflows to automate rights request handling, including but not limited to:
    - Intake, acknowledgment, validation, approval, fulfilment, and closure
    - Embedded identity verification prior to execution of any sensitive action

- Maker–checker and multi-level approval controls for high-risk actions such as erasure or bulk disclosures
- Self-service consent viewing and revocation capabilities to reduce manual intervention

b. Workflow configuration shall support Bank-defined SLAs, escalation paths, approval thresholds, and exception handling mechanisms.

c. The solution shall orchestrate multi-channel notifications, including digital and assisted channels, as approved by the Bank.

d. The solution shall enforce statutory timelines for Data Principal Rights requests as per applicable DPDP Rules and generate alerts and escalation triggers for potential SLA breaches or delays.

e. The solution shall support bulk processing of Data Principal rights requests with appropriate workflow controls, approvals, and audit trails.

f. Solution shall notify the data principals at least 48 hours prior to the deletion of their personal data, when the retention period is expiring.

**Multi-Channel and Assisted Request**

a. The DPRM capability shall support Data Principal rights requests initiated through multiple channels, including but not limited to:
   - Web and mobile digital channels
   - Branch and field-level assisted interactions
   - Agent-led or call-center-assisted service channels

b. The solution shall support notification of workflow status to Data Principals through Bank-approved channels including SMS, email, and other messaging platforms such as WhatsApp where applicable.

c. The solution shall support additional assisted and semi-digital channels including ATM/Kiosk, IVR-based interactions, and SMS-based request initiation where applicable.

d. All assisted handling actions shall be subject to maker–checker controls, role-based access, and tamper-proof logging.

e. The bidder shall support workflow simulation across digital and assisted channels to identify potential data exposure risks and enable mitigation prior to production rollout.

**Identity Verification**

a. The solution shall embed identity verification and security controls across the rights management lifecycle, including:
   - Identity verification prior to processing access, correction, erasure, nomination, or grievance actions, using Data Principal identifiers (such as email, phone, account ID, employee ID, customer ID, or any other verified identifier)
   - Step-up authentication prior to data export, download, or irreversible actions
   - Session timeout and session invalidation controls
   - Role-based access control (RBAC) and segregation of duties for operators and reviewers

b. All identity verification, authentication failures, and security-relevant events shall be logged in immutable audit logs and retained as per Bank policy.

**Data identification and Third-Party Coordination**

a. The solution shall integrate with Bank systems and repositories to enable accurate and complete fulfilment of Data Principal rights, including:
   - Identification of systems of record and downstream systems
   - Automated or assisted collation of relevant personal data for access requests
   - Orchestration of correction, update, or erasure actions across internal systems and third-party Data Processors
   - Verification of applicable consent and lawful basis prior to fulfilment

   For access requests, fulfilment responses shall include required contextual disclosures such as:
   - Purpose(s) of processing
   - Categories of personal data
   - Data recipients or sharing context
   - Retention or deletion context, where applicable

**Grievance Redressal**

a. The solution shall provide a centralized grievance redressal mechanism for privacy-related complaints, including receipt, acknowledgment, investigation, resolution, and closure.
b. The grievance module shall enforce statutory and Bank-defined timelines and escalation workflows.
c. The solution shall support generation of evidence packages and structured responses required for submission to the Data Protection Board of India, where applicable.
d. Complete records of grievances, communications, decisions, and resolutions shall be retained in an audit-ready form.

**Tracking, Reporting, and Auditability**

a. The solution shall maintain a centralized DPRM registry capturing all rights requests, actions taken, responses issued, approvals, and timelines.
b. The solution shall maintain tamper-proof logs of all DPRM activities to support audits and investigations.

#### 1.6.4.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply.

#### 1.6.4.3 Deliverables/Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

**Architecture Deliverables**

a. End-to-end rights management and grievance workflows.
b. Identity verification and security control designs.
c. SLA, escalation, exception, and approval models.

**Configured DPRM Platform and Workflows**

a. Production-ready DPRM portals for Data Principals and operators.
b. Configured workflows for access, correction, erasure, consent withdrawal, grievances, and nomination.
c. Bank-approved response templates and communication orchestration.

**Integration and Fulfilment Artefacts**

a. System integration mappings and interface specifications.
b. Evidence of fulfilment across internal systems and Data Processors.
c. End-to-end logging and traceability artefacts.

**Reporting and Audit Evidence Package**

a. Centralized operational and compliance dashboards.
b. DPDP-aligned and DPBI-ready evidence packs.
c. Immutable audit logs capturing all DPRM activities.

**Testing, Training, and BAU Handover**

a. User Acceptance Testing (UAT) scenarios and execution evidence.
b. Operational runbooks and standard operating procedures (SOPs).
c. Role-based training, knowledge transfer, and BAU handover documentation.

### 1.6.5 Personal Data Breach Management

#### 1.6.5.1 Detailed Requirements

**Scope**

a. The bidder shall implement a solution for personal data breach management, and reporting in line with the requirements of the Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025.
b. The solution shall adhere to a robust breach management framework that enables timely detection, assessment, reporting, and mitigation of personal data breaches.

**Integration**

a. The selected bidder shall integrate with all in-scope systems to enable effective breach monitoring, escalation, and regulatory reporting.
b. The solution shall include breach management coverage across on-premises, cloud, and hybrid environments, including third-party service providers where the Bank's personal data is processed or stored.
c. The solution shall support integration with the Bank's security and incident ecosystem to enable centralized monitoring and orchestrated response, including but not limited to SIEM, SOAR, DLP, IDS/IPS, UEBA, the Bank's incident/ticketing system, and anomaly detection tools.

**Breach Indicators and Monitoring**

a. The solution shall define and maintain breach indicators for unauthorized access, exfiltration, modification, or misuse of personal data.

**Incident Logging and Evidence**

a. The solution shall maintain tamper-proof logs of all security events affecting personal data, including detection triggers, correlation results, investigation actions, and outcome decisions.
b. The solution shall maintain a structured evidence collection process to support, including but not limited to, internal investigations, legal proceedings, and regulatory inquiries.
c. The solution shall maintain records of all reported breaches for audit and compliance verification, including investigation notes, timelines, decisions, notification evidence, and closure approvals.

**Breach Assessment and Risk Thresholds**

a. The solution shall classify breaches based on severity, type of data compromised, number of Data Principals affected, and potential impact.
b. The solution shall define and operationalize risk-based thresholds for breach reporting to the Data Protection Board of India (DPBI), aligned to Bank-approved criteria and regulatory requirements.
c. The solution shall support structured impact assessment to determine the nature and extent of harm, whether notifications are required, and what mitigation actions shall be recommended.
d. The solution shall leverage end-to-end data lineage and relationship mapping to accurately identify impacted systems, datasets, data principals, and downstream data flows in the event of a breach, enabling precise impact assessment and regulatory notification.

**Notifications**

a. The solution shall maintain a repository of pre-approved templates to support timely and compliant breach reporting and communications.
b. The solution shall send reports to impacted Data Principals and to the Data Protection Board of India, as required by DPDP and Bank policy.
c. The solution shall create cohorts of Data Principals to ensure notifications are issued only to affected Data Principals based on investigation outcomes and confirmed impact scope.
d. The solution shall notify affected Data Principals promptly and shall ensure notices include, at minimum, the nature of the breach, the type of personal data compromised, mitigation steps taken, and recommended actions to prevent harm.
e. The solution shall enable automated cohorting based on breach investigation data, including mapping of impacted records and affected populations as evidence evolves during investigation.
f. The solution shall support bulk generation and dispatch of breach notices across Bank-approved channels including but not limited to email, SMS, and in-app notifications, using templated content that includes required breach details and remediation guidance.
g. The solution shall expose dashboards showing which Data Principals were notified, delivery status, bounce/failure handling, and re-notification actions where needed, including audit-ready evidence of dispatch and outcomes.

h. The solution shall track and enforce regulatory breach notification timelines in accordance with applicable laws (including DPDPA), ensuring timely notification to the Data Protection Board of India (DPBI) and affected Data Principals.
i. The solution shall provide a real-time dashboard showing elapsed time since breach detection, breach confirmation, internal escalation, regulator notification, and Data Principal notification, against Bank-defined and regulatory timelines, with alerts for approaching or breached thresholds. The solution shall provide real-time alerts, escalation workflows, and dashboards for potential delays or non-compliance.

**Response and Recovery**

a. The solution shall define standard operating procedures (SOPs) for breach response planning, notification, reporting, and impact mitigation, and shall align breach management workflows to the defined SOPs.
b. The solution shall support post-breach review to identify gaps, update playbooks, and document corrective and preventive actions.
c. The solution shall support periodic breach simulation exercises (e.g., tabletop or automated simulations) to validate breach detection, response workflows, and regulatory reporting readiness, with documented outcomes, metrics, and audit trails.

**Regulatory and Standards Alignment**

a. The solution shall ensure breach management is aligned not only to DPDP requirements but also to other applicable regulatory and standards requirements, including but not limited to RBI, CERT-In, SEBI, IRDAI, ISO 27001, and NIST frameworks and other laws of the land as applicable to the Bank's operations.
b. Where multiple reporting obligations apply, the solution shall support consistent evidence capture, timeline tracking, and reporting artefacts aligned to Bank policy and regulator expectations.

### 1.6.5.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply in addition to the module-specific requirements.

**Third-Party Coverage**

a. The breach management process shall include personal data processed by third parties and service providers in scope, including mechanisms to ingest alerts, track third-party incidents affecting Bank data, and evidence third-party communications and remediation actions, as required by contract and Bank policy.

### 1.6.5.3 Deliverables / Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

**Solution Design and Documentation**

a. Breach indicator library (e.g. unusual access to customer data) and detection scenario catalogue aligned to Bank systems and data flows.

b. SOP package for breach response plan, escalation, investigation, evidence handling, notification, regulator reporting, containment, recovery, and post-incident review.
c. Integration specifications and implementation evidence for SIEM, SOAR, DLP, IDS/IPS, UEBA, incident/ticketing systems, anomaly detection tools, and other Bank-designated sources.
d. Tamper-proof logging configuration and evidence retention approach.

**Notification and Reporting**

a. Pre-approved template repository for breach notifications and reports.
b. Cohorting capability configuration and evidence of targeted notification controls.
c. Dashboards and reporting for notifications and regulatory submissions

**Testing, Exercises, and Readiness**

a. Tabletop exercise plan, scenarios, and execution evidence.
b. Red team assessment support artefacts and improvement tracking mechanism.
c. Post-incident review template and corrective action tracking mechanism.

**Training and Knowledge Transfer**

a. Training plan, training materials, and training completion evidence for employees.
b. Awareness communication templates and governance approach for customer/data principal communications on a need basis.

### 1.6.6 Data Discovery, Classification and Lineage

#### 1.6.6.1 Detailed Requirements

**Scope and Compliance**

a. The bidder shall implement an enterprise-grade capability to discover, classify, and trace (lineage) personal data across the Bank's in-scope technology landscape.
b. The solution shall support the Bank's initial scope of ~400+ applications and scale further as defined by the Bank.
c. The solution shall support coverage across on-prem DC/DR, private cloud, and public cloud environments as applicable.
d. The solution shall align to DPDP Act, DPDP Rules, RBI expectations, and other laws of the land as applicable to the Bank's operations, with audit-ready evidence.
e. The solution shall support linkage of Data Discovery, Classification, and Lineage with Consent and Preference Management, DPIA and ROPA modules to enable consistent processing activity references, risk visibility, and evidence traceability

**Discovery Coverage**

a. The solution shall support discovery across Bank-defined in-scope platforms, including at minimum:
   - Relational databases and data warehouses
   - Data lakes and analytics platforms
   - File shares and unstructured repositories

- Email and collaboration systems
- End-user endpoints
- SaaS platforms and cloud object storage

b. The solution shall support full scans and incremental/differential scans based on change detection, metadata, or Bank-defined schedules.
c. The solution shall support scheduled scans with throttling/window controls to meet Bank performance constraints.
d. The solution shall automatically detect new objects within onboarded sources (e.g., schemas/tables/folders/repos) on the next scan cycle.
e. The solution shall capture scan status, timestamps, failures/exceptions, and remediation notes for audit evidence.
f. The solution shall include configurable performance safeguards for data discovery scans, ensuring that scanning activities do not exceed defined thresholds (e.g., CPU, memory, I/O utilization) on source systems during business hours, with the ability to schedule or throttle scans dynamically.
g. The solution shall support masking, tokenization, or redaction of sensitive data within scan results, logs, and user interfaces to prevent unnecessary exposure of personal or confidential data, with role-based access controls governing visibility.

**Classification**

a. The solution shall support rule-based and context-based classification for personal data detection.
b. The solution shall support custom classifiers defined by the Bank (patterns, dictionaries, rules).
c. The solution shall classify data into personal vs non-personal, and further into Bank-defined categories (PII/high-risk types).
d. The solution shall detect India-specific identifiers, including at minimum: Aadhaar, PAN, UAN, Passport, Voter ID, Driving License, Account/Customer IDs, transaction/loan identifiers, and KYC artefacts, including historical formats where applicable.
e. The solution shall provide tuning controls to manage false positives/false negatives and retain tuning evidence (before/after outcomes).

**Labels and Overrides**

a. The solution shall support applying classification labels/metadata at Bank-defined trigger points where supported (create/save/share/upload/download/modify).
b. Where technically feasible, labels/metadata shall remain intact across movement/replication/backup/sharing/archival.
c. The solution shall support role-based overrides for classification changes with mandatory justification and audit logging.

**Lineage Scope**

a. The solution shall provide lineage for Bank-defined in-scope sources to evidence: origin → movement → consumption, including third-party/processor touchpoints where personal data is stored or shared.

#### 1.6.6.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply.

#### 1.6.6.3 Deliverables / Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

a. Onboarded discovery and classification coverage across Bank-prioritized in-scope sources.
b. Configured classifier library (default + Bank custom classifiers), labels, and tuning controls, with tuning evidence.
c. Configured scan schedules
d. Dashboards for scan coverage/health
e. Configured lineage capture

### 1.6.7 Data Protection Impact Assessment

#### 1.6.7.1 Detailed Requirements

**Scope and Alignment**

a. The bidder shall implement an enterprise-wide Data Protection Impact Assessment capability to enable structured identification, assessment, approval, mitigation, and monitoring of privacy risks arising from the processing of personal data.
b. The DPIA capability shall align with the Digital Personal Data Protection (DPDP) Act, applicable DPDP Rules, RBI expectations, and other laws of the land as applicable to the Bank's operations and the Bank's internal privacy, risk, and governance policies.
c. The solution shall support complete end-to-end DPIA lifecycle management, including initiation, assessment, collaboration, approvals, mitigation tracking, reporting, periodic review, and reassessment, with full traceability and auditability.
d. The solution shall support linkage of DPIA with RoPA records and Data Discovery to enable consistent processing activity references, risk visibility, and evidence traceability.
e. The solution shall support integration with the Bank's enterprise risk management systems to align privacy risks identified in DPIA with overall operational and risk registers.

**DPIA Templates and Assessment**

a. The solution shall provide standardized DPIA templates aligned to requirements for SDF as per DPDPA and questionnaires including but not limited to
   - Description of processing activities, including systems, data categories, involvement of third parties, nature, scope, context, purposes of processing
   - Assessment of necessity and proportionality
   - Identification and analysis of privacy and data protection risks
   - Risk categorization and risk scoring based on Bank-defined criteria
   - Identification of mitigation measures, controls, and safeguards
   - Residual risk assessment and recommendation for approval or escalation

b. DPIA templates shall be aligned with DPDP Act requirements and regulatory expectations and shall be configurable for different business units, products, processes, risk levels, and regulatory or industry-specific contexts.

**Automated DPIA Triggering and Risk-Based Initiation**

a. The solution shall support automated initiation of DPIAs based on Bank-defined trigger events, including but not limited to:
   - Introduction of new personal data categories
   - Launch, modification, or decommissioning of applications or business processes
   - Onboarding or change of third-party vendors or data processors
   - Initiation of cross-border data transfers
   - Introduction of new technologies, analytics, automation, profiling, or AI use cases

b. The solution shall generate configurable risk scores and automatically route DPIAs through appropriate review and approval workflows based on Bank-defined risk thresholds and criticality.

**Workflow Automation and Governance Controls**

a. The solution shall support configurable, tool-based workflows enabling:
   - Role-based access, permissions, and task assignments
   - Multi-level review and approval hierarchies aligned to Bank governance
   - Automated reminders, escalations, and SLA tracking
   - Upload, versioning, and retention of supporting evidence and artefacts
   - Immutable audit trails capturing every user action, comment, decision, and approval

**Assisted and Context-Aware DPIA Execution**

a. The solution shall support assisted DPIA execution by auto-populating assessment fields using available contextual information, including but not limited to:
   - Prior DPIAs and similar processing assessments
   - Data mapping and data flow artefacts
   - Consent and purpose records
   - Processor and third-party information
   - Data discovery and classification outputs (where integrated)

b. Users shall be able to review, validate, modify, and override auto-populated inputs with mandatory justification capture, ensuring accountability and traceability.

**Periodic Reviews and Re-Assessments**

a. The solution shall support scheduled, periodic DPIA reviews to ensure ongoing regulatory and policy compliance.

b. The solution shall enforce reassessment of DPIAs upon material changes to processing activities, systems, data categories, vendors, or transfer mechanisms.

c. All re-assessments shall be versioned, with previous approved versions preserved as read-only and fully traceable.

d. The solution shall provide dashboards highlighting active, pending, overdue, and high-risk DPIAs against defined SLAs.

**Risk Management**

a. The solution shall enable documented privacy risk treatment plans specifying:
   - Recommended controls and remedial measures
   - Responsible owners and accountable functions
   - Target remediation timelines
   - Implementation and completion status

b. The solution shall support residual risk evaluation and formal risk acceptance workflows, including DPO and governance approvals where required.

c. All mitigation actions shall be tracked to closure with supporting audit evidence.

d. The solution shall provide mechanisms to periodically validate the effectiveness of implemented mitigation controls and update risk ratings based on observed outcomes.

**Reporting and Regulatory Readiness**

a. The solution shall provide real-time dashboards showing, at a minimum:
   - DPIA lifecycle status and progress
   - Risk levels and criticality distribution
   - SLA adherence and exception tracking
   - Business-wise, function-wise, and branch-wise DPIA coverage

b. The solution shall support one-click generation of DPIA reports and evidence packs in Bank-approved formats for management review, audits, and regulatory inspections.

c. All reports and artefacts shall be retained with integrity controls, versioning, and restricted access.

**Security and Access Control**

a. The solution shall enforce role-based access controls in alignment with bank policy.

b. The solution shall support session controls including authentication, idle timeouts, step-up authentication for sensitive actions, and session invalidation.

c. The solution shall maintain tamper-proof audit logs capturing all DPIA actions including creation, edits, reviews, approvals, and exports.

d. The solution shall align with the Bank's security baseline, logging, and audit requirements.

#### 1.6.7.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply.

#### 1.6.7.3 Deliverables/Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

**DPIA Governance and SOP Package**

a. Bank-approved DPIA methodology, SOP, and operating model.
b. Defined roles, RACI, escalation paths, and approval thresholds.
c. DPIA templates, questionnaires, and reporting formats.
d. Risk categorization, scoring, and treatment framework.

**Configured DPIA Tooling**

a. Production-ready DPIA solution with configured templates, workflows, risk scoring, approvals, and audit trails.

**Reporting, Dashboards, and Evidence Artefacts**

a. Regulator-ready DPIA reports and evidence exports.
b. DPIA-wise evidence packs including decisions, approvals, and mitigation tracking.

**Testing, Training, and BAU Transition**

a. UAT scenarios, execution evidence, and acceptance sign-off.
b. Training and knowledge transfer for business, privacy, and governance teams.
c. Go-live, hyper care, and business-as-usual (BAU) transition documentation.

### 1.6.8 Records of Processing Activities (ROPA)

#### 1.6.8.1 Detailed Requirements

**Scope and Alignment**

a. The bidder shall implement a centralized Data Inventory and RoPA capability to document and maintain personal-data processing activities across the Bank.
b. The capability shall align with the DPDP Act, applicable DPDP Rules, RBI expectations, and other laws of the land as applicable to the Bank's operations and Bank policies, and support audit-ready accountability.
c. The RoPA repository shall be the system of record for processing activity documentation for Bank-defined in-scope products, processes, systems, and third parties/processors.
d. The solution shall support linkage of RoPA records with the Data Discovery and DPIA modules to enable consistent processing activity references, risk visibility, and evidence traceability
e. The solution shall support automated impact analysis of changes to systems, processes, or data flows by identifying affected RoPA records through relationship mapping, and shall trigger notifications, tasks, and workflows to ensure timely review and update of impacted records.

**RoPA Data Model**

a. The solution shall maintain a RoPA entry for each Bank-defined processing activity, capturing at minimum:
    - Processing activity name/ID and description
    - Business owner and technology owner

- Purpose(s) and (where applicable) lawful basis/consent dependency reference
- Data principal category
- Personal data categories
- Source systems and primary storage locations (system-level)
- Recipients / third parties / processors (where applicable)
- Cross-border transfer flag and destination (where applicable)
- Retention reference and deletion/erasure dependency reference (where applicable)
- Security/control notes (high-level, Bank-defined fields only)

b. The RoPA model shall support linkages to Bank-defined identifiers for: system/application, process/product, and vendor/processor.

**Creation and Review**

a. The solution shall support controlled workflows for: create → review → approve → publish → revise → retire.
b. The workflow shall support Bank-defined roles (author/reviewer/approver) and maker–checker approvals where required.
c. Each RoPA record shall be versioned; prior approved versions shall remain retrievable as read-only.
d. The solution shall support periodic review cycles and ad-hoc review triggers when a Bank-defined “material change” occurs (e.g., new system, new vendor, new purpose, new data category, cross-border transfer introduced).

**Import/Export Records**

a. The solution shall support bulk import of RoPA records using Bank-approved formats.
b. The solution shall support export of RoPA registers and record packs.

**Retention, Restriction, and Erasure Controls**

a. The solution shall support Bank-defined retention schedules linked to processing activities, data categories, systems, and lawful retention obligations.
b. The solution shall support orchestration of deletion, erasure, restriction, or suppression actions upon expiry of retention periods, completion of processing purpose, withdrawal of consent, or validated rights requests, subject to legal hold and statutory/regulatory exceptions.
c. The solution shall maintain auditable records of retention decisions, deletion/erasure actions, legal holds, exceptions, approvals, and downstream confirmations in Bank-approved formats.

### 1.6.8.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply.

### 1.6.8.3 Deliverables/Outcomes

a. Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

b. Configured RoPA data model (fields, taxonomies, mandatory rules) as per Bank-approved template.
c. Configured workflows for create/review/approve/publish/revise/retire including maker–checker approvals where required.
d. Configured versioning and review cadence controls.
e. Migration/import of Bank-provided RoPA (excel files) into the tool with validation and exception handling.
f. Baseline RoPA coverage for Bank-prioritized Tier-1 processing activities (as per Bank-provided list).

### 1.6.9 Third Party Risk Management

#### 1.6.9.1 Detailed Requirements

**Third-party Inventory and Processor Registry**

a. The bidder shall implement a Third-Party Risk Management (TPRM) capability that enables the Bank to assess, monitor, and govern third-party solutions, vendors, service providers, and data processors that process personal data on behalf of the Bank.
b. The solution shall maintain a centralized database of vendors/data processors to simplify risk management, enable consistent governance, and act as the system of record for third-party privacy and security obligations.
c. The solution shall support maintenance of complete vendor profiles including entity identifiers, service categories, processing roles (processor/sub-processor), onboarding status, risk tiering, and linkage to relevant Bank business owners and system owners.

**Third Party Self-service Portal**

a. The solution shall provide a secure vendor self-service portal that allows vendors/data processors to access assigned assessments, upload evidence, respond to clarifications, and track remediation actions.
b. The vendor portal shall support controlled access, role-based permissions, and traceable activity logs of vendor actions, submissions, and updates.
c. The solution shall enable Bank administrators to configure vendor portal access lifecycles including invitations, authentication, access expiry, and suspension/termination controls.

**Risk Assessments**

a. The solution shall support creation, assignment, execution, and lifecycle management of third-party risk assessments for vendors and data processors, including draft, in-progress, review, remediation, and closure statuses.
b. The solution shall provide pre-defined vendor assessment questionnaire templates that can be customized by the Bank.
c. The solution shall support scoring, evidence attachment, reviewer comments, exception handling, and approval workflows for assessments, including maker-checker or multi-level approvals where required by Bank governance.

**Processor Mapping**

a. The system shall allow mapping of each processor to the purpose(s) they serve and the personal data/PII types they handle.
b. The system shall create and maintain an auditable linkage between processors, Bank purposes, and processing contexts, enabling impact analysis and risk reporting for third-party processing.

**Integration with Privacy Governance Modules**

a. The system shall integrate with the Bank's Data Principal Rights, DPIA, and Breach modules to fetch processor-linked activities, risks, and status updates.
b. Integration shall enable end-to-end traceability between processors and rights actions (including deletion), between processors and DPIA risk findings, and between processors and breach events/notifications.
c. The system shall maintain consistent audit logs across integrated workflows, ensuring that third-party actions and Bank actions are traceable and exportable for audit/regulator's needs.

#### 1.6.9.2 Functional and Business Requirements

Common Business and Functional Requirements, where applicable, shall apply.

#### 1.6.9.3 Deliverables/Outcomes

Common deliverables / outcomes, where applicable, shall apply to the module-specific requirements, including but not limited to:

**Registry and Portal**

a. Configured third party/processor database with fields required for Bank governance including authorized contact details and escalation mapping.
b. Configured third party self-service portal with RBAC, onboarding/invite workflow, evidence upload capability, and activity logs.

**Questionnaire and Assessment**

a. Pre-defined assessment questionnaire templates delivered and configured for Bank use, with Bank customization capability.
b. Import mechanism and evidence for importing existing Bank questionnaires/templates with version control and governance.
c. Configured assessment lifecycle workflows including assignment, vendor response, review, remediation tracking, approvals, and closure.

## 1.7 Technical requirements (Hardware, Software, volumetric etc.)

The Bidder shall ensure that the proposed solution and its components comply with the following technical requirements:

- The solution shall consist of proven, industry-standard products and technologies. Customization may be applied only where necessary to meet the Bank's business objectives.

- The solution must be scalable to handle growth in data volumes, concurrent users, and query complexity. Scalability shall be linear, ensuring predictable performance improvements as nodes or racks are added without performance penalty.
- The solution should be interoperable and support open architecture standards (e.g., XML, LDAP, SOA) to enable information flow and integration with internal and external systems.
- High availability must be ensured through redundancy in hardware and connectivity, enabling 24x7x365 service continuity.
- The solution should maintain data integrity, reliability, and business continuity at all times.
- The solution shall protect against technology obsolescence by supporting co-existence of at least two hardware node generations, current (n) or Latest Generation for seven years from installation. In case of upgrades beyond projected growth or contract extension, the Bank will migrate to latest available generation. If co-residency is not feasible, mutually agreed price discounts will apply for technology obsolescence.
- The Bidder shall supply, install, commission, and maintain all required hardware at Data Centre (DC), Disaster Recovery (DR), and other Bank-specified sites. This includes servers, storage, archival, and backup components.
- Bidder shall implement the proposed solution at DC and DR locations.
- Rack space including power cooling, electricity, and fire safety will be provided by Bank via colocation provider. Bidder needs to mention in the proposal how many racks space at DC and DR will be required to host the infrastructure.
- All solution components should be scalable, secure, flexible, and supported by 24x7x365 onsite support.
- The Bidder shall ensure proper hardware sizing to meet current and projected requirements, in compliance with all Service Level Requirements (SLRs).
- The Bidder must quote a single make and model for each component. Quoting multiple options will not be accepted. If any options are found in the Manufacturer Authorization Form (MAF), technical proposal, masked Bill of Materials, or Bill of Materials, the bid will be rejected.
- The overall compute and security of the enterprise data privacy governance & compliance platform shall be the responsibility of the Bidder. The Bank's security team will provide the compliance requirements, and the Bidder shall ensure adherence to them for application and network security.
- The Bidder shall design, supply, size, commission, and manage the infrastructure to meet the RFP requirements.
- The proposed hardware technology must be best-of-breed, latest stable release, and OEM-tested.
- Infrastructure shall remain Bank-owned but Bidder-managed during the contract. Training, knowledge transfer, and documentation must be provided to Bank officials at contract completion.
- Virtualization technologies may be leveraged, provided there is no adverse impact on performance.
- The Bidder shall install, maintain, and manage antivirus software for all servers at the Data Centre (DC) and Disaster Recovery (DR) sites. The Bank will provide antivirus licenses for its existing solution (TrendMicro). The Bidder must ensure compatibility with the Bank's antivirus system. If any proposed components do not support TrendMicro, the Bidder must provision an alternative antivirus solution acceptable to the Bank. This compatibility requirement must be validated with the Bank's Infrastructure Security team.

- Bidder is responsible for accurate sizing. If quoted sizing is insufficient, upgrades/replacements must be provided at no cost. Infrastructure must have sufficient headroom to handle projected growth. Horizontal scaling costs are Bidder's responsibility.
- The proposed solution must not have a single point of failure (servers, network, storage, etc.).
- All goods must be fully insured against loss or damage during transport, storage, assembly, implementation, and maintenance until delivery to the Bank.
- All servers must run on commercially supported OS versions.
- The Bidder must provide all requisite licenses required to host the proposed application, which includes licenses for the OS, compilers, multipathing, file systems, volume managers, clustering, failover agents, and any other required system software, for unlimited instances wherever applicable.
- The Bidder shall provision monitoring consoles for all the hardware components and applications supplied by them, which includes servers, network, security events/incidents,
- Appropriate rack enclosures from OEM must be included for the storage solution.
- Servers must be load balanced, with failover capabilities.
- Infrastructure and network must support industry-standard protocols.
- The Bidder must maintain spare hardware at DC and DR for immediate replacement to ensure high availability as per the defined SLA. The Bank may audit the same.
- The solution must comply with all relevant regulatory and statutory guidelines (not limited to Government, RBI, IBA, IDRBT). During the contract, Bidder shall implement required upgrades at no additional cost. Bidder shall comply with the Bank's Information Security guidelines while implementing its proposed solutions.
- The Bidder must provide user manuals, requirement documents, implementation methodology, architecture documentation, UAT scenarios, and test cases.
- All solution components must be fully integrated with minimal manual intervention and support standards-based, reusable interfaces for flexible integration.
- Hardware details (SIT, Development, UAT, Production, DR) must be submitted as per Annexure XXVI and Appendix II (Masked BOM).
- Hosting space, power, and DR configuration details must be submitted as per Annexure XX. For Bank to plan the hosting area, Bidders must provide the space required in DC and DR in per square feet.
    a. Space requirements
    b. Cooling requirements
    c. Power requirements (Consumed power in a rack should not exceed 3.5 KVA)
    d. Standard temperature requirements / heat
    e. DR configuration
- All hardware (required for interface, staging, Web Server, Production and Non-Production related hardware components) and system software components required for the project must be included in the original bill of Material of the Bidder. In case Bidder fails to do so, and the project demands additional components at a later stage, then Bidder should provide additional components at no additional cost to the Bank.
- All the ATS and AMC of the software and infrastructure supplied through this RFP needs to be factored by the Bidder. All bug resolution / issue fix / patch management and all coordination with OEM needs to be done by the Bidder. The bidder must submit backlining agreements or confirmations from all proposed OEMs.
- Bidder shall maintain all in-scope items across environments and perform vendor management during the contract.

- All proposed hardware and software must support IPv4 and IPv6 where applicable.
- At least 20% spare storage capacity must be maintained at all times.
- No component shall be end-of-sale within 2 years of delivery. All equipment must be supported for the entire duration of the contract period. If any component is announced as end-of-life or end-of-support during the contract period, the bidder should upgrade the component to a supported version at no additional cost to the bank.
- The platform must provide centralized management for provisioning, monitoring, capacity planning, SLA monitoring, and administration of all enterprise data privacy governance & compliance platform services.
- The Bidder shall adopt leading development practices, including SDLC, Agile, or Hybrid methodologies, as applicable to the Bank's requirements. Analytical use cases shall be developed in an agile manner. The approach should include software testing strategy, plans, and execution cycles for UT, SIT, UAT, and Performance Testing.
- The bidder shall be responsible for providing and managing all necessary cabling, patch cords, transceivers, fibre/copper connectivity, cable dressing and labelling required for successful installation and integration of the proposed solution within the Bank's infrastructure standards.
- The proposed solution shall be deployable within the rack space available at the Bank's Data Centre and Disaster Recovery Centre. The bidder shall specify the total number of network connectivity ports, storage connectivity ports with redundancy, rack space, power, cooling and environmental requirements for all proposed hardware and infrastructure components. All hardware/software must meet Technical and Functional Requirements in Appendix I.
- Bidder must provide onsite support for planned and unplanned DR activities as and when requested by the bank. The bidder shall be responsible for ensuring DR activities are done within the stipulated RPO / RTO. Penalty will be applicable otherwise.
- The Bidder to ensure that all the hardware component rack mountable and air cooled.

### 1.8 Data Security & Privacy Management

The proposed Privacy Management Platform shall incorporate robust data security and privacy controls to ensure protection of personal data in compliance with the Digital Personal Data Protection Act, 2023, RBI cybersecurity guidelines, and other applicable regulatory requirements.

Data security and privacy shall act as a foundational cross-cutting layer across all modules of the proposed solution.

The Bank will provide enterprise security solutions such as:

- SIEM / Logging & Monitoring
- Data Loss Prevention (DLP)
- Web Application Firewall (WAF)
- Anti-Virus
- Network / Perimeter Firewalls
- Intrusion Detection / Prevention Systems (IDS/IPS)
- Encryption & Key Management tools
- Privileged Access Management (PAM) systems
- VAPT tools

The bidder shall ensure seamless integration of the proposed privacy platform with these existing controls wherever required.

### 1.8.1 Access Control & Identity Management

The solution must support Role-Based Access Control (RBAC) with the principle of least privilege, ensuring users have access only to data and functionalities required for their roles.The platform must enforce:

The platform must enforce:

- Separation of Duties (SoD) across administrative, operational, and audit functions
- Periodic access review and recertification
- Controlled access for privileged users (admins, DBAs, etc.)

The system shall support:

- Granular access controls (module-level, function-level, and where applicable, data-level)
- Approval workflows for user provisioning and access requests
- Controlled handling of ad-hoc data access requests with appropriate approvals

### 1.8.2 Data Protection & Encryption

The solution must ensure protection of personal data through:

- Encryption of data at rest, in transit, and during processing where applicable
- Support for masking, anonymization, and pseudonymization techniques, especially for sensitive personal data

The bidder shall ensure that:

- Even privileged users cannot directly access sensitive data unless explicitly authorized.
- Secure mechanisms are implemented for data sharing (internal/external) using encryption and access controls.

### 1.8.3 Environment & Deployment Requirement

a. The bidder shall supply and deploy all hardware, system software, and application components required to host the proposed solutions in the Bank's approved DC/DR locations.

b. The bidder shall provide a detailed environmental deployment matrix covering DC, DR, Development and UAT, including server sizing, storage sizing, network and security dependencies, operating system/database versions, middleware dependencies, clustering, and failover design.

c. The bidder shall ensure that the architecture is reviewable and subject to approval by the Bank, and any modifications suggested by the Bank shall be incorporated during the design stage without additional cost or impact on project timelines.

d. The bidder shall propose a physically segregated and dedicated setup for components hosted in DMZ

e. Production and Non-Production environments for Militarized Zone as well as De-Militarized Zone, shall be physically isolated; however, shared storage infrastructure may be proposed provided logical segregation (separate LUNs/volumes) is ensured with strict access controls.

f. The bidder shall ensure that adequate licenses are provisioned to support all environments throughout the contract period.

g. The proposed solution shall support Disaster Recovery (DR) through asynchronous data replication from Data Center (DC) to DR site.

h. The solution must meet the following requirements:

   i. Recovery Time Objective (RTO): 2 hours

   ii. Recovery Point Objective (RPO): 15 minutes

   iii. Failover to DR shall be carried out strictly in accordance with the Bank's DR policy.

i. The bidder shall be responsible for:
   i. Designing and implementing data synchronization and replication mechanisms
   ii. Ensuring data consistency across DC and DR environments
   iii. The DC and DR environments may be designed in Active-Active or Active-Passive configuration, clearly specifying workload distribution.

j. The bidder shall propose and size infrastructure for the following environments:
   i. Production Environment (DC & DR):
      - Production environment for both DC and DR shall be identical.
      - Production environments at DC must be configured in High Availability (HA) mode. Production environments at DR must be configured in High Availability (HA) mode.
   ii. Non-Production Environments:
      - Separate environments must be provided for:
      - Development and User Acceptance Testing (UAT)
      - Mirror the software stack, configurations, and security controls of production
      - Have scaled-down infrastructure (At least 30% of production capacity based on Year-3 sizing)

### 1.8.4 Security

a. The bidder shall ensure that all supplied hardware, virtual machines, operating systems, databases, middleware, and supporting components are hardened and aligned to the Bank's security baseline, cybersecurity controls, privacy requirements, and regulatory expectations.
b. All supplied components shall support installation and integration of Bank-mandated security controls, including but not limited to monitoring agents, antivirus agents, certificates, connectors, logging agents, and patch management controls
c. The bidder shall be responsible for closure of all infrastructure-level, operating-system-level, database-level, and application-level vulnerability observations attributable to the proposed solution stack during implementation and throughout the contract period.
d. The solution shall integrate all relevant logs (application, access, consent, DPR, audit logs) with the Bank's SIEM and incident management systems.
e. The solution shall comply with applicable standards including ISO 27001, ISO 27701, DSCI guidelines, e-Governance standards, IT Act 2008, and DPDP Act, 2023 and Rules 2025.
f. The solution shall follow security by design and privacy by design principles across all modules.
g. The bidder shall ensure closure of all VAPT observations identified by the Bank or its auditors at no additional cost.
h. The solution shall adhere to the Bank's IT, Information Security, Cyber Security, and Data Protection policies.
i. The solution shall support integration with the Bank's Active Directory / IAM for authentication, role-based access control, and segregation of duties, along with SSO using standard protocols.
j. The solution shall maintain complete audit trails for all user actions and access to personal data.
k. The solution shall ensure encryption of sensitive data (including PII) at rest and in transit and PII Data shall be masked/encrypted at application, when data in use.
l. The solution shall support data masking, anonymization, or pseudonymization where required.
m. The bidder shall ensure server hardening, patch management, and endpoint security for all solution components.
n. The bidder shall ensure secure APIs, periodic security assessment, and remediation of vulnerabilities.
o. The bidder shall comply with audit, monitoring, and incident response requirements, including timely closure of audit observations.

p. The bidder shall sign NDA and ensure confidentiality, integrity, and availability of all Bank data and systems.
q. The bidder needs to provide SBOM, CBOM, API BOM wherever applicable for the version of application deployed and subsequently version when upgraded.
r. The bidder shall provide the Certificate of confirmation that the application deployed is free from malware.

### 1.9 Backup & restoration

a. The bidder shall ensure backup and restoration capability for all supplied hardware and solution components, including application data, configuration, logs, audit trails, and supporting metadata, in line with the Bank's backup policy and retention requirements.
b. The bidder shall define and implement backup schedules, retention periods, restore procedures, validation processes, and recovery evidence for all in-scope environments.
c. The bidder shall propose a backup and restoration solution for the Privacy Management Platform covering application data, consent records, DPR data, audit logs, and configuration data.
d. The solution shall support incremental and full backups as per the Bank's backup and archival policy, including:
    - Daily incremental backups
    - Weekly full backups
    - Monthly full backups
e. Backups shall be stored at the Data Centre (DC) with replication to Disaster Recovery (DR) for long-term retention, as per the Bank's archival policy.
f. The solution shall support secure, reliability, and timely restoration at the level of:
    - Individual records / files
    - Application components
    - Full system (where required)
g. The solution shall provide a centralized interface (GUI) for backup monitoring, management, and restoration activities.
h. The bidder shall ensure that backup data is encrypted and protected in line with Bank security policies and regulatory requirements.
i. The bidder shall conduct periodic restoration testing (at least quarterly) and submit reports to the Bank.
j. The bidder shall ensure that backup and restoration processes meet business continuity and disaster recovery requirements of the Bank.
k. The bidder shall be responsible for supply, installation, configuration, and maintenance of the backup solution throughout the contract period without additional cost.

### 1.10 Scalability

a. The proposed hardware architecture shall support horizontal and vertical scalability to meet increased user load, transaction volumes, integrations, scan volumes, storage growth, reporting loads, and log retention requirements over the contract period.
b. The bidder shall provide growth assumptions and indicate the upgrade path without major disruption to Bank operations.
c. The solution shall be highly scalable to support current and projected volumes of digital users, data principals, and transactions across the Bank.
d. The solution shall be sized to meet defined Service Level Requirements, including response time and throughput, under expected and peak workloads.

e. The solution shall ensure that real-time operations (e.g., consent capture, DPR processing) are not impacted by batch processing activities such as data discovery and reporting.
f. The solution shall support varying load patterns, including peak scenarios such as regulatory deadlines, campaign surges, and high user activity periods.
g. The bidder shall factor in growth and workload variations for sizing. In case of performance or scalability shortfalls, the bidder shall upgrade or optimize the solution at no additional cost to the Bank.
h. The solution shall support efficient handling of increasing volumes of personal data, audit logs, and compliance records while maintaining consistent performance.
i. The solution shall ensure scalability of key capabilities including consent management, DPR workflows, data discovery, reporting, and audit logging.

### 1.11 Training & Knowledge Transfer

a. Training shall be provided to Bank personnel using a Train-the-Trainer model, covering IT team, privacy operations team, and business users.
b. Training shall be role-based, simple, and hands-on, covering key modules such as consent management, DPR handling, data discovery, DPIA, and reporting.
c. The bidder shall provide in-depth technical training to the Bank's IT and admin teams for configuration, administration, and integration of the solution.
d. Training shall be conducted at Bank locations or through online mode, as decided by the Bank.
e. The bidder shall propose a detailed training plan, including batch size, duration, and schedule, for Bank approval.
f. Training materials, user manuals, and documentation shall be provided in advance and updated as per the deployed solution.
g. The bidder shall ensure knowledge transfer and operational readiness, including reverse KT sessions and hands-on exposure for identified Bank personnel.
h. The bidder shall collect feedback after each training session; in case of unsatisfactory feedback, the training shall be re-conducted at no additional cost.
i. The bidder shall provide ongoing and periodic training support during the contract period.
j. OEMs shall provide training for their respective products/modules wherever applicable.
k. The bidder shall ensure all relevant users are trained on solution functionalities aligned to the scope of the RFP.

### 1.12 Escrow

a. The Bank and the successful bidder agree to appoint an escrow agent to provide escrow mechanism for the deposit of the customized source code for the solution supplied by the bidder to the Bank to protect the Bank's interests in an eventual situation.
b. Source code for customization done for the Bank in the solution and for other related services shall be provided by the bidder to the Bank for unlimited and unfettered use by the Bank.
c. The customized 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.
d. The 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.
e. The bidder shall transfer all Intellectual Property Right on non-exclusive basis for all the customizations done for the Bank for the solutions.
f. The Bidder will bear 100% of the costs for the Escrow.

g. 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.
h. As a part of the escrow arrangement, the bidder shall be required to provide detailed code documentation which has been duly reviewed and certified by an external independent organization. The escrow code along with all documentation shall be periodically updated every year by the bidder. Bidder shall submit a self-certificate confirming the same after every update.
i. The Escrow arrangement shall meet all the necessary regulatory and statutory compliances.
j. The Escrow arrangement suggested by the successful bidder shall not be binding on the Bank.
k. The Bank reserves the right to explore alternate escrow mechanisms based on the Bank's existing practices.

### 1.13 Licensing

a. The bidder shall ensure that all hardware components proposed under this RFP are supplied to the Bank on an outright purchase basis, with ownership transferred to the Bank upon delivery, along with all associated firmware and embedded system software required for their functioning.
b. The proposed solution shall support enterprise-scale deployment aligned to the volumes and capacity envisaged in this RFP.
c. Further, the licensing model shall not impose any restrictions on the number of users, consent transactions, data principal requests, API integrations, or internal processing activities within the Bank's ecosystem.
d. For the entire contract duration of three (3) years, the bidder shall provide comprehensive support, maintenance, upgrades, security patches, and all regulatory or statutory updates (including but not limited to DPDP Act, Rules, and any future guidelines) without any additional cost to the Bank. During this period, the solution shall remain fully operational and compliant without requiring any separate subscription or license renewal for core capabilities.
e. All software licenses shall be non-restrictive and portable across the Bank's environments, including Data Centre (DC), Disaster Recovery (DR), Development and User Acceptance Testing (UAT) environments, ensuring seamless scalability and operational flexibility.
f. The solution shall remain usable and fully functional post completion of the contract period, with the Bank retaining full usage rights of the deployed platform and infrastructure, thereby ensuring business continuity and eliminating dependency on recurring subscription or usage-based charges for core solution capabilities.
g. Successful Bidder must provide required licenses in the name of Bank either through OEM or through OEM's licensing partners. However, payment will be made by Bank to successful Bidder only.
h. As per the recent advisory by RBI on availability of Software Bill of Material (SBOM) and Cryptographic Bill of Material (CBOM), the End User License Agreement must be in the name of Indian Bank and SBOM / CBOM details of all the components in the proposed solution by the respective OEM should be made available with the bank after the completion of implementation phase.

## 2. Project Governance and Project Timelines

### 2.1 Project management & Governance

The bidder will constitute a team to manage the project activities. As part of the bidder's Scope of Work they are expected to:

### 2.1.1 Project Planning

a. Define a project plan/roadmap for contract period from onboarding till project completion
b. Interact with relevant stakeholders within the bank to align them with the current state of the project, governance tools, metrics and escalation mechanisms
c. Prepare monitoring templates and monitoring the progress made (including SLA adherence)
d. Sharing project status updates with all the relevant stakeholders.
e. Define escalation matrix in conjunction with the Bank & identify actions to the project.
f. Workout mitigation plans for each/any delayed initiative
g. Foresee and inform of any risks and gaps in the plan proposed and minimize and/or mitigate those risks
h. Define an approach for Knowledge Transfer & Reverse Knowledge Transfer.
i. Drive regular project cadence, monthly meetings & steering committee meetings along with following-up on the deliverables.

The Bank would be responsible for reviewing the progress of the Program and taking all decisions related to overall policy and technology matters. The Bank would continue to have oversight during all the phases of project including implementation phase.

### 2.1.2 Setup and Execution

The Bidder will perform the following activities:

a. Engage Senior Architects & SMEs at important stages of project.
b. Bring in Industry & Technology experts from time to time to resolve any longstanding issues and give certain path-breaking direction to the project.
c. Define escalation matrix in conjunction with the Bank & identify actions to the project.
d. Weekly progress meeting & action tracking.
e. Monthly/Quarterly meeting of Management to take critical decisions & resolve disputes.
f. The ‘Project Director’ would head the Program and would be supported by project managers.
g. The Bidder has to ensure oversight from its top management by conducting engagements every three months between the bank and its counterpart in the Bidder organization.
h. Bidder is expected to steer the project by conducting monthly/quarterly steering committee engagements between the bank and the Bidder senior management.
i. Proper Work base schedule, Risk register and monthly assessment need to be maintained and shared with the Bank.
j. The Bidder should report the project progress to the Bank.
k. For all the change requests, the Bank will review the design & implementation of all components and their changes, if any. The Bidder will have to present their approach and get sign-off from the Bank before developing/building the same. The effort estimates and timeframe for implementation will be mutually agreed by the Bidder and the Bank.
l. Set up the project management office and framework comprising of:
    - Project charter formulation
    - Project risk analysis
    - Assistance in project management and project delivery team identification and resourcing
    - Change management procedures
    - Project planning and detailing
    - Project quality management procedures
    - Employ a formal project methodology on all Enterprise Data Privacy Governance & Compliance Platform modules undertaken with the level of detail and control scaled

appropriately to the magnitude of the project effort and adhere to all project management processes and procedures

m. Project Manage the following phases of the project:
   - Understand the current business landscape
   - Business parameterization
   - Customization based on business needs
   - User Acceptance testing
   - Integrations with computing, storage, and networking
   - Go-live/ Rollout
n. Closure of issues pending for resolution
o. Measure the progress made in the implementation of the project
p. Track customization and gaps
q. Monitor the progress of defined business parameters and customizations as per delivery schedules
r. Provide regular updates to the steering committee and board as required by the Bank
s. Participate in all technical and functional discussions relating to projects
t. The bidder is required to project manage the Go-Live and provide periodic reports.
u. The bidder is required to sufficiently staff Project Managers on-site for the entire program across the various phases.

Bidder is required to establish a well- defined and properly staffed project team structure in place to ensure smooth implementation of the project. The focus should be on having the right mix of personnel in the project team with respect to both the area of expertise as well as the relevant experience in that area.

The description for the project team should come out clearly as part of manpower deployment scheme that the Bidder will have to propose in its technical bid. Project team design will go a long way in setting the right communication lines, winning the bank's confidence in the Bidder and facilitating smooth coordination in regular project functioning as well as in resolving issues and therefore will be one of the important criteria for bid evaluation. The Bidder will have to describe the project team design and structure keeping the following aspects in view:

a) Implementation of phase requirements

b) Operations and maintenance phase requirements

### 2.1.3 Resource Deployment & Evaluation

Bidder needs to factor below mentioned minimum resources for the program. Bidder needs to size the resources to meet the implementation timelines. All the roles are mutually exclusive. Bidder needs to submit the Annexure XXIV with the required document for all the resources.

| S.No | Role | Location | Resource Criteria | Description |
|---|---|---|---|---|
| 1 | Program Director / Program Manager | Chennai | Graduate/Postgraduate in Law / IT / Information Security / IT Risk Management. Certifications: CIPP/CIPM/CIPT/CDPSE preferred. 8-12 years experience | Leads the overall privacy management program from the bidder side and drives end-to-end governance, |

| | | | | |
|---|---|---|---|---|
| | | | managing Privacy / Data Governance / Regulatory programs, including implementation in large BFSI environments. | delivery, stakeholder coordination, and milestone execution. |
| 2 | Privacy SME | Chennai | 5-8 years BFSI experience in Privacy / Compliance / Risk / Governance roles. Strong knowledge of DPDP, RBI, SEBI regulations. Experience in enterprise privacy implementations preferred. | Provides deep domain expertise on DPDP, privacy governance, consent, rights handling, and regulatory interpretation for solution implementation. |
| 3 | Techno-Functional Team Member (Privacy) | Chennai | 3-5 years' experience in BFSI domain. Experience in requirement gathering, workflow design, and privacy solution implementation. Exposure to Data Mapping / Discovery preferred. | Translates business, regulatory, and operational privacy requirements into functional workflows, use cases, and implementation specifications. |
| 4 | Data Discovery / Classification Lead | Chennai | 3-5 years' experience in data discovery, classification, metadata, and inventory management. Experience in structured/unstructured scanning. | Designs and governs discovery, scanning, classification, and inventory approaches for structured and unstructured personal data across in-scope systems. |
| 5 | Integration / API Expert | Chennai | 3-5 years' experience in API integration, system connectivity, and enterprise application integration. Exposure to middleware and banking integration scenarios required. | Designs and implements secure integration of the privacy platform with Bank systems through APIs, connectors, and orchestration mechanisms. |
| 6 | Data Governance / Privacy Governance Lead | Chennai | 3-5 years' experience in data governance, lineage, classification, retention policies, and regulatory compliance frameworks. | Establishes governance controls for data ownership, lineage, retention, classification, and privacy operating model alignment. |
| 7 | Security & Privacy Controls Specialist | Chennai | 3-5 years' experience in security and privacy controls. Certifications like CISSP/ISACA preferred. Hands-on experience in encryption, masking, access control, logging. | Designs and validates security, encryption, masking, access control, logging, and privacy safeguard |

| | | | | |
|---|---|---|---|---|
| | | | | requirements for the solution. |
| 8 | Infrastructure Support | Chennai | 3-7 years' experience in administration and support of enterprise IT infrastructure and deployment, configuration, and maintenance of enterprise applications and supporting infrastructure. | Hands-on experience in Windows/Linux servers, virtualization, network administration, Active Directory/LDAP, patch management, infrastructure hardening, and troubleshooting. Experience in BFSI environments preferred. |
| 9 | Support Engineer | Chennai | 2-4 years' experience in application/infrastructure support and incident management. | Hands-on experience in troubleshooting, log analysis, user support, ticketing tools, monitoring, and operational support. Exposure to privacy, security, or compliance solutions preferred. |

### 2.1.4 Governance

a. Bidder governance is an important aspect of tool enablement projects. Bidder governance shall cover:
   - The objective of the governance management process is to ensure seamless delivery of quality services to Bank, so that the Bank is able to perform effectively & mitigate risks emerging out of enterprise data privacy governance & compliance platform. The Teams are expected to operate as a single cohesive unit, working closely with relevant business, functional stakeholders & associated vendors, and partners, with each role and responsibilities clearly defined.
   - The Bank is thus looking for effective governance procedures & clear escalation matrix from the bidder that would involve their Executives, Decision Makers & corresponding teams from the Bank.

b. Governance Structure

| S.NO | Governance Layer | Governance Participants | | Responsibilities | Review Frequency |
|---|---|---|---|---|---|
| | | Bank | Bidder | | |
| 1 | Steering Committee | Executive Sponsor | Executive Sponsor | Define strategic objectives<br>Ensure continual executive<br>Performance reporting<br>Issue resolution (Final escalation level) | Quarterly/ Semi Annually |
| 2 | Program Management | Head IT Department | Program Managers | Account Management | Monthly |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Monitor service delivery<br>Single point of contact for issue escalation<br>Issue resolution (Intermediate escalation) | |
| 3 | Operations Management | IT Department Team lead | Team Leads | Issue resolution and escalation<br>Manage people issues<br>Plan, track and review SLAs<br>Plan and track timelines | Weekly / Ad-hoc |

c. All members of the project team should have relevant and sufficient experience and qualifications as mentioned in the above table.
d. Names of core team members must be provided in the RFP response. The members must be proposed for overall implementation period.
e. The Bank reserves the right to conduct interviews for all proposed onsite resources.
f. Only upon the Bank finding the candidate suitable, the resource shall be formally onboarded for the project.
g. The resources should be dedicated and deployed onsite in Bank premises as per the Bank's calendar working days for this project.
h. The Bidder shall provide round-the-clock (24/7) support to the Bank following the implementation of the solution (Application Support) & Infrastructure support from the time of the delivery of the Hardware, with support personnel physically present at the Bank's premises (Office, Data Centre/Disaster Recovery Centre) to resolve the issues (if any) within the turnaround time (TAT) and SLA as per Bank's defined guidelines. For the CVs proposed (other than Named Resources), the Bidder must provision proposed resources or resources having similar or better qualification and experience mentioned in the CVs in the Bid. If required, the Bank may seek in person interview of the person being proposed.
i. Performance Monitoring and Replacement: At any point during the contract period, the Bank assesses that a deployed onsite 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.
j. 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. The bank will not consider substitutions except in cases of incapacity of Named Resources for reasons of health/ separation from the organization. Similarly, after award of contract the Bank expects all of the proposed Named Resource to be available during implementation of the contract. For the reason where replacement is proposed by the Bidder due to nonavailability of the originally proposed Named Resources or in cases where replacement has become necessary as a Named Resource proposed by the Bidder has been found to be unsuitable for the project by Bank during contract implementation, the following shall apply: The replacement shall have similar or better qualifications and experience. The Bank reserves the right to interview the replacement candidate before giving its approval. There should be a minimum of 2 weeks' transition period

between the outgoing Named Resource and the incoming Named Resource. Any transition of less than 2 weeks will attract a penalty as mentioned in the SLA of RFP.

k. In case any of the proposed resources are found to be not performing or not meeting the expectations of Bank, the SI shall find a replacement for the resource with matching or better qualifications and experience within two weeks. Bank will evaluate the replacement profile and indicate the acceptance / rejection of the profile. If required, Bank may seek a personal interview of the person being proposed.

l. Named Resources should be present during the technical presentations.

m. Only one person can be proposed for the role of one Key Team Member. The Bidder must provide the CVs as per the format given in Annexure XXV

### 2.1.5 Project Timelines

The Selected Bidder shall be responsible for delivery, installation, commissioning, implementation, integration, testing, and rollout of all hardware, software, and services required under this RFP, within the timelines prescribed by the Bank. If the BIDDER fails to do so within the stipulated time schedule or by the date extended by the Bank, it will be a breach of contract. In such case, the Bank would be entitled to charge a penalty or would have the right to terminate the contract, as specified in this RFP.

The implementation timelines shall include activities such as hardware sizing finalization, Bill of Materials (BoM) freeze, procurement, delivery, installation, hardening, environment setup, system software readiness, integration validation, and acceptance testing.

| Sr. No. | Milestones | Timelines |
|---|---|---|
| 1 | Delivery of Hardware and Installation | T1 + 8 Weeks = T2 |
| 2 | Implementation and Integration of Software | T2 + 14 Weeks |
| 3 | Training and Knowledge Transfer | T2 + 16 Weeks |
| 4 | Go-Live | T2 + 16 Weeks = T3 |
| 5 | Post Go-Live Support | T3 + 3 Years |

*T1 – Date of PO issuance by the Bank*

**Extension period:**
Bank at its discretion may extend the contract after Maintenance and Support period for another Two (2) years. This extension will be at discretion of the Bank and will be on mutually agreed terms and conditions.

## 2.2 Acceptance Criteria

Solution will be considered as 'Go-live' only if below mentioned points are successfully completed by the Bidder.

1. All the Components supplied by the Bidder as part of the bill of materials (Hardware, Software, Integration) are completely installed, tested, and signed off by the Bank.
2. All the software functionalities as per BRD and Technical and Functional Requirements in Appendix I has been tested and signed off by the external testing agency under the scope of Functional and Acceptance testing and by the Bank.

3. The entire solution been tested and signed off by any external testing agency (if required) under the scope of Functional and Acceptance testing and by the Bank.
4. Provided all the Documents and Manuals as per the scope of the RFP and accepted by the Bank.
5. Bidder should have performed one time DR Drill, and the report of the same has been accepted and signed off by the Bank.
6. All the issues identified during the first VAPT audit post deployment of the solution are closed and signed off by the Bank.

All the training mentioned as part of the scope are completed.

**3. Operations, Support and Services**

**3.1 OEM responsibilities**

a. The bidder shall be committed to the success of the project and take ownership during the actual implementation. The bidder shall also ensure requisite support from the OEM for various aspects of project including configuration, customization, sizing, performance tuning and implementation support. The Bidder shall assess the requirement of professional services from OEMs for all components of the solution, and provision for requisite support from OEMs.
b. Provision of qualified personnel to ensure highest standards during implementation and support phases. OEM's involvement should be onsite during the implementation of each key solutions being proposed by the bidder during implementation Phase. After the implementation is completed, the OEM should support the bidder for solution reviews and fine-tuning. Bidder needs to submit Annexure XXIII as part of eligibility criteria confirming the same. The OEM has to review and submit the report on Functional Requirement Specification Document, System Requirement Specification Document, High Level Design Document, Low Level Design Document, migration strategy and Go-Live directly to Bank with their issues/concerns/observations. OEM has to review till all the issues/concerns/observations are rectified by the bidder. OEM shall also provide
c. Certification of solution compatibility
d. Endorsement of sizing and architecture
e. Confirmation of long-term roadmap alignment
f. Dedicated escalation matrix from OEM for critical issues.
g. OEM shall support
   - Security assessments
   - Regulatory compliance reviews
h. Appendix II Bill of Materials should be filled in accordingly.
i. Adequate participation from key OEM's is required during design, development and implementation phases. The bidder is required to submit an undertaking from the OEM for the same. The bank will also have the right to interview the resource or/and evaluate the resume of the resource against the criteria stated in the RFP, if the resource is found unsuitable, the bank may ask for replacement of resource.
j. Bidder will have to replace the resources found unsatisfactory to the bank upon interviewing. The new resources could be either internal or from independent agencies at no additional cost to the Bank.
k. The bidder will take the help of concerned OEMs for vetting and auditing the technical solution.

### 3.2 Post Go-Live Support

The Bidder shall take end-to-end responsibility for Annual Maintenance Contract (AMC) services, and Warranties covering all hardware, software, middleware, and databases forming part of the Bank's Enterprise Data Privacy Governance & Compliance Platform and related infrastructure. These responsibilities shall encompass all functions required to ensure sustained performance and availability of the environment. Responsibilities include, but are not limited to:

1. Services shall be delivered across all environments, including production and non-production.

2. A working day shall mean any day when any branch or office of the Bank is operational. For the purpose of service standards, business hours shall be from 7:00 to 23:00 hours on all working days.

3. All AMC operations shall be carried out from the Bank's premises. The Bidder shall deploy qualified operational support staff with proven onsite experience in managing the entire Enterprise Data Privacy Governance & Compliance Platform and associated application and hardware components.

4. The Bidder shall provide comprehensive support in accordance with the Agreement of this RFP.

5. The Bidder shall ensure that any Standard Operating Procedures (SOPs) are aligned with ISO 27001 and ITIL standards, covering infrastructure installation, monitoring, management, data backup and restoration, security, business continuity, disaster recovery, and all operational procedures. SOPs shall be reviewed, approved, and updated based on the Bank's operational and compliance requirements.

6. AMC and ATS payments shall follow the payment terms defined in this RFP. Bidders must note that any Warranty pertaining to Hardware and Software / Applications that extends beyond the contract period due to the Hardware / Software / Applications supply towards the terminal years of the contract must be provided and supported by the Bidder without any additional cost to the Bank.

The following subsections outline the scope of activities and services to be undertaken by the Bidder for support services and the list is indicative and not exhaustive. The Bidder shall include any additional activities necessary to ensure uninterrupted, compliant, and efficient operation of the Enterprise Data Privacy Governance & Compliance Platform and its supporting infrastructure.

#### i. Infrastructure Management

The Bidder shall be responsible for comprehensive infrastructure management services covering all components of the Enterprise Data Privacy Governance & Compliance Platform environment. These services shall ensure the stability, performance, scalability, and compliance of the underlying infrastructure.

**Scope of Infrastructure Management Services:**

- Provide full support for servers, operating systems, system management software, and utilities, including minor upgrades and release updates.

- Deliver periodic maintenance services, including system health checks and trend analysis reports.
- Manage system IDs, domain structures, OS-level security configurations, and overall OS administration.
- Administer file system directories, distributions, and replications to ensure efficient data organization and access control.
- Continuously analyze, monitor, and enhance system performance.
- Ensure strict adherence to the Bank's IT policies, including Security, Information Security (IS), and Backup policies.
- Support all infrastructure-related migration and testing activities.
- Coordinate and manage any infrastructure changes that could affect the service levels of dependent systems or providers.

**Incident and Restoration Management:**

- Manage incidents from detection to service restoration.
- Validate problem severity classifications and initiate appropriate resolution procedures.
- Facilitate Service Recovery Team meetings for major incidents.
- Escalate unresolved issues as per the escalation matrix.
- Conduct Root Cause Analysis (RCA) and implement corrective and preventive actions.
- Prepare and execute restoration plans to minimize downtime.

**Monitoring and Problem Determination:**

- Monitor hardware and software performance within the defined service windows and uptime parameters specified in the RFP.
- Perform basic problem determination for hardware, system software, and network-related issues.
- Evaluate planned changes to servers or appliances and provide technical recommendations to support these changes.
- Monitor and respond to system, hardware, and application alerts, including file system utilization and event logs.
- Maintain system error logs and perform required ad-hoc batch setup activities.

**Configuration, Performance, and Capacity Management:**

- Implement effective configuration, performance, and capacity management to maintain optimal system utilization and stability.
- Generate reports and insights to assist the Bank in proactive infrastructure scaling and performance planning.

**Implementation and Support Services:**

- Conduct requirement analysis, assist in hardware and system software acquisition, and perform installation, testing, and verification.
- Implement and maintain hardware and licensed software necessary for business-critical operations.
- Provide expert-level support to isolate and resolve complex network, operational, and software-related issues.

- Conduct responsive maintenance to identify and rectify faults affecting system performance.
- Coordinate and scheduled maintenance activities with relevant Bank functions such as network and facility management teams.
- Act as a single point of contact for end users for hardware-related issues, upgrades, or consultations.
- In the event of permanent replacement, provide substitute equipment of the same or higher configuration and make/model. If the Hardware supplied by the Bidder is to be replaced permanently, then the Bidder shall replace the equipment of same Make / Model with same configuration or of higher configuration.

**Performance and Process Management:**

- Manage CPU, memory, input/output performance, and Ethernet traffic to maintain optimal system performance.
- Execute process and memory management functions to ensure system stability.

**Backup and Recovery Management:**

- Define and maintain backup schedules in alignment with the Bank's policies.
- Perform routine data backups and restoration to ensure data integrity and availability.
- Ensure that daily backup copies are created and stored securely in compliance with the Bank's data protection policies.
- Produce and maintain system audit logs for the retention period agreed with the Bank.
- Archive expired audit logs and store them off-site in accordance with the Bank's retention policy.
- Periodically review audit logs to detect and report any security lapses or anomalies.
- Maintain full backup coverage for the entire Facilities Management period.

**ii. Application Management**

The Bidder shall be responsible for end-to-end management of all applications forming part of the Enterprise Data Privacy Governance & Compliance Platform, ensuring continuous availability, optimal performance, and compliance with the Bank's operational requirements.

**Scope of Application Management Services:**

- Install, configure, and uninstall applications as required by the Bank.
- Deploy application objects and manage deployments within the application server environment.
- Configure, start, stop, and manage application server services.
- Configure and manage HTTP services supporting the applications.
- Process and implement approved change requests related to applications.
- Identify, analyze, and fix application bugs in a timely manner.
- Perform vulnerability assessments and apply necessary corrective measures.
- Execute data migration and data upload activities to support application transition and upgrades.
- Migrate application code and components to new environments while ensuring version integrity.
- Provide 24x7 monitoring and management of application performance.
- Establish and maintain Disaster Recovery (DR) setups, including DR synchronization and periodic DR drills and conduct quarterly DR drills or as per the Bank's defined policy.
- Perform capacity management to ensure applications operate within optimal thresholds.

- Troubleshoot issues related to the application server, products, and patch management.
- Utilize and maintain monitoring tools provided for application servers.
- Manage application server backup and restoration to ensure data and configuration integrity.
- Coordinate with product vendors for technical support and issue resolution.
- Manage application patching and maintain version control for all deployed applications.
- Execute version migrations, testing, and implementation of updated application releases.
- Maintain file-level backups of application servers to ensure recoverability.
- Administer portal and content management activities associated with application platforms.
- Provide resolution and support for known errors and recurring issues.
- Monitor web and application server availability, generate alerts for anomalies, and take corrective action to prevent disruptions.

**Software Development and Version Control**

- Maintain a defined Secure Software Development Life Cycle (SSDLC) for all components, covering development, testing, deployment, and maintenance stages.
- Prepare and maintain required documentation for each SSDLC phase, including design, testing, and approval records.
- Implement and maintain version control for software components and related documentation to ensure change traceability.
- Segregate development, User Acceptance Testing (UAT), and Production (DC & DR) environments to prevent cross-environment contamination.

**Security Policies and Governance**

- Maintain compliance with the Bank's Information Systems Security Policy (ISSP), network security policy, and software license policy.
- Ensure implementation of the Bank's disaster recovery (DR) plan and compliance with isolated and integrated DR requirements.
- Review existing Bank security procedures and recommend improvements to strengthen protection of system and application resources.
- Implement a Bank-approved access control programme covering authentication, virus detection and eradication, logon administration, and synchronization across servers and applications.
- Synchronize security configurations and access information across all relevant systems to maintain uniform policy enforcement.

**Operational Security Management**

- Bidder must integrate various log types and logging options into Bank's SIEM, ticketing, workflow, and case management system during support phase also in case if there are any changes in the Bank's ecosystem.
- All security incidents, including those reportable to CERT-In, should be reported to the Bank by the bidder within the timelines stipulated under the Bank's IS Policy, along with proper documentation.

**Personnel and Vendor Security**

- The bidder needs to ensure that all the developers allocated to the Banks should be trained in the secure development practices.

- Conduct mandatory background verification for all personnel involved in service delivery.
- Ensure all Bidder resources comply with the Bank's security guidelines, confidentiality clauses, and acceptable use policies.
- Coordinate with Bank's officials or Bank's third parties for integrated security operations and monitoring as required.

**Compliance and Continuous Improvement**

- Use system access provided by the Bank strictly for performing contracted services.
- Support the Bank in creating users, maintaining authorization, and audit mechanisms.
- Continuously evaluate and enhance security configurations to maintain compliance and resilience.
- Maintain complete documentation and evidence of all security operations for audit and regulatory review.

**Software Management**

The Bidder shall provide complete Software Management services to ensure continuous functionality, stability, and maintainability of all licensed, developed, and supported software forming part of the solution.

**Technical Support and Maintenance**

- Provide comprehensive technical support for all licensed and Bank-owned software, including defect and non-defect issues related to office automation products, systems, and applications.
- Deliver end-to-end support encompassing problem tracking, source identification, impact assessment, resolution, bypass, recovery assistance, and management reporting.
- Conduct trend analysis to identify recurring issues and propose corrective actions.
- Provide any additional software support required by the Bank within the defined service scope.
- Maintain and operate a helpdesk for software support, ensuring all service records and calls are logged, monitored, and reviewed monthly by the Bank.

**Incident and Problem Management**

- Log every reported incident and track it through to resolution.
- Ensure that the Bank assigns a severity level (P1 to P4) for each incident and comply with the defined response and resolution timelines.
- For P1 incidents, provide real-time updates and hourly progress reports until full resolution.
- For defect-related problems, issue defect correction details, workarounds, or bypass solutions where reproduction is possible in the defined software environment.
- Provide the Bank with periodic updates and a monthly consolidated report detailing the status and resolution of all reported incidents.
- Extend assistance to end users for Non-Standard Software support, including problem diagnosis and resolution.

**Operational Continuity and Service Obligations**

- Continue delivering all facilities management services without interruption during disputes or arbitration proceedings.
- Maintain overall functionality and stability of the solution, ensuring immediate corrective action in case of any software failure affecting the solution.
- Ensure uninterrupted functioning of the system during any software, hardware, or network failure through redundancy and recovery mechanisms.

**Change, Configuration, and Performance Management**

- Perform configuration changes, performance monitoring, and troubleshooting of all software components under this RFP.
- Provide technical support for data ingestion processes, database tuning, and maintenance of application and data components.
- Take and maintain database backups, perform recoveries, and manage query generation and optimization as required.

**Bug Fixing, and Knowledge Management**

- Identify, log, and correct all detected software errors within the timelines agreed with the Bank.
- Undertake immediate bug fixing for any defects impacting operational continuity or service levels.
- Provide tools and mechanisms to create and maintain a knowledge repository covering identified bugs, resolution methods, and version or upgrade history for applications, operating systems, and databases.

**Compliance and Reporting**

- Maintain auditable records for all software management activities including incidents, patches, configuration changes, and version updates.
- Submit periodic status and compliance reports to the Bank as part of ongoing operational reviews.

**iii. Patch and Version Management**

The Bidder shall be responsible for end-to-end patch and version management across all components of the solution, ensuring system stability, compliance, and continuity of operations.

**Patch Management Responsibilities**

- Plan, schedule, and execute rollout of all software patches and upgrades.
- Obtain formal Bank sign-off before implementing any patch release.
- Communicate release schedules and train operational teams to ensure readiness for patch implementation.
- Maintain controlled storage of all software versions and patches across centralized and distributed environments.
- Distribute, install, and verify all patch releases to ensure successful deployment.
- Adhere to the Bank’s patch management policy and applicable security control requirements.

- Perform testing and validation of all patches and upgrades before deployment in the production environment.
- Execute hardware and firmware patching for all application and database servers.

**Version Upgrade and Change Control**

- Provide version upgrades during the contract period, ensuring all existing configurations and customizations are successfully migrated.
- Ensure backward compatibility and seamless transition during version upgrades, minimizing system downtime and operational disruption.
- Deliver all standard version upgrades and related enhancements at no additional cost to the Bank.
- Undertake major version upgrades only upon Bank's request, subject to mutually agreed terms and costs.
- Maintain the ability to revert to earlier system versions upon request from the Bank.
- Ensure all modifications such as bug fixes, patches, and minor enhancements are implemented without disrupting ongoing operations.
- Maintain complete traceability and documentation of version changes, upgrade histories, and related approvals.

**Service Continuity and Compliance**

- Conduct all patching and upgrade activities with minimal service impact. Any downtime not pre-approved by the Bank shall be attributed to the Bidder and excluded from "Agreed Service Down-Time."
- Ensure immediate correction of detected software errors within agreed resolution timelines.
- Include all statutory, regulatory, and industry-mandated upgrades as part of standard patch and version management services at no extra cost.

**iv. Warranty Management**

The Bidder shall provide comprehensive Warranty Management services to ensure continued operational availability and compliance of all hardware and software components for the solution.

**Warranty Coverage and Period**

- All products and solutions proposed under this RFP shall include Original Equipment Manufacturer (OEM) warranties of a minimum of three (3) years for hardware (including necessary system software) and one (1) year for application software.
- In addition, the bidder shall submit documentary proof of backlined AMC/ATS agreements with all proposed OEMs, confirming that support obligations (patches, updates, bug fixes, and security releases) shall be honored for the entire contract period.
- Post-warranty, the Bidder shall provide Annual Maintenance Contract (AMC) or Annual Technical Support (ATS) for the remaining contract period.
- The warranty shall cover all components like hardware, software, media, patches, updates, and licenses with full on-site support as provided by the OEM.
- Hardware (including necessary system softwares) warranty shall commence from the date of commissioning; application software warranty shall commence from the Go-Live date.
- No hardware parts, accessories, or subsystems shall be excluded from warranty coverage.

- Warranty obligations shall comply with all applicable technical standards, security, operational, and recovery requirements defined by the Bank.

**Maintenance, Repair, and Replacement**

- The Bidder shall perform all maintenance, repairs, and replacements at the Bank's site at no additional cost.
- If any equipment requires off-site repair, the Bidder shall provide a substitute unit, transfer data securely, and wipe all data from the original device prior to removal. Transportation and logistics costs shall be borne entirely by the Bidder.
- Equipment with repeated hardware failures (four or more times within three months or six times within twelve months) must be replaced with new equipment of equivalent or higher configuration at the Bidder's cost.
- The Bank reserves the right to impose penalties for delays in repair, replacement, or delivery of equipment or for any failure to meet commissioning or acceptance timelines.
- Preventive maintenance shall be conducted quarterly, including internal and external cleaning and virus checks. Proper records shall be maintained at each site.
- Failure to perform preventive maintenance or delays in repairs shall result in an automatic extension of the warranty period equivalent to the delay duration.

**Warranty Data Management**

- The Bidder shall maintain a centralized inventory database of all hardware and software warranties, including registration details, renewal dates, and license information for all Bank-owned or Bidder-supplied assets.
- Perform warranty and license registration with OEMs for all procured components, whether supplied by the Bidder or directly by the Bank.
- Provide periodic reports on warranties, hardware leases, and software licenses as requested by the Bank.
- Maintain complete data on entitlements for software upgrades, refreshes, replacements, and maintenance.
- Perform a comprehensive inventory of all warranties and licenses at project commencement.

**Compliance and Warranty Conditions**

- The warranty shall remain valid even if the Bank installs supplementary hardware or software purchased from certified third parties, provided proper intimation is given to the Bidder.
- The Bidder warrants that all goods supplied are new, unused, of current models, and incorporate the latest design improvements.
- All equipment supplied shall be free from defects in design, materials, and workmanship, except where the Bank's specifications dictate otherwise.
- The Bidder shall bear all costs associated with labour, spares, preventive and unscheduled maintenance, and transportation for repairs or replacements.
- If equipment is taken outside Bank premises for repair, the Bidder shall coordinate Insurance, warranty claims, dispatch authorized vendor service providers, and bear all related costs.

**Standards and Preventive Controls**

- The Bidder shall develop and maintain technical standards, operating procedures, and recovery procedures jointly with the Bank to ensure compliance and uniformity.
- Design, update, and maintain logical network configurations, servers, and PC environments in line with service level commitments.
- Conduct hardware maintenance, including preventive, corrective, and scheduled activities, to maintain OEM-specified performance levels without affecting system uptime during working hours unless explicitly approved by the Bank.

**Reporting and Compliance Assurance**

- Provide warranty maintenance data and related documentation as reasonably requested by the Bank to support replacement or refresh planning.
- Submit periodic compliance reports confirming warranty status, service records, and adherence to service levels.
- Ensure all warranty obligations remain active and enforceable throughout the contract term, including during extensions or transitions.

**v. Asset Tracking and Relocations**

The Bidder shall manage asset tracking and relocation services to ensure complete visibility, control, and accountability of all hardware and software assets throughout their lifecycle.

**Asset Inventory and Tracking**

- Perform an initial inventory of all hardware and software to establish or validate the Bank's baseline asset database.
- Affix inventory tags on all assets and record relevant information in the centralized asset tracking system.
- Define and implement a standardized process for tracking all hardware and software assets from procurement to disposal, including configuration or ownership changes during their lifecycle.
- Act as the single point of contact for asset management data, maintaining accurate and up-to-date equipment information for all items supplied under this RFP.
- Conduct periodic physical inventory checks and audits as per Bank-defined guidelines and assist in resolving any identified discrepancies.
- Maintain complete documentation of the current location, operational status, and repair status of all hardware assets.
- Provide the Bank with all required updates to maintain synchronization between the Bidder's asset database and the Bank's asset management system.
- Track and report Mean Time Between Failures (MTBF) for all hardware components to support performance analysis and replacement planning.

**Relocation and Reinstallation Services**

- Provide full logistical support, reinstallation, and reconfiguration services if the Bank decides to relocate or shift infrastructure to a new or alternate site during the contract period.
- Ensure continuity of operations during relocation and minimize disruption to business functions through proper scheduling and execution planning.
- Perform all relocation activities outside business hours unless explicitly approved by the Bank.

- Bear all costs associated with relocation, transportation, and setup under the contract; no additional charges shall be levied on the Bank.
- Ensure that all contractual terms, service levels, and obligations remain in full force following relocation or site change.

**Operational and Cost Responsibilities**

- All costs, including travel and logistics, related to the execution of asset tracking and relocation activities shall be borne entirely by the Bidder.
- Maintain complete and verifiable audit trails for all asset management activities to ensure traceability and compliance with contractual and operational standards.

**vi. Monitoring and Incident Response**

The Bidder shall establish and operate a comprehensive Monitoring and Incident Response framework to ensure uninterrupted system availability, security, and compliance across the environment.

**Monitoring and Performance Management**

- Implement continuous and automated monitoring mechanisms covering all applications, infrastructure, and security components of the solution.
- Deploy advanced monitoring tools to track platform health, uptime, performance metrics, and response times.
- Provide the Bank's designated personnel with secured dashboard access to view audit logs, system alerts, and performance reports in real time.
- Conduct ongoing evaluation of system and application performance against defined SLA and RFP benchmarks.
- Monitor hardware utilization and performance daily and provide reports with capacity planning recommendations.
- Ensure 24x7x365 monitoring and management of system availability, data integrity, and overall infrastructure security.
- Maintain full oversight of Data Centre components, including web/application servers, databases, storage, and backup infrastructure.
- Undertake periodic performance tuning of systems to ensure optimal efficiency and compliance with service levels.

**Logging, Auditing, and Security Oversight**

- Maintain detailed logs of all user and system activities, including access to critical data, privileged account actions, administrative changes, and authorization attempts.
- Ensure audit trails capture all activities, including failed login and authorization attempts, and are securely maintained for forensic and compliance purposes.
- Make all audit logs and records readily available to the Bank upon request for investigation or audit.
- Integrate all logs and alerts with the Bank's SIEM or ticketing system to enable centralized incident management and correlation analysis.

**Incident Detection and Response**

- Establish a robust incident detection and response framework with automated alerts and escalation protocols.
- Implement advanced security monitoring and threat detection systems, including real-time anomaly analysis, intrusion detection, and automated response mechanisms.
- Report all security incidents, anomalies, or breaches immediately to the Bank, with simultaneous logging into the Bank's incident response systems.
- Perform detailed Root Cause Analysis (RCA) for each incident, implement corrective actions, and submit incident reports to the Bank.
- In the event of a data breach, promptly notify the Bank and relevant regulatory authorities, assist in legal investigations, and fully cooperate with forensic and compliance teams.

**Business Continuity and Recovery**

- The Bidder shall ensure to have effective business continuity and disaster recovery plan. The Bidder shall develop and establish a robust framework for documenting, maintaining and periodic testing of business continuity and recovery procedures and shall maintain a record of the same as per applicable law.
- The Bidder is also required to conduct at least one DR drill of the proposed Platform in a quarter or as per the Bank's requirement and submit report for the same to Bank. During Bank's scheduled DR drill, proposed solution should seamlessly integrate with Bank's DR environment.

**Coordination and Escalation**

- Coordinate with OEMs and third-party vendors for resolution of critical incidents and underlying hardware or software faults.
- Maintain a defined escalation matrix to ensure timely response and resolution for all operational and security events.

**vii. Change Management**

The Bidder shall establish and maintain a structured Change Management process approved by bank to ensure controlled, traceable, and compliant execution of all system modifications, upgrades, and enhancements within the solution.

**Regulatory and Statutory Changes**

- Implement all statutory or regulatory changes mandated by the Government of India (GOI), Reserve Bank of India (RBI), or any other competent authority at no additional cost to the Bank.
- Ensure timely deployment of such changes without impacting existing operations or compliance obligations.

**Customization and Controlled Change Execution**

- All customizations, enhancements, or modifications during the maintenance and support period shall follow a formal Change Management process defined jointly with the Bank. This includes statutory and regulatory requirements as well as any dashboards, reports, or models requested by the Bank during the AMC period. All such changes must be implemented without any additional cost to the Bank.

- No change shall be executed without written approval from the Bank's designated authority.
- Each approved change must be logged, version-controlled, auditable, and documented with traceability to its source request and outcome.

**Maintenance and Continuous Improvement**

- Maintenance activities shall include production monitoring, troubleshooting, issue resolution, and implementation of system change requests.
- The Bidder shall perform necessary enhancements and software adjustments arising from statutory, regulatory, or industry-driven changes as part of routine support services.
- Additional modifications required by the Bank's IT team for compliance or operational needs shall also be implemented under the defined Change Management framework.

**viii. IT Service Desk**

The Bidder should maintain an IT Service desk that supports L1/L2/L3 support for both hardware and software where in L1 would generally handle basic resolution, L2 provides technical solution support and SLA coordination and L3 provides specialist resolution for critical defects, outages, performance, security, and platform issues as applicable along with the Bank's internal support staff, external service providers and/or other agencies as appropriate. The Bidder must ensure that the resources proposed for the IT helpdesk should have adequate experience in the relevant areas of support. Also, reports should be provided that effectively summarize and communicate the performance and compliance with service levels defined in the Bank's service level agreement (SLA) with the Bidder. Bidder must note that helpdesk services should be available for all environments viz., production (DC and DR) and non-production (Development and UAT). Bidder is required to allocate sufficient number of resources to meet the SLA. Also, Help Desk resources should be part of only the Help Desk team and should not be shared resources between Help Desk, maintenance, support, and development teams. Bidder in coordination with the Bank's existing vendor should ensure that all the proposed hardware, software and other peripherals application should seamlessly integrate with the Banks's Monitoring and Ticketing tool.

It is the responsibility of the Bank to provide the necessary seating space, furnishing, desktops, and electrical connections for the Helpdesk resources along with PSTN telephones with STD facility, etc.,

Bank also has the right to audit the production, development and test systems including desktops, laptops for data security, at any time. Also, the Bank can reject resources of the Bidder, if they do not have the necessary skill set to be staffed for providing support. The Bank will have the ability to directly generate standard and ad hoc reports as needed.

Bidder support should have the following features / functionalities:

- Liaison with third party vendors.
- Should act as a Single Point of Contact for all services.
- Should encompass Helpdesk, Asset Management and Vendor Management.
- A focused approach for delivering integrated Service Management.
- Providing telephonic and/or electronic mechanisms for problem reporting requests for service, and status updates with each seat having an out-bound dialing facility.
- Tracking problems from initial call to restore service.

- Log Tickets in the Service Desk Tool on behalf of users calling service desk over phone with the correct category, severity, problem description, user information.
- Route Service Requests to the appropriate teams.
- Notifying users/customers of problem status and resolution.
- Monitoring systems to proactively determine, diagnose, and resolve problems.
- Receive incidents, service requests, queries, change requests from End Users and IT through one of the agreed modes for communication.
- Escalate issues/ tickets which are going beyond service levels or pertain to Vendors non-performance or delays or pertain to users' non-availability or non-cooperation.
- Track all issues and send status updates on the progress.
- Prepare MIS for the tickets.
- Extract agreed and ad-hoc reports from the Service Desk tool and send them to concern groups/ upload them in the reporting portal.
- Maintain up-to-date information on the customer contacts, Vendor contacts, management contacts, SLA matrix, Severity, and categorization matrix.
- Ensure the workspace is clean and has all the relevant information (contact details, escalation matrix, etc.) which is easily retrievable.
- Bidder to ensure to integrate with the Banks applications for monitoring performance and installed software and applications with all the solution proposed in the RFP before the Go-Live to ensure smooth functioning.
- Bidders must maintain a knowledge base for recurring issues and their resolutions. Standard Operating Procedures (SOPs) are required for common tasks such as patching and user provisioning. Bank's SOPs must be followed for all activities, except for non-standard tasks, for which the bidder hall create new SOPs.
- Bidder should onboard the resources as per the timelines and before onboarding any resources, Bidder needs to submit the background verification check document and should take approval from the Bank.
- Bank will do a quarterly performance review of all the deployed resources and will have the right to ask for replacement with any resource based on the performance review. Bidder needs to provide the equivalent or higher qualified resource within the timeframe.
- Bidder needs to factor below mentioned minimum resource for the maintenance and support period. These are only the minimum number, and Bidder needs to right size number of resources to meet the SLA. Bidder needs to submit Annexure-XXIV with the required document for all the resources.

**Resources for maintenance and Support**

| S. No. | Role | Location, Type & Shift |
|---|---|---|
| 1 | Platform Support | • L1 (Chennai, Mumbai): 24x7 (including Holidays)<br>• L2 (Chennai): Bank Working Hours and Holidays<br>• L3 (Chennai): Bank Working Hours |
| 2 | Infrastructure Support | • L1 (Chennai, Mumbai): 24x7 (including Holidays)<br>• L2 (Chennai): Bank Working Hours and Holidays<br>• L3 (Chennai): Bank Working Hours |

| | | |
|---|---|---|
| 3 | Program Manager | • Bank Working Hours |

- Bidder can deploy additional resources to meet the SLA of the RFP with no additional cost to Bank.
- Support engineers should be responsible for customization, development, MIS / Reports / dashboard and analytical requirements, resolving any technical, operational related issues either with application integration, support day-to-day activities and any back-end activities etc.,
- Support engineers should be responsible for including but not limited to log shipment, DC to DR cut-over, App / Data Backups, Restoration, Application Patches / Upgrades, User Access Review, resolution of VAPT / IS Audit observations, integration with Bank's security solutions (SIEM, PIM, DAM etc.), Active Directory and other IT solutions.
- For all the L1 and L2 level support, Bank will evaluate the resource for day-to-day operations and/or implementation skills and if found that the resource is not meeting
- For all the L1 and L2 level support, Bank will evaluate the resource for day-to-day operations and/or implementation skills and if found that the resource is not meeting the tasks required to be fulfilled by the resource, the Bank may ask the Bidder to replace the resource. The Bank will also have the right to interview the resource or/and evaluate the resume of the resource against the criteria stated in the RFP, if the resource is found unsuitable, the Bank may ask for replacement of resource.
- All the Statutory, regulatory changes required need to be done at no additional cost by the bidder during the contract period. All the reports, dashboard, and Model which bank would be required during the contract period need to be built by the bidder using the support and maintenance resources at no additional cost by the bidder. The priority of the delivery can be mutually agreed between bank and Bidder.
- The on-site engineers are expected to provide following services: Configuration changes, version up-grades, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, and liaison with OEM for various support issues, taking periodic backup of the database, query generation, etc.,
- RBI master direction on Outsourcing of Information technology services to be followed by the Bidder.
- Bank will check the relevant work experience of the resources deployed and will not permit, if not satisfied with any of the resources. Bidder should provide substitute resources within 3 working days while ensuring that the overall service levels are not impacted.
- The Bank reserves the unconditional right to accept / replace any team member with the qualifications and competence as required by the Bank during the course of assignment pursuant to this RFP.

### 3.3 Development Process Guidelines

- The Platform / software developed or customized should follow a standard development process to ensure that it meets functional, security, performance & regulatory requirements of the Bank.
- For every software including any third-party software delivered to the Bank, the Bidder must deliver to the Bank, documents including user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/ database administrative documents, debugging/ diagnostics documents, test procedures. The Bidder

should also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all product components, list of all dependent/ external modules and list of all documents related to traceability of the product as and when applicable. Any level / version changes and / or clarification or corrections or modifications in the above-mentioned documentation should be supplied by the Bidder to the Bank without any additional cost to Bank.

- All the patches/ fixes/ updates, minor version upgrades of all the software components released by the OEM during the contract period should be provided. The Bidder should ensure implementation of all the patches/ fixes/updates and minor version upgrades in the production environment to the latest version during the contract period, without any additional cost to Bank.
- The Platform integration testing will be followed by user acceptance testing, plan for which must be submitted by the Bidder to the Bank. The UAT includes Functional tests, Resilience tests, Benchmark Comparisons, Operational tests, Load tests. Indian Bank staff/ third Party vendor designated by the Bank will carry out the functional testing. This staff / third party vendor to be trained by bidder for this purpose. Bidder should carry out other testing like resiliency / benchmarking / load. Bidder should submit result log for all testing to the Bank.

### 3.4 Escalation Matrix

The bank as well as the bidder will decide on an escalation matrix to resolve any issues that may crop up during implementation of the project. Both the bank and bidder and respective OEM shall inform the names of the people, email ids and their telephone numbers for the escalation matrix to be effective.

## 4. Commercial, Legal & Compliance

### 4.1 Malicious Code Certificate

The Bidder should submit following certificate in the bid:

1. This is to certify that the Solutions and Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:
   a) Inhibit/ alter/ disable essential functions / critical settings, rending the application unusable or unreliable

   b) Block communications or data flow, isolating the application from networked systems and preventing updates or controls

   c) 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 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.

### 4.2 Data Protection

Bidder will process Bank's personal data on Bank's behalf as part of the Services, bidder will comply with the Information Technology Act, 2000, Digital Personal Data Protection Act' 2023 and other applicable law and regulation and will comply with all applicable privacy and data protection provisions and applicable laws. Further, it must be ensured that due care be taken while collecting and dealing with sensitive personal data or information. Data to be stored within the physical boundary of the country.

Any Web portal used by the bidder to procure Bank Data will be secured to avoid hacking, infusion of virus, unauthorized copying, tampering, etc. and all sort of security required as per applicable law & practices to be adopted and implemented by the bidder.

### 4.3 Monitoring & Audit

Compliance with best security practices /statutory or regulatory guidelines may be monitored by periodic computer security audits/Information Security Audits performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The successful bidder must provide the Bank access to various monitoring and performance measurement systems. The successful bidder must provide the Bank access to the auditing menu through the application itself and facilitate the audits. 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 Service Level Agreement (SLA) (format will be shared with the Successful bidder along with Purchase order), 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.

The Bank may conduct security audit in the proposed solution after complete implementation. Bidder should enable bank or bank’s appointed vendor in performing periodic information security, IT security, VAPT etc. on infrastructure provisioned for bank. Bidder should close the audit gaps as per the timelines stipulated by Bank without any additional cost to the Bank. The observations may be made at any frequency by the bank or bank appointed external system audit team. Bidder shall provide certification of the auditor to the Bank regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed.

Whenever required by the Bank, Bidder should furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/ Reserve Bank of India and or any regulatory authority required for conducting the audit. The Bank reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the bidder (e.g., financial, internal control and security reviews) and findings made on the Bidder in conjunction with the services provided to the Bank.

The Bank may audit Bidder’s records during normal business hours related to the Services covered under this Agreement.

### 4.4 Documentation:

Detailed documentation (functional and technical) shall be provided to the Bank on all the implementation and customization done. Documentation and data dictionary shall be updated and provided to the Bank after every customization.

The following minimum documentation (hard copy and soft copy) on any proposed software components must be made available in English as per the Bank’s deployment and architecture.

1. Detailed project plan.
2. Software Requirement Specification document (SRS).

3. Documentation of technical requirements.
4. Documentation of architecture requirements.
5. Mapping of Functionality and specifications document.
6. Development of low level and high-level design documents.
7. Documentation of testing plan, test cases, test scenarios, test scripts, gaps, bugs, fixes, etc. as a part of quality assurance.
8. All documentation including technical, operations, like release notes, license terms, user manuals, training manual, technical manual, standard operating procedures, solution architecture and design, system flow document, data dictionary and other necessary documents etc.
9. Error tracking and defect resolution documentation process.
10. Statement of Work (SOW), Quality Plan, Test Plan, Requirement traceability Matrix, Design Document, Report Design, Delivery Notes documents, etc.
11. System configuration documents.
12. System/debugging/diagnostics documents.
13. All the SOPs related to the implementation and operations.
14. All the API specification document.

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

### 4.5 Period of Validity of Bids

Bids should remain valid for 120 days after the last date for submission of bid prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive. Bank may seek extension of bid validity period, if required. Bidder needs to extend the bid without any additional cost to Bank.

### 4.6 Authorization to Bid

Responses submitted by a Bidder to this RFP (including response to functional and technical requirements) represent a firm offer to contract on the terms and conditions described in the tender document. The proposal must be signed by an official authorized to commit the bidder to the terms and conditions of the proposal. Bidder must clearly identify the full title and authorization of the designated official and provide a statement of bid commitment with the accompanying signature of the official and submit the copy of power of attorney on the stamp paper authorizing the signatory to sign the bid.

### 4.7 Payment Terms

The scope of work is divided in different areas, and the payment would be linked to delivery and acceptance. All/any payments will be made subject to LD / penalty / compliance of Service Levels defined in the RFP document.

Payments for hardware shall be milestone-linked and shall be made only after successful delivery, installation, commissioning, and acceptance sign-off by the Bank.

The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank.

The payments shall be made within 30 Working days from the date of receipt of valid claims that are supported by original invoice, original Proof of Delivery (POD), acceptance by the bank and upon fulfilment of other conditions stipulated in the contract. The invoices and other documents are to be duly authenticated by Bidder.

On receiving each payment, the Bidder shall submit a stamped receipt for the payment received including TDS. The payment will be released by the Bank after deducting applicable TDS. All payments will be made only by electronic transfer of funds either by NEFT or RTGS to the bank account number mentioned in the original invoice submitted by the bidder.

Payments as per the schedule given below will be released only on acceptance of the order and on signing the agreement/contract by the selected bidder and also on submission of performance guarantee through Bank Guarantee as per Annexure IV

| Deliverables | % of Payment | STAGES (On completion of the activities) |
|---|---|---|
| **Infrastructure Cost** | **70% of Table C in Appendix II** | On delivery and commissioning of Hardware and required Software items for the setup of infrastructure for the proposed solution and on submission of Invoice and Acceptance/Sign off by the Bank and on production of relevant documents and after deducting Liquidated Damages (if Any). |
| | **20% of Table C in Appendix II** | On successful go-live of the proposed solution and on submission of Invoice and Acceptance/Sign off by the Bank and on production of relevant documents and after deducting Liquidated Damages (if Any). |
| | **10% of Table C in Appendix II** | On completion of warranty period or on submission of BG for the equivalent amount and after deducting Liquidated Damages (if Any). |
| **License Cost** | **80% of Table A in Appendix II** | Upon successful Supply, Installation, Integration, Implementation of the respective modules, the Bidder shall submit an invoice along with an installation report. These documents must be accepted and signed off by the Bank. Payment will be made after relevant documents are reviewed and any applicable penalties or liquidated damages, if any, are deducted. |
| | **20% of Table A in Appendix II** | On final sign off and Go-live of the respective module, the Bidder shall submit an invoice along with an installation report. These documents must be accepted and signed off by the Bank. Payment will be made after relevant documents are reviewed and any |

| | | |
|---|---|---|
| | | applicable penalties or liquidated damages, if any, are deducted. |
| **Implementation & Integration Cost** | **50% as per Table B of Appendix II** | On successful completion of Milestone 2 – "Implementation and integration of Software" and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any). |
| | **20% as per Table B of Appendix II** | On submission and acceptance of final Documentation (SOPs, Manuals, Reports, etc.), Milestone 3 -Trainings and Knowledge Transfer and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any). |
| | **30% as per Table B of Appendix II** | On successful implementation and Milestone – 4 Go-live of solution and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents and after deducting Liquidated Damages (if Any). |
| **Post Go-Live Support** | Payment will be Quarterly in arrears and after deducting applicable penalties and Liquidated damages (if Any) as per Table-D of Appendix II | |

Note: Successful Completion refers to the sign off from the Bank.

- The Bank shall pay each undisputed invoice raised in accordance with this RFP and subsequent agreement, within thirty (30) Working Days after its receipt unless otherwise mutually agreed in writing, provided that such invoice is dated after such amount have become due and payable under this RFP and subsequent agreement.
- Any objection / dispute to the amounts invoiced in the bill shall be raised by the Bank within reasonable time from the date of receipt of the invoice. Upon settlement of disputes with respect to any disputed invoice(s), the Bank will make payment within thirty (30) Working Days of the settlement of such disputes.
- All out of pocket expenses, traveling, boarding and lodging expenses for the entire Term of this RFP and subsequent agreement is included in the amounts and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out of pocket expenses, including travel, boarding and lodging etc.
- The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, etc. but exclusive of only applicable GST, which shall be paid / reimbursed on actual basis on production of bills with GSTIN. 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, increase in custom duty. The bank will not pay any out-of-pocket expense.

### 4.8 Change Orders

- The Bank may at any time, by a written order given to the bidder make changes within the general scope of the Contract in any one or more of the following:
  a. the place of delivery; and / or
  b. the Services to be provided by the Supplier;

If any such change causes substantial increase or decrease in the cost of, or the time required for, the Bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the bidder's receipt of the Bank's change order.

### 4.9 Service Level Agreement (SLA)

The supplier shall be required to sign Service Level Agreement (SLA) covering all terms and conditions of this RFP and Purchase Order within 15 days from the date of acceptance of purchase order.

SLA format will be shared with the Successful bidder along with Purchase order.

### 4.10 Human Resource Requirements

The bidder to ensure that experienced resources (with both functional and technical expertise on the project domain and solutions used to implement the project) are assigned and available in the project throughout the project lifecycle.

The selected bidder shall confirm that every person deployed by them on the project has been vetted through a third-party background check prior to their engagement. The bidder shall manage the activities of its personnel or others engaged in the project, etc. and shall be accountable for all the personnel deployed/engaged in the project. Bidder to provide the profile and list of the resources working on the project after kickoff meeting. Any change in the resources during the project shall be with the permission of the bank and it will be the responsibility of the bidder to ensure that a replacement resource is assigned and available in the project with similar experience and sufficient knowledge transfer is carried out to ensure smooth functioning of the project. In case of any such events leading to deficiency in the project deliverables / functioning, the same will be treated as lack of performance on part of bidder.

Throughout the lifecycle of the project, resources shall be available onsite on all days. The successful bidder shall be the principal employer of the employees, agents, contractors, etc., engaged by them and shall be vicariously liable for all the acts, deeds, matters or things, of such persons whether the same is within the scope of power or outside the scope of power, vested under the contract.

The successful bidder shall agree to hold the bank, its successors, assigns and administrators fully indemnified and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the bank through the action of supplier's employees, agents, contractors, etc.

### 4.11 Installation Requirements

The bidder shall install and commission all supplied hardware and system software at the Bank's designated locations, including DC/DR and any approved non-production sites, and shall ensure readiness of racks, network dependencies, power, firmware, drivers, and installation documentation.

The bidder shall test all software operations and accomplish all adjustments necessary for successful and continuous operation of the software solution at all installation sites.

### 4.12 Maintenance

The Successful Bidder must provide uninterrupted availability of the enterprise data privacy governance & compliance platform and ensure that the problem is resolved within the time schedule as prescribed in the RFP.

Also, the successful bidder agrees to maintain the entire supplied enterprise data privacy governance & compliance platform, on 24x7x365 basis to ensure meeting the terms of the RFP. For any major breakdown such as application crash, the successful bidder must arrange for immediate onsite support for recovery and resumption of operations. During the contract period, all updates and upgrades should be free and must be implemented without any additional cost to the bank.

In case the successful bidder is not the OEM of the solution offered, then the solution supplied by the successful bidder must be maintained under back-to-back support from the respective OEMs and the versions installed must not be end of life / support.

### 4.13 Contract Period

The contract period will commence from the date of Releasing the PO and will be valid up to a period of implementation time plus 3 years. The contract is extendable / renewable further for 2 years at the option of the Bank on mutually agreed terms.

### 4.14 Sub-Contracting

The successful bidder will not subcontract or delegate or permit anyone other than the bidders' personnel to perform any of the work, service or other performance required of the supplier under this agreement without the prior written consent of the Bank. Bank at its own discretion may permit or deny the same. The selected bidder should abide by guidelines issued by RBI Master Direction on Outsourcing of IT Services.

### 4.15 Insurance

The Service Provider may be required to take adequate insurance cover against all kinds of risks including fidelity clause for the loss arising from acts of omission/ commission/ dishonesty of its employees and / or agents and would be required to keep the insurance policy alive at all times during the currency of the agreement. Bidder should have cyber insurance policy to cover first party and third-party liability coverage to organization when cyber risk materializes and / or cyber security controls at organization fails. The coverage established by the cyber insurance shall cover property, theft and network level security.

### 4.16 Place of Delivery

All supplied hardware shall be delivered to Bank-designated data centre / disaster recovery / other approved locations as specified in the Purchase Order or implementation plan.

### 4.17 Delivery and Documents

Delivery of the goods and services shall be made by the Supplier in accordance with the terms specified in the schedule of requirements. The details of shipping and / or other documents to be furnished by the Supplier are as follows:

(i) Copy of the Supplier Invoice showing contract number, description, quantity, unit price, total amount.

(ii) Manufacturer's / Supplier's Warranty Certificate.

(iii) License Certificates.

### 4.18 Delays in the Bidder's Performance

Delivery of the Goods and performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Purchaser in the Schedule of Requirements.

If at any time during performance of the Contract, the Supplier or its duly permitted subcontractor(s) should encounter conditions impeding timely delivery of the Goods and performance of Services, the Supplier shall promptly notify the Purchaser in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, the Purchaser shall evaluate the situation and may at its discretion extend the Supplier's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties in writing and the same shall be deemed to be an amendment of the Contract.

### 4.19 Jurisdiction and Applicable Law

The Contract shall be interpreted in accordance with the laws of India. Any dispute arising out of this contract will be under the jurisdiction of Courts of Law in Chennai. Compliance with labour and tax laws, etc. will be the sole responsibility of the service provider at their cost.

### 4.20 Liquidated Damages (LD)

The successful bidder must strictly adhere to the schedules for completing the assignments. Failure to meet these Implementation schedules, unless it is due to reasons entirely attributable to the bank, may constitute a material breach of the bidder's performance. In the event that the Bank is forced to cancel an awarded contract (related to this RFP) due to the successful bidder's inability to meet the established delivery dates, the purchaser may take suitable penal actions deemed fit in addition to invocation of performance guarantee. Delay beyond the implementation schedule/ scope of RFP, the supplier shall be liable to forfeit 0.5% of the cost of the deliverables for the respective implementation phase, as per the project implementation timelines mentioned in RFP for every week or part thereof subject to maximum of 10% of cost of project for the delay solely not attributable to purchaser. Once the Liquidated Damages (LD) crosses 10% of the cost of the project, Bank reserves the right to terminate the contract.

### 4.21 Service Level Criteria

- The Bidder shall be bound by the Service Levels described in this document. Successful Bidder shall have to enter into "Service Levels Agreement" with Bank covering all terms and conditions of this tender while providing the service support and onsite support. Once go live of application, the services should be available on 365X24x7 basis and hence any technical problem should be resolved as per the response Time Matrix given below.
- Bidder is expected to respond and resolve issue within prescribed time frame based on the severity description decided by bank mentioned above and needs to strictly adhere to Service Level Agreement (SLA). The SLA will be reviewed on a monthly basis.
- Penalties will be applicable due to downtime of Infra and software application. "System downtime" subject to the Service Level requirement (SLR), means accumulated time during which the System is not available to the Bank's users or customers due to in-scope system failure, and measured from the time the Bank and/or its customers log a call with the Bidder of the failure or the failure is known to the Bidder from the availability measurement tools to the time when the System is returned to proper operation. Availability commitments shall apply to the complete supplied solution stack, including bidder-supplied hardware, operating systems, databases, middleware, and application components. The bidder shall define and commit to incident response, restoration, replacement, and escalation timelines for failed hardware components affecting availability, performance, or security.
- Any failure of supplied hardware resulting in breach of uptime or service levels shall be treated as bidder responsibility and shall be remediated without additional cost to the Bank.
- Any denial of service to the Bank users and Bank customers would also account as "System downtime". If any significant part of the solution or cluster is unavailable or inaccessible or unresponsive to end users, it will be considered down-time. The Bank's decision will be final in determining downtime.
- "Incident" refers to any event / abnormalities in the functioning of the equipment / specified services that may lead to deterioration, disruption in normal operations of Banks services.
- "Resolution Time" shall mean the time taken in resolving (diagnosing, trouble shooting and fixing) an incident after it has been reported to the selected bidder through verbal/email/phone/SMS/other electronic form. The resolution time shall vary based on the category of the incident reported at the service desk.
- Response Time: Maximum Response Time for Remedial Maintenance under the CONTRACT is measured in elapsed coverage hours from the time a service request is received to the time THE VENDOR's customer engineer arrives at Bank Site.
- Total down time in a month would be summation of non-concurrent down time of individual systems
- The business hours in the offices are 7:00 hours to 23:00 hours, 7 days a week including holidays.
- Any technical glitch/ issue in installed infrastructure of the solution (i.e. System and software, OS/DB etc.) should be attended on priority and should be covered under warranty/AMC.
- For penalty calculation, the total time elapsed between the intimation of break down message from Bank side to the vendor and receipt of rectification message from the Bidder to Bank side will be considered. During the warranty period, the penalty will be deducted in quarterly FMS payment. In case, Bank is unable to adjust penalty in FMS payment, the Bank at its discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.
- Post warranty period, the penalty will be deducted in ATS/AMC or Any other payment. In case, the Bank is unable to adjust penalty in AMC/ATS payment, the Bank at its discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.

- If any critical component of the entire configuration setup is out of service, then the Bidder & OEM shall either immediately replace the defective unit (with new one) or replace it at its own cost or provide a standby, on immediate basis, not more than 4 hours, the Bidder should maintain proper inventory of standby components for early resolution of issues. The Bidder should comply with the security and audit standards of the Bank and various regulatory guidelines. For this, the Bidder should apply new patches related to OS/ firmware & BIOS updates etc. without any additional cost to the bank, during the contract period.
- Replacement/ Repair of faulty part of provided in scope items -All defective parts/ faulty shall be replaced as part of maintenance at no additional cost by the Bidder. Replacement parts shall be new part from the same manufacturer(s) (OEM). Whether a defective item or component is to be replaced or repaired shall be at the sole discretion of the bank. The Recovery Point Objective (RPO) is 2 hours and Recovery Time Objective (RTO) is 15 minutes. The SI must ensure that there is 'Zero Data Loss'.
- Integration with all IT/ Security Solutions procured by the Bank as per RBI Guidelines time to time; along with integration with any solutions / product / application without any additional cost to the bank. The Successful Bidder shall provide, as part of monthly evaluation process, reports to verify the Successful Bidder performance and compliance with the SLRs
- Bank will provide 3 months of stabilization period after Go-Live after which the service level will be applicable to the bidder. During this stabilization period penalty apart from the "Resource Deployment, Replacement/Absence" will be applicable

### 4.21.1 Availability / Uptime

- Availability requirement mentioned below refer to the availability of the solutions at the Data Centre and Disaster Recovery center.
- Availability refers to the business system being up, running and actively processing transactions without dropping/rejecting any requests from users, customers or external entities. In case of business systems being partially up (i.e. accepting some transactions and rejecting others), the particular business system would be considered NOT available for calculation of Availability Service Level Requirement compliance. Data centre / Disaster recovery centre availability (%) = (Total minutes during the month – Planned down–time - Downtime minutes during the month) *100 / Total minutes during the month • Total Time shall be measured on 24x7 basis.
- Planned data centre Downtime refers to unavailability of data centre services due to infrastructure maintenance activities such as configuration changes, upgradation or changes to any supporting infrastructure. Details related to such planned outage shall be agreed with the data centre. Compliance to this SLR would be measured on a monthly basis. Bidder will be responsible for providing Resolution / Fix for the reported incident but not limited to, and replacement of any faulty or defective infrastructure component / software within the specified timeline or the one that will be mutually agreed between the bidder and Indian Bank. Failure to render such support within specified timeline will incur penalty as specified below:

| Availability and Uptime Service Level Penalty Matrix | | |
|---|---|---|
| **Service level Objective** | **Target** | **Penalty** |
| Availability | Where Uptime above 99.90% | Nil |
| | Where Uptime between 99.00% - 99.90% | Rs.50,000/- for every 0.25% of default below 99.90% |

| | | |
|---|---|---|
| | | or part thereof |
| | Where Uptime between 98.0%-99.0% | Rs. 1,00,000 + Rs.50,000/- for every 0.25% of default below 99.0% |
| | Where the uptime is below 98.0% | No AMC/ATS charges will be paid for that month |
| | On those days where the downtime exceeds 60 minutes (either continuously or total) | Additional Rs.25,000/- will be charged on those days |

### 4.21.2 Resource Deployment / Replacement / Absence

- Attendance register will be maintained by the bank team. Based on attendance, AMC/ATS cost will be paid. Bank may deduct the AMC/ATS cost on per day basis for the absence beyond the permitted days/leaves.
- Bank may allow 12 days casual leave & 12 days of sick leave in a year to Bidder Team members, however, for the critical application, vendor should replace with suitable Bidder's Team members for the same. Bank has the right to interview the proposed resource and if found not satisfactory then bidder need to provide a alternative resource as per the satisfaction of the Bank. If the Bidder has to replace the resource working on the Bank project for any reason, the Bidder should make necessary provision to provide the new resource of equivalent or higher skillset. Bank has the right to interview the proposed resource and if found not satisfactory then bidder need to provide a alternative resource as per the satisfaction of the Bank. There should be a handover period of 1 month for L1 resource, 45 days from L2 resource and 60 days for any other resource. If Bidder fails to make provision or replace, the penalty would be computed at the rate of 0.5% of the total monthly cost for that respective resource, for every day of delay/absence. If Bidder fails to make adequate handover period, the penalty would be computed at the rate of 0.5% of the total monthly cost for that respective resource on prorate bases for shorter handover period. In case of resource replacement, the Bidder has to inform 30 days in-advance to the bank about the replacement. The Bidder shall deploy the required resources as per scope under AMC/ATS at Bank centralized locations. If the Supplier fails to deploy the resources within the time period specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct a sum equivalent to 0.5% per week of the total AMC/ATS cost for each week or part thereof of delay, until actual delivery subject to maximum deduction of 10% of the total price of the Facility Management Support.

**Note:** The Bank reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the Monthly payouts and the cap on Monthly penalty will be 15% of the Monthly payout. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a maximum of 10% of the overall contract value. and thereafter, Bank has the discretion to cancel the contract.

**Note:** The selected bidder will be required to sign the formal agreement/contract/ Service Level Requirement with the Bank within 15 days of the acceptance of the LOI/ Purchase Order. After issuance of PO/LOI, terms of RFP and Purchase Order/LOI shall be binding and act as contract. The draft format of SLRs will be provided after acceptance of the LOI/ Purchase Order by the successful bidder. IT Service Desk / Helpdesk and Facility Management Service level Bidder must provide root-cause analysis report (RCA report) and action taken report (ATR) within 5 working days of the issue closure for closure of any ticket. No ticket shall be considered closed without these reports. The RCA report and the ATR would be subject to scrutiny by the Bank. Bidder must close any queries or concerns raised by the Bank on the RCA or ATR in a satisfactory manner. Number, format and frequency of project governance reports of helpdesk activity will be decided later in consultation with the Bank. Compliance to this SLR would be measured monthly.

| Severity level | Severity level Description | Target Response Time | Target Resolution Time |
|---|---|---|---|
| Priority 1 (Critical) | • Any problem due to which users cannot access the proposed solution or infrastructure, or the proposed solution is unavailable for use or any problem due to which the proposed solution does not perform according to the defined performance and query processing parameters required as per the RFP.<br>• Showstoppers involve major functional failure in the application, where there are no usable workarounds.<br>• Priority Level 1 Incident will take precedence over all other non-Priority Level 1 Incidents. | Response time should be 30 Minutes during business and non-business hours of the incident being logged. | During business hours, within 2 hours of incident being logged and during non-business hours, within 3 hours of incident being logged. |
| Priority 2 (High) | • Any incident which could have been classified as "Critical" but for which an acceptable workaround has been provided by the Bidder or any problem due to which the proposed solution produces does not perform according to the defined performance and query processing parameters required as per the RFP or users face severe functional restrictions in the application due to partial failure, irrespective of the cause. | Response time should be 60 minutes during business and non-business hours of the incident being logged. | During business hours, within 3 hours of incident being logged and during non-business hours, within 5 hours of incident being logged. |
| Priority 3 (medium) | • Any other incident causing a partial disruption of service or incorrectness of results or moderate functional restrictions in the application irrespective of the cause, which have a convenient and readily available workaround. | Response time should be 120 minutes during business and non-business hours of the incident being logged. | During business hours, within 4 hours of incident being logged and during non-business hours, within 6 hours |

| | | | |
|---|---|---|---|
| | | | of incident being logged. |

**Penalty of Rs.10, 000/- shall be charged for every non-conformance with the service response and resolution timetable above.**

### 4.22 Bank's right to accept or reject any bid or all bids

- The Bank reserves the right to accept or reject any bid/all bids or annul the bidding process at any time before awarding the contract, without incurring any liability to the affected Bidder or Bidders.
- Bank reserves the right to modify the terms and conditions of this RFP duly informing the same before the due date of submission of bids & publishing the same on Bank Website and GEM portal.

### 4.23 Performance Bank Guarantee

a. The Performance Bank Guarantee shall cover the complete scope of hardware, software, implementation, integration, warranty, and support obligations under the RFP.
b. The bidder shall maintain adequate insurance coverage for supplied hardware, transit risk, installation risk, and operational liability as applicable for the contract period
c. Within 15 days of acceptance of Purchase Order, the successful bidder shall furnish to the Bank the Performance Security equivalent to 5% of the contract value in the form of a Bank Guarantee, valid for 38 months with further three-months claim period, in the format enclosed **(Annexure-IV).** Relaxation if any, extended by GOI/ competent authorities for furnishing PBG shall be passed on to eligible bidders.
d. The performance security submitted by the successful bidder shall be invoked by the Bank as compensation for any loss resulting from the bidder's failure in completing their obligations under the Contract.
e. The performance security will be discharged by the Bank and returned to the successful bidder not later than thirty (30) days following the date of completion of the successful bidder's performance obligations under the Contract.
f. Failure of the successful bidder to comply with the requirement of signing of contract and performance security shall constitute sufficient grounds for annulment of the award and forfeiture of the bid security, in which event the Bank may call for new bids.

### 4.24 Limitation of Liability

Successful bidders' aggregate liability under the contract shall be at actual and limited to a maximum of the contract value. For the purpose for the section, contract value at any given point of time means the aggregate value of the purchase orders placed by bank on the vendor that gave rise to claim, under this tender.

This limit shall not apply to third party claims for

a. IP Infringement indemnity
b. Bodily injury (including death) and damage to real property and tangible property caused by vendor/s' gross negligence. If a third party asserts a claim against bank that a vendor

product acquired under the agreement infringes a patent or copy right, vendor should defend bank against that claim and pay amounts finally awarded by a court against bank or included in a settlement approved by vendor**.**

c. In case, any personal information of the customer is required to be shared to the vendor in course of the proposed services, to protect against any liability arisen on account of breach, the said event may be considered for addition under this exemption from application of limitation of liability.

### 4.25 Indemnity Clause

If at the time of the supplying, installing the hardware / software in terms of the present contract/ order or subsequently it appears at any point of time that an infringement has occurred of any patents, trademarks or other rights claimed by any third party in India or abroad, then in respect of all costs, charges, expenses, losses and other damages which the Bank may suffer on account of such claim, the supplier shall indemnify the Bank and keep it indemnified on that behalf.

In case of data breach solely and directly attributable to Service Provider in view of the Bank (which is final and binding), the Service provider should indemnify Bank for all its acts and omissions. Any penalty imposed on Bank by regulatory / statutory bodies related to data security on cloud due to reasons stated in forgoing para**,** will be passed on to the service provider

### 4.26 Disclaimer

The Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

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

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

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

The Supplier shall indemnify the Bank against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods or software or hardware or any part thereof.

### 4.27 IT Act 2000

The equipment's to be quoted as per this tender should comply with the requirements under Information Technology (IT) Act 2000 and subsequent amendments and related Government/Reserve Bank India guidelines issued from time to time.

### 4.28 Intellectual Property Rights (IPR)

While the successful bidder/ OEM shall retain the intellectual property rights for the application software, it is required that successful bidder shall grant Enterprise / Core based/ user-based annual subscription License to the bank for the bank's exclusive use without limitation on the use of those licenses.

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

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

In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, bidder shall at its choice and expense: [a] procure for Bank the right to continue to use such deliverables; [b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; or [c] if the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse bank for any amounts paid to bidder for such deliverables, along with the replacement costs incurred by Bank for procuring an equivalent equipment in addition to the penalties levied by Bank. However, Bank shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the bidder shall be responsible for payment of penalties in case service levels are not met because of inability of the bank to use the proposed product. The indemnification obligation stated in this clause apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby. The bidder acknowledges that business logics, workflows, delegation and decision-making processes of Bank are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors.

### 4.29 Acceptance of Purchase Order.

Acceptance of purchase order should be submitted within 15 days of issuance of purchase order along with authorization letter. If for any reason H1 bidder backs out after issuance of purchase order or the purchase order issued to the H1 bidder does not get executed in part / full, Bank shall invoke performance bank guarantee and blacklist the bidder for a period of one year.

### 4.30 Signing of Contract Form, NDA, SLA and Submission of Proof of Customized Source Code Audit

Within fifteen (15) days of acceptance of Purchase Order, the successful bidder shall sign the contract form (Annexure-III), Non-Disclosure Agreement (Annexure-VII) and Service Level Agreement and return it to the Bank. Pre-Contract Integrity Pact (Annexure-VI) executed between the Bank and successful bidder(s) is deemed to be a part of the contract.

Successful bidder has to submit the proof of customized source code (related to Bank) audit (Annexure-XI) as per timeline and periodicity defined by the Bank that the code developed is free from any known vulnerabilities and standard coding practice including proper version control is followed during development of the code.

### 4.31 Settlement of Disputes

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

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

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

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

a) In case of dispute or difference arising between the Bidder and the Bank relating to any matter arising out of or connected with the agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996.
b) The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the bidder and the bank; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator.
c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.
d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation,

presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

e) Where the value of the contract is Rs. 10 million and below, the disputes or differences arising shall be referred to the Sole Arbitrator.

f) Notwithstanding any reference to arbitration herein,

   a. the parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and

   b. the Bank shall pay the supplier any monies due to the supplier.

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

### 4.32 Authorization Letter from OEM

The bidder has to obtain and submit Authorization letter from Original Equipment Manufacturer (OEM) as per **Annexure-V**. If bidder is an OEM and they quote their own product, then MAF (Manufacturer's Authorization Form) need not be submitted but document related to IP rights of the products needs to be submitted.

### 4.33 Coverage of Successful Bidder under the EPF & MP Act 1952 Employees' Provident Funds and Miscellaneous Provisions Act, 1952/ Code of Social Security, 2020

The Successful bidder has to submit necessary details of all the outsourced employees for any type of services engaged either through contractors or directly whenever required by the Bank. If engaged through contractors, list of all the contractors engaged for any/all services and whether the said contractors are covered independently under the EPF & MP Act 1952/ Code of Social Security, 2020 is to be submitted on the Bank's request. The agreement of contracts with the contractors, the PF code number of the contractors, if covered, the attendance of the contract employees, the remitted PF challan with the Electronic Challan cum Return (ECR) should be submitted on the Bank's request.

**Minimum Wages Act/ Code of Wages, 2019**

As per Government (Central / State) Minimum Wages Act in force, it is imperative that all the employees engaged by the bidder are being paid wages / salaries as stipulated by government in the Act. Towards this, Successful Bidder shall submit a confirmation as per format provided in **Annexure XVI** of the RFP.

### 4.34 Exit Requirements

In the event of Agreement comes to end on account of termination or by the expiry of the term / renewed term of the Agreement or otherwise, the Supplier shall render all reasonable assistance and help to the Bank and to any new vendor engaged by the Bank, for the smooth switch over and continuity of the Services. Bidder needs to factor at least 3 months of reverse transition period in which bidder needs to provide all the SOP and environment related document to the Bank/new vendor. Bidder needs to work as a showdown of the Bank/new vendor during the last 1 month of the reverse transition. All the applicable SLA will be levied during the reverse transition period. Bank will be paying the bidder as per the FM/ATS/AMC amount quoted in the RFP during the period.

### 4.35 Termination for Default

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

a. if the successful bidder fails to deliver any or all of the Goods and Services within the period(s) specified in the Contract, or within any extension thereof granted by the Purchaser.

b. if the successful bidder fails to perform any other obligation(s) under the Contract.

c. If the successful bidder, in the judgement of the Purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

d. In case of successful Bidders revoking or cancelling their Bid or varying any of the terms in regard thereof without the consent of the Bank in writing.

'For the purpose of this clause:

**"Corrupt practice**" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution; and

"**Fraudulent practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

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

### 4.36 Termination for Convenience

Bank, by 90 days' written notice sent to the Successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the bank's convenience, the extent to which the performance of the Successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.
The Goods that are complete and ready for shipment within ninety (90) days after the Supplier's receipt of notice of termination shall be accepted by the Purchaser at the Contract terms and prices. For the remaining Goods, the Purchaser may elect:

a. to have any portion completed and delivered at the Contract terms and prices; and / or
b. to cancel the remainder and pay to the Supplier an agreed amount for partially completed Goods and Services and for materials and parts previously procured by the Supplier.

### 4.37 Force Majeure

The Successful bidder shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure. For purposes of this clause, "Force Majeure" means an event beyond reasonable control of the Successful bidder and not involving the Successful bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes. Delay by sub suppliers of vendor to Vendor will not be considered as cause of force Majeure.
If a Force Majeure situation arises, the Successful bidder shall promptly notify the Bank in writing of such condition and the cause thereof but in any case, not later than 10 (Ten) days from the moment of their beginning. Unless otherwise directed b
the Bank in writing, the Successful bidder shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

If the impossibility of complete or partial performance of an obligation lasts for more than 6 (six) months, either party hereto reserves the right to terminate the contract totally or partially upon giving prior written notice of 30 (thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the goods received or complete transition / handover to the in-coming Vendor / Service Provider**.**

### 4.38 Confidentiality

The supplier will be exposed to internal business information of the Bank, affiliates, and / or business partners by virtue of the contracted activities. The Bidder / their employees shall treat all data & information collected from the Bank during the project in strict confidence. The Bank is expected to do the same in respect of Bidder provided data / information. ***After termination of the contract also the successful bidder / supplier shall not divulge any data/ information collected from the Bank during the project.***

The supplier will have to enter into a Non-Disclosure agreement (Annexure-VII) with the Bank to safeguard the confidentiality of the Bank's business information, legacy applications and data.

The successful bidder and its employees either during the term or after the expiration of this contract shall not disclose any proprietary or confidential information relating to the project, the services, this contract, or the business or operations without the prior written consent of the Bank.

The successful Bidder and its employees 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 successful Bidder under this contract or existing at any Bank location. The successful Bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The successful Bidder shall also ensure that all permitted 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 successful Bidder under this contract or existing at any Bank location. Negligence in connection with the work or contravenes the provisions of other Terms, if the successful bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the successful bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the successful bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the successful bidder.

### 4.39 Amalgamation

If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the obligations of the Service Provider under this RFP. In such case, decision of the new entity will be binding on the successful bidder.

### 4.40 Inspections and Tests

It shall be the responsibility of the bidder to successfully conduct and conclude acceptance tests for all hardware and software components delivered under this RFP. The bidder shall demonstrate all required features and capabilities of the respective hardware and software items during acceptance testing.

Acceptance testing shall be conducted only after all hardware and software have been successfully supplied, installed, configured, and made ready across the applicable environments. If any hardware and/or software component fails acceptance testing, the bidder shall rectify the defect within the Bank-defined timeline or replace the component at no additional cost to the Bank.

No component shall be considered accepted unless formal sign-off is issued by the Bank after successful completion of acceptance tests

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

Any charges payable to the Purchaser's representative designated for inspection shall be borne by the Purchaser.
The Purchaser's right to inspect, test and, where necessary, reject the Goods or software after the delivery shall in no way be limited or waived by reason of the software having previously been inspected, tested and passed by the Purchaser.

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

All the clauses specified under this point shall be applicable and extended to any entity to which the bidder has outsourced any part (if allowed by the Bank) of the prescribed activity under any of the modules proposed. It shall be the responsibility of the bidder to ensure unrestricted access to the authorities/officials as mentioned above to the places where such services

re outsourced, for inspection and verification.

### 4.41 Use of Contract Documents and Information

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

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

### 4.42 Pre-Contract Integrity Pact

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

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

**Adoption of Pre-Contract Integrity Pact**

- The Pact essentially envisages an agreement between the prospective bidders and the Bank, committing the persons /officials of both sides, not to resort to any corrupt practices in any aspect/ stage of the contract.
- Only those bidders, who commit themselves to the above pact with the Bank, shall be considered eligible for participate in the bidding process.
- The Bidders shall submit signed Pre-Contract integrity pact as per the Annexure-VI. Those Bids which are not containing the above are liable for rejection.
- Foreign Bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principles or associates.
- Bidders to disclose the payments to be made by them to agents/brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.

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

- The Pre-Contract Integrity Pact Agreement submitted by the bidder during the Bid submission will automatically form the part of the Contract Agreement till the conclusion of the contract i.e. the final payment or the duration of the Warranty /Guarantee/AMC if contracted whichever is later. Integrity Pact, in respect of a particular contract would be operative stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings. Pre-Contract Integrity Pact shall be signed by the person who is authorized to sign the Bid. The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

| |
|---|
| 1. Shri. M J Joseph<br>Email: mohan.joseph@gmail.com<br><br>2. Shri. Shri Manoj Pant<br>Email: mpant2007@gmail.com |

- Change of law / policy / circular relating to Pre-Contract Integrity Pact vitiate this agreement accordingly with immediate effect on written intimation.

- Any violation of Pre-Contract Integrity Pact would entail disqualification of the bidders and exclusion from future business dealings, as per the existing provisions of GFR, 2017, Prevention of Corruption Act (PC Act), 1988 or other Financial Rules as may be applicable to the organization concerned.

## 4.43 GENERAL TERMS AND CONDITIONS

### 4.43.1 Rejection of Bids

The Bank reserves the right to reject the Bid if,

i. Bidder does not meet any of the pre-bid eligibility criteria mentioned above including non-payment of the bid cost.

ii. The bid is incomplete as per the RFP requirements.

iii. Any condition stated by the bidder is not acceptable to the Bank.

iv. If the RFP and any of the terms and conditions stipulated in the document are not accepted by the authorized representatives of the bidder.

v. Required information not submitted as per the format given.

vi. Any information submitted by the bidder is found to be untrue/fake/false.

vii. The bidder does not provide, within the time specified by the bank, the supplemental information / clarification sought by the bank for evaluation of bid.

viii. If bidder does not submit the dully signed compliance statement Annexure XVIII

The Bank shall be under no obligation to accept any offer received in response to this RFP and shall be entitled to reject any or all offers without assigning any reason whatsoever. The Bank may abort entire process at any stage without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for Bank's action.

In order to promote consistency among the Proposals and to minimize potential misunderstandings regarding how Proposals will be interpreted by the Bank, the format in which Bidders will specify the fundamental aspects of their Proposals has been broadly outlined in this RFP.

Any clarifications to the RFP should be sought by email as per the dates mentioned in **"Schedule [A] Important Dates"**. Responses to the queries will be uploaded on Bank's website. Bank will hold a pre-bid meeting, to answer all the questions / queries received by email which would also be uploaded on bank's website.

Proposals received by the Bank after the specified time on the last date shall not be eligible for consideration and shall be summarily rejected.

In case of any change in timeline, the same shall be updated on the Bank's website and shall be applicable uniformly to all bidders.

### 4.43.2 Representation and Warranties

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

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

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

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

iv. That there are –

(a) no legal proceedings pending or threatened against Bidder or any sub-Bidder/third party or its team which adversely affect/may affect performance under this Contract; and

(b) no inquiries or investigations have been threatened, commenced or pending against Bidder or any sub-Bidder / third part or its team members by any statutory or regulatory or investigative agencies.

v. That the Bidder is validly constituted and has the corporate power to execute, deliver and perform the terms and provisions of this Contract and has taken all necessary corporate action to authorize the execution, delivery and performance by it of the Contract.

vi. That all conditions precedent under the Contract has been complied.

vii. That neither the execution and delivery by the Bidder of the Contract nor the Bidder's compliance with or performance of the terms and provisions of the Contract:

a) will contravene any provision of any applicable law or any order, writ, injunction or decree of any court or government authority binding on the Bidder,
b) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a Party or by which it or any of its property or assets is bound or to which it may be subject or
c) Will violate any provision of the Memorandum and Articles of Association of the Bidder.

viii. That the Bidder certifies that all registrations, recordings, filings and notarizations of the Contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the Bidder which is necessary to ensure the legality, validity, enforceability, or admissibility in evidence of the Contract have been made.

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

x. That the Bidder owns or has good, legal or beneficial title, or other interest in, to the property, assets and revenues of the Bidder on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.

xi. That the Bidder owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all Intellectual Property Rights, which are required or desirable for the project and the Bidder does not, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. None of the Intellectual Property or Intellectual Property Rights owned or enjoyed by the Bidder or which the Bidder is licensed to use, which are material in the context of the Bidder's business and operations are being infringed nor, so far as the Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property or Intellectual Property Rights licensed or provided to the Bidder by any person. All Intellectual Property Rights (owned by the Bidder or which the Bidder is licensed to use) are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required to maintain the same in full force and effect have been taken thereon and shall keep the Bank indemnified in relation thereto.

xii. Any intellectual property arising during the course of the execution under this contract related to tools/ systems/ product/ process, developed with the consultation of the bidder will be intellectual property of the Bank.

#### 4.43.3 Relationship of Parties

i. Nothing in this Contract constitutes any fiduciary relationship between the Bank and Bidder/Bidder's Team or any relationship of employer – employee, principal and agent, or partnership, between Indian Bank and Bidder and /or its employees.

ii. No Party has any authority to bind the other Party in any manner whatsoever, except as agreed under the terms of the Contract.

iii. Indian Bank has no obligation to the successful Bidder, except as agreed under the terms of the Contract.

iv. All employees/personnel/ representatives/agents etc., engaged by the Successful Bidder for performing its obligations under the Contract/RFP shall be in sole employment of the Successful Bidder and the Successful Bidder shall be solely responsible for their salaries, wages, statutory payments etc. Under no circumstances, shall Indian Bank be liable for any payment or claim or compensation (including but not limited to any compensation on account of any injury / death / termination) of any nature to the employees/personnel/representatives/agent etc. of the Successful Bidder.l

v. The Successful Bidder shall disclose to Indian Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Successful Bidder or its team/agents/representatives/personnel etc.) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

vi. The Successful Bidder shall not make or permit to be made a public announcement or media release about any aspect of the Contract unless Indian Bank first gives the Successful Bidder its prior written consent.

#### 4.43.4 No Right to Set Off

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

#### 4.43.5 Publicity

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

#### 4.43.6 Conflict of Interest

The Bidder shall disclose to the Bank in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the services / appointment as soon as practical after it becomes aware of that conflict.

### 4.43.7 Solicitation of Employees

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

a) recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or

b) induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

Notices and Other Communication:
A notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be sent personally or by certified or registered post with acknowledgement due or overnight courier or email duly transmitted, addressed to the other party at the addresses, email given in the contract.
Notices shall be deemed given upon receipt, except that notices sent by registered post in a correctly addressed envelope shall be deemed to be delivered within 5 working days (excluding Sundays and public holidays) after the date of mailing dispatch and in case the communication is made by email, on business date immediately after the date of successful email. (that is, the sender has a hard copy of the page evidencing that the email sent to correct email address).

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

### 4.43.8 Substitution of Team Members

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

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

### 4.43.9 Right to alter Quantities

Bank reserves the right to alter the requirements specified in the RFP. The Bank also reserves the right to delete one or more items from the list of items specified in the RFP. The Bank will inform all Bidders about changes, if any.

The Bidder agrees that Bank has +/- 25% limit on the additions or deletions on the items. The bidder agrees that

1. Increase upto 25% on the items is applicable at the time of placing order with the bidder or till the delivery of the initial order is completed.
2. Decrease upto 25% on the items is applicable at the time of placing order with the bidder.

Further the Bidder agrees that the prices quoted by the Bidder would be adjusted on prorate basis with such additions or deletions in quantities. The Unit price quoted by the Bidder will be valid for all the items, and the Bank reserve the right to procure the additional items within the specified limit as per the unit price mentioned in the bill of material.

**4.43.10 Severability**

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

**4.43.11 Notices and Other Communication**

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

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

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

**4.43.12 Other Terms and Conditions**

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

b. Successful Bidder/ OEM shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the successful Bidder / OEM and shall be liable for all the acts, deeds, matters or things of such persons whether the same is within the scope of power or outside the scope of power, vested under the contract. No rights of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc., by the successful Bidder/OEM, for any assignment under the contract. All remuneration, claims, wages, dues, etc., of such employees, agents, contractors, subcontractors, etc., of the successful Bidder/OEM shall be paid by the successful Bidder/OEM alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the successful Bidder's/OEM's employees, agents, contractors, subcontractors, etc.,

c. The Successful Bidder/OEM shall agree to hold the Bank, its successors, assigns and Administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of Successful Bidder/OEM's employees, agents, contractors, subcontractors etc.

d. The cost of preparing the proposal, including visits to the Bank by the Bidder, is not reimbursable.

e. All pages of the Bid Document, Clarifications/Amendments, if any, should be signed by the Authorized Signatory (Power of Attorney (POA) proof to be submitted). A certificate of authorization should also be attached along with the bid.

f. The Bank is not bound to accept any of the proposals submitted and the Bank has the right to reject any/all proposal/s or cancel the tender without assigning any reason, there for.

g. Any additional or different terms and conditions proposed by the Bidder would deem to be rejected unless expressly assented to in writing by the Bank.

h. Bank reserves the absolute right to reject any bid if the same is not in accordance with its requirements and no further correspondence, whatsoever, will be entertained by the Bank in the matter.

i. Each bid should specify only a single solution which should meet the specifications mentioned in this RFP and should not include/suggest any alternatives.

j. To assist in the scrutiny, evaluation, and comparison of offers, Bank may, at its discretion, seek clarification from the Bidder. The request for clarification and the response shall be in writing/through e-mail and no change in the price or substance of the bid shall be sought, offered, or permitted.

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

l. The Bidder shall submit a non-disclosure agreement duly signed by authorized signatories.

m. This procurement is extendable to bank sponsored Regional Rural Banks and subsidiaries of the Bank at rates not exceeding the agreed rates; however, payments for such services shall be made separately.

## SECTION - IV

## INSTRUCTIONS TO BIDDERS FOR ONLINE TENDER THROUGH GEM PORTAL

### 1. SUBMISSION OF BIDS THROUGH GEM PORTAL

The Bid documents, to be uploaded as part of online bid submission, are as follows:

a. Eligibility Criteria, along with all supporting documents required.

b. All Annexures as per this tender on Bidder's letter head with authorizing person's signature and Bidder seal on all pages.

c. All supporting documents and product literature in support of Technical specifications.

d. Relevant brochures

e. Compliance to Technical Specifications as per Technical Bid.

f. Any other information sought by the Bank with relevant to this tender.

Bidder should upload all the copies of relevant documents without fail in support of their bid and as per the instructions given in tender documents. If the files to be uploaded are in PDF format, ensure to upload it in "Searchable" PDF Format. After filling data in predefined forms bidders need to click on final submission link to submit their encrypted bid.

Please take care to scan documents so that total size of documents to be uploaded remains minimum. **All documentary evidence provided to the Bank shall be in PDF Format. The Scanned Documents shall be OCR enabled for facilitating "search" on the scanned document.** Utmost care may be taken to name the files/documents to be uploaded on e-tendering portal.

### 2. BID RELATED INFORMATION

Bidders must ensure that all documents uploaded on e-tendering portal as files or zipped folders, contain valid files and are not corrupt or damaged due to any processing at bidder PC system like zipping etc. It shall be the responsibility of bidder themselves for proper extractability of uploaded zipped files.

Any error/virus creeping into files/folder from client end PC system cannot be monitored by e-tender software/server and will be bidder's responsibility only.

### 3. OFFLINE SUBMISSIONS

In addition to uploading the documents in our e-Tendering portal, Bidders should also submit the following in a sealed envelope, super scribing with the tender Reference number, due date, Name of the Bidder, etc.

a) Bid Security (EMD) in the form of DD/ Fund transfer/ Bank Guarantee (issued by a nationalised / scheduled commercial Bank (other than Indian Bank) in favour of “Indian Bank” payable at Chennai.

b) Pre-Contract Integrity Pact

The bidder is requested to submit the original documents (as mentioned under point no. 9 of Schedule [A]) in a Sealed Envelope on or before **07/08/2026 at 03:00 PM** to the address mentioned under point no. 4 of [A] (Important Dates and Information on RFP Submission) of schedule of this tender. The envelope shall be super scribed as “**Supply, Installation, Implementation, Integration and Maintenance of Enterprise Data Privacy Governance & Compliance Platform to Comply with Digital Personal Data Protection Act 2023 and DPDP Rules 2025.**” and the words ‘**DO NOT OPEN BEFORE (07/08/2026 at 03:30 PM**)’.

### 4. OTHER INSTRUCTIONS

For further instructions like system requirements and manuals, the bidder should visit GEM portal or banks Website.

**SECTION-V**

**Appendix I - Technical & Functional Requirements**

Date:

The General Manager
Indian Bank, Head Office,
Information Technology Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sirs,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025.**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

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

The listed features represent the required capabilities for the platform. Our responses will be evaluated in accordance with the RFP's scope of work.

The abbreviation for the below table are:

1. Mandatory (M) for bid submission
2. Optional (O) would be an added value
3. Available (A) for out-of-the-box functionality,
4. Customizable (C) for features achievable through configuration or development. All 'Optional' must be at least Customizable if not Available out of the box.

**TECHNICAL AND FUNCTIONAL SPECIFICATIONS:**

The detailed technical requirement for each of the feature is as follows:

| S.No | Particulars | Mandatory / Optional | Response (A/C) | Detailed Response |
|---|---|---|---|---|
| | **I. Technical Specifications** | | | |
| | **Consent & Preference Management** | | | |
| 1 | Does the solution support explicit, purpose-specific consent capture aligned with lawful basis prior to any processing activity across all channels? | M | - | |

| | | | | |
|---|---|---|---|---|
| 2 | Can the platform serve as an enterprise-wide consent repository (single system of record) that stores consent with all requisite capabilities, including records that contain the consent purpose, timestamp, consent status (active/revoked), and reference to the notice provided? | M | - | |
| 3 | Can consent validation be enforced programmatically in real-time before downstream system processing is triggered? | M | - | |
| 4 | Does the system support granular consent structuring across purpose, sub-purpose, channel, product, and data-sharing categories? | M | - | |
| 5 | Can consent be modified, partially withdrawn, or revoked with automated propagation across integrated systems? | M | - | |
| 6 | Does the solution support digital, assisted, and offline consent capture journeys with centralized synchronization? | M | - | |
| 7 | Are consent artefacts immutable and legally defensible with timestamping and traceability? | M | - | |
| 8 | Does the platform maintain a complete audit trail of consent lifecycle events? | M | - | |
| 9 | Can consent expiry, renewal, and re-consent workflows be automated? | M | - | |
| 10 | Can bulk consent collection be executed for legacy customer base with tracking? | M | - | |
| 11 | Can the platform provide a defined process to handle exceptions including incorrect consent mapping, consent disputes, and failed revocation propagations and seamlessly link them to the bank's grievance handling system within mandated timelines? | O | | |
| 12 | Can the platform notify customers of material changes affecting consent (e.g., change in purpose of processing, data categories collected, third-party sharing/recipients, retention period, or consent terms) and obtain fresh/re-confirmed consent? | M | - | |

| | | | | |
|---|---|---|---|---|
| 13 | Can the platform seamlessly integrate with the Bank's existing public-facing applications? | M | - | |
| **B** | **Cookie Consent Management** | | | |
| 14 | Can the platform manage cookie consent by fully supporting all current and future similar tracking technologies? | M | - | |
| 15 | Does the platform support categorization of cookies based on purpose and risk (essential, functional, analytics, marketing)? | M | - | |
| 16 | Can the system automatically scan, detect, and classify cookies across web and application environments? | M | - | |
| 17 | Does the solution enforce real-time blocking or activation of scripts based on user consent choices? | M | - | |
| 18 | Can cookie consent preferences be modified or withdrawn dynamically by users across sessions? | M | - | |
| 19 | Does the platform support configurable, multilingual, and channel-specific cookie banners? | M | - | |
| 20 | Can unidentified or newly introduced cookies be flagged and classified automatically? | M | - | |
| 21 | Does the system maintain audit trails of cookie consent capture and enforcement events? | M | - | |
| **C** | **Privacy Notice Management** | | | |
| 22 | Does the solution support configurable, reusable, and regulation-aligned privacy notice templates across products and channels? | M | - | |
| 23 | Can dynamic, context-aware notices be delivered based on user journey, product, and data processing purpose? | M | - | |
| 24 | Does the system maintain full version control with backward traceability of notice changes and applicability timelines? | M | - | |
| 25 | Can customers on outdated notice versions be identified and automatically triggered for re-consent workflows? | M | - | |

| | | | | |
|---|---|---|---|---|
| 26 | Can privacy notices be programmatically linked to consent capture and audit trails for regulatory evidence? | M | - | |
| 27 | Does the solution support multilingual privacy notice delivery across all supported channels, with configurable language coverage supporting English as well as all official languages recognized under the Eighth Schedule to the Constitution of India? | M | - | |
| **D** | **Data Principal Rights Management** | | | |
| 28 | Does the solution provide a unified self-service portal for Data Principal requests across channels? | M | - | |
| 29 | Can Data Principals access, download, and track the lifecycle of their requests and consent history? | M | - | |
| 30 | Does the platform support all DPDP rights including access, correction, erasure, withdrawal, and grievance handling? | M | - | |
| 31 | Are end-to-end workflows supported including intake, identity verification, fulfilment, and closure? | M | - | |
| 32 | Can deletion requests be orchestrated across Data Fiduciaries, Processors, and downstream applications? | M | - | |
| 33 | Is there a centralized registry for all requests with SLA tracking and audit visibility? | M | - | |
| 34 | Can identity verification mechanisms be integrated (KYC, OTP, etc.) into request workflows? | M | - | |
| 35 | Are multi-channel notifications supported with configurable triggers and templates? | M | - | |
| 36 | Can requests be routed and fulfilled across multiple backend systems through orchestration workflows? | M | - | |
| 37 | Are SLA breaches tracked with automated escalation mechanisms? | M | - | |

| | | | | |
|---|---|---|---|---|
| 38 | Can the platform configure and manage nominee-based workflows under the DPDP Act, including verifying nominee credentials, authorizing the exercise of rights (access, correction, erasure), and maintaining a compliant audit trail? | M | - | |
| 39 | Are all request lifecycle activities recorded in immutable audit logs? | M | - | |
| **E** | **Personal Data Breach Management** | | | |
| 40 | Does the solution support end-to-end breach lifecycle management including detection, registration, triage, containment, impact assessment, notification, and closure? | M | - | |
| 41 | Can the platform automatically determine breach severity based on type of data impacted (personal vs sensitive), volume, and processing context? | M | - | |
| 42 | Does the system enforce DPDP-aligned regulatory notification timelines (internal escalation, regulator reporting, Data Principal notification) with configurable SLAs? | M | - | |
| 43 | Can the solution identify affected Data Principals by correlating breach events with data inventory, data lineage, and processing systems? | M | - | |
| 44 | Does the platform support cohort-based communication workflows to notify affected Data Principals across channels (SMS, Email, App, etc.)? | M | - | |
| 45 | Can containment, remediation activities, and root-cause analysis be tracked with workflow orchestration and approval checkpoints? | M | - | |
| 46 | Does the system support integration with SOC/SIEM tools for automated breach/incident ingestion and correlation? | M | - | |
| 47 | Are all data breach and incident logs stored in a tamper-proof, immutable, and audit-defensible format with unalterable history and complete event traceability? | M | - | |
| **F** | **Data Discovery, Classification & Lineage** | | | |

| | | | | |
|---|---|---|---|---|
| 48 | Does the solution support automated discovery of digital personal data across structured, semi-structured, and unstructured data stores (including endpoints) to ensure comprehensive visibility and compliance under the DPDP Act? | M | - | |
| 49 | Can the system classify data based on predefined and custom classification rules aligned to regulatory definitions (e.g., personal, sensitive)? | M | - | |
| 50 | Does the platform support data lineage from source to processing systems? | M | - | |
| 51 | Can discovered data elements be mapped to business metadata such as application, data owner, processing purpose, and retention policy? | M | - | |
| 52 | Does the solution support incremental and continuous data discovery with change detection mechanisms? | M | - | |
| 53 | Can the solution be configured to define custom classification rules and patterns specific to the Bank's business requirements without modifying the product source code? | M | - | |
| 54 | Can classification outputs be programmatically consumed by downstream modules such as DPRM, DPIA, and breach management? | M | - | |
| 55 | Can data assets discovered through external tools be reconciled and maintained with referential integrity within the platform? | M | - | |
| 56 | Does the system maintain linkage between data elements, consent records, processing purposes, and applications for traceability? | M | - | |
| 57 | Can the solution detect and classify PII present within free-text or narrative fields (e.g., remarks, comments, descriptions)? | O | | |
| 58 | Can the solution identify and classify PII embedded within XML, JSON, or other semi-structured data stored in database columns? | O | | |

| | | | | |
|---|---|---|---|---|
| 59 | Does the solution use contextual analysis, in addition to pattern matching, to distinguish between similar data types? | O | | |
| 60 | Can the platform ingest and parse customizable, manually prepared Records of Processing Activities (RoPA) uploads to integrate our existing baseline? | M | - | |
| **G** | **Data Protection Impact Assessment** | | | |
| 61 | Does the solution support standardized and configurable DPIA templates aligned with DPDP and internal risk frameworks? | M | - | |
| 62 | Does the platform support triggering Data Protection Impact Assessments (DPIAs) based on predefined conditions, such as a new product launch, modifications to data processing, or high-risk data classifications? | O | | |
| 63 | Does the platform support automated identification and scoring of privacy risks using inputs from data discovery and processing activities? | O | | |
| 64 | Are multi-level review, approval, and escalation workflows configurable with role-based access control? | M | - | |
| 65 | Can DPIAs capture detailed processing flows, data categories, risk factors, mitigation plans, and third-party involvement in a structured manner? | M | - | |
| **H** | **Record of Processing Activities (ROPA)** | | | |
| 66 | Does the solution maintain a centralized and continuously updated inventory of personal data across applications, systems, and business processes? | M | - | |
| 67 | Can the platform maintain Records of Processing Activities (ROPA) mapped to purpose, data category, system, retention period, and legal basis? | M | - | |
| 68 | Does the system support automated updates to inventory based on inputs from discovery and classification tools? | O | | |

| | | | | |
|---|---|---|---|---|
| 69 | Can each digital personal data element be mapped to a specific data owner?? | M | - | |
| 70 | Does the platform enforce retention and deletion policies linked to ROPA entries and regulatory requirements? | M | - | |
| 71 | Can regulator-ready compliance reports be generated with verifiable traceability linking processing activities directly to the underlying digital personal data assets and corresponding consent records? | O | | |
| **I** | **Third Party Risk Management** | | | |
| 72 | Does the solution maintain a centralized, version-controlled repository of all third-party vendors and data processors? | M | - | |
| 73 | Can vendors access a secure self-service portal to complete assessments, submit documents, and track compliance status? | O | | |
| 74 | Are risk assessment questionnaires configurable based on vendor type, data access, and risk profile? | M | - | |
| 75 | Does the system provide automated risk scoring and classification of vendors based on assessment responses and data sensitivity? | M | - | |
| 76 | Can contractual obligations, SLAs, and compliance requirements be tracked and monitored throughout the vendor lifecycle? | M | - | |
| 77 | Can data-related requests (e.g., deletion, restriction) be routed to processors and tracked with acknowledgment and closure evidence? | O | | |
| 78 | Does the solution support contract lifecycle management including versioning, renewals, and compliance tracking? | M | - | |
| 79 | Can vendor risk data be integrated with DPIA, DPRM, and breach management modules for unified risk visibility? | O | | |
| | **II. Functional Specification** | | | |
| 80 | Does the solution support secure on-premise deployment within Bank-controlled infrastructure with no mandatory cloud dependency? | M | - | |

| | | | | |
|---|---|---|---|---|
| 81 | Does the platform support high availability and business continuity through a robust DC-DR architecture (supporting Active-Passive configurations) that aligns with the Bank's corporate Recovery Time Objective (RTO) and Recovery Point Objective (RPO) thresholds? | M | - | |
| 82 | Can the platform scale horizontally and vertically to handle enterprise-wide transaction volumes and concurrent user loads? | M | - | |
| 83 | Does the solution support API-first architecture for integration with CBS, CRM, digital channels, and data platforms? | M | - | |
| 84 | Can real-time consent validation and enforcement be performed with defined latency thresholds and fallback mechanisms? | M | - | |
| 85 | Does the platform support multiple integration modes (API, batch, event-driven) with error handling and retry mechanisms? | M | - | |
| 86 | Does the solution comply with DPDP Act 2023, RBI guidelines, and relevant regulatory frameworks applicable to banking? | M | - | |
| 87 | Is encryption implemented for data at rest and in transit using industry-standard protocols and algorithms? | M | - | |
| 88 | Does the system support RBAC, MFA, and integration with enterprise identity and access management systems? | M | - | |
| 89 | Can the platform support ≥99.9% uptime with monitoring and automated failover capabilities? | O | | |
| 90 | Are performance SLAs defined, measurable, and trackable through dashboards with alerting mechanisms? | O | | |
| 91 | Does the vendor provide a detailed implementation methodology including phases, milestones, dependencies, and deliverables? | M | - | |
| 92 | Are dedicated resources (project manager, SMEs) and governance structures defined for implementation and support? | M | - | |

| | | | | |
|---|---|---|---|---|
| 93 | Does the solution provide audit-ready logs with end-to-end traceability across all modules? | M | - | |
| 94 | Can the platform generate regulator-ready compliance reports both on-demand and on a scheduled basis, with integrated end-to-end data lineage linkage? | O | | |

**Hardware Specification**

| | | | | |
|---|---|---|---|---|
| 95 | Is the proposed solution deployable on industry-standard x86 server infrastructure within the Bank's on-premise data center environment ? | M | - | |
| 96 | Does the solution support deployment on physical, virtualized and containerized infrastructure environments? | M | - | |
| 97 | Does the proposed architecture support scalability of compute, storage and application components without major redesign or disruption? | M | - | |
| 98 | Does the proposed solution support high availability architecture with no single point of failure for critical application components? | M | - | |
| 99 | Does the solution support deployment on enterprise-grade storage platforms and support future storage expansion requirements? | M | - | |
| 100 | Does the solution support secure storage of privacy records, consent artefacts, audit trails, DPIA records, notices and related compliance evidence? | M | - | |
| 101 | Are backup, archival and recovery mechanisms supported for application data, configurations and audit records? | M | - | |
| 102 | Is the platform flexible enough to seamlessly integrate with the Bank's existing infrastructure for backups and DC-DR (Data Center-Disaster Recovery)? | M | - | |
| 103 | Does the solution support secure network communication using standard enterprise protocols and interfaces? | M | - | |

| | | | | |
|---|---|---|---|---|
| 104 | Is the platform flexible enough to seamlessly integrate with the Bank's existing enterprise network, security architecture and monitoring infrastructure? | M | - | |
| 105 | Does the solution support load balancing and failover capabilities to ensure business continuity and service availability? | M | - | |
| 106 | Does the solution support centralized monitoring, health checks, logging and operational alerting mechanisms? | O | | |
| 107 | Does the solution support non-disruptive maintenance, software upgrades, patches and capacity expansion activities? | M | - | |
| 108 | Does the solution support secure administrative access, infrastructure-level audit logging and role-based administration controls? | M | - | |

If the mandatory requirements in the above table for technical specifications is not complied, then Bank reserves the right to technically disqualify the bid.

For

Office Seal

Place:

Date:

Authorized Signatory

Name:

Designation:

Mobile Number:

Business Address:

Telephone No.:

Official E-Mail ID:

## Appendix II - Commercial Bid

(Price bid along with Breakup to be submitted with Technical Bid in a separate envelope)

Date:

To
General Manager,
Indian Bank, Head Office
Information Technology Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sirs,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your** RFP No GEM/2026/B/**7823086 dated 23/07/2026**

We submit hereunder the price breakup details along with a detailed Bill of Materials (BoM) in a separate sheet, clearly listing all proposed components, including but not limited to Hardware, Software, Storage, Middleware, Database, Operating System, Licenses, and any other associated products/services. The submission shall include the corresponding specifications, quantities, versions, model numbers (where applicable), and any relevant technical details of each item proposed as part of the solution.

**Price Schedule**

**A. Enterprise perpetual License cost for three years for following modules:**

1. Consent & Preference Management
2. Cookie Consent
3. Privacy Notice Management
4. Data Principal Rights Management
5. Personal Data Breach Management
6. Data Discovery, Classification & Lineage
7. Data Protection Impact Assessment
8. Records of Processing Activities
9. Third Party Risk Management

| TABLE A (License Cost) | | | | |
|---|---|---|---|---|
| **S.NO** | **Year** | **License Cost of 9 Modules (Exclusive of Taxes)** | **Taxes** | **Total cost of 9 Modules inclusive of taxes** |
| | | **(a)** | **(b)** | **(c) = [(a) + (b)]** |
| A1 | Year-1 | | | |
| A2 | Year-2 | | | |
| A3 | Year-3 | | | |
| **Total License Cost (A) = A1+A2+A3** | | | | |

Note: Licensing may be based on users / data volume / transactions depending on module. Pricing should clearly indicate basis (user-based / TB-based / website-based / vendor-based etc.).

The Year-1 starts from the date of activation of license. Cost of licenses will be paid upfront yearly in advance based on the licenses procured on delivery of licenses.

Successful bidder has to provide required licenses in the name of Bank either through OEM or through OEM's licensing partners, however, payment will be made by Bank to successful bidder only.

**B. IMPLEMENTATION & INTEGRATION COST:**

| TABLE – B (IMPLEMENTATION & INTEGRATION COST) | | | | | |
|---|---|---|---|---|---|
| **S. No.** | **Item Details** | **Price Details [Excl. of Tax]** | **Tax %** | **Tax Value** | **Total Cost for implementation [Incl. of Tax]** |
| | | **(a)** | **(b)** | **(c)** | **(d) = [(a)+(c)]** |
| B | One-Time Implementation (installation, configuration, integration, customization, migration, testing, deployment, training, etc. of Hardware and Software) | | | | |
| **Total Implementation Cost (B)** | | | | | |

**C. INFRASTRUCTURE COST:**

| TABLE C (Infrastructure Cost) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| S. No. | Item Details* | | Number of Units | Yearly Cost Per unit | Yearly Cost for all the units (Excl. Tax) | Tax for all the units | Number of Years | Total Cost |
| | | | (a) | (b) | (c) = (a)*(b) | d | e | f=e*(c+d) |
| C1 | Compute (Servers / VM / Containers) | DC | | | | | | |
| | | DR | | | | | | |
| | | Dev / UAT / SIT | | | | | | |
| C2 | Storage (Structured + Unstructured Data) | DC | | | | | | |
| | | DR | | | | | | |
| | | Dev / UAT / SIT | | | | | | |
| C3 | Others | | | | | | | |

**Note1:** Bidder to add Separate line item for all applicable components proposed for this solution

**Note2:** DR as per DC except Dev/UAT/SIT.

**Total Infrastructure Cost [C] (C1+C2+C3) :** ______________________

**D. Post Go-Live Support**

| TABLE D (Post Go-Live Support) | | | | |
|---|---|---|---|---|
| S.No. | Item Details | Year 1 | Year 2 | Year 3 |
| D | Post Go-Live Support^ (Exclusive of Taxes) (a) | | | |
| | Taxes (b) | | | |
| | Total Cost Post Go-Live Support | | | |

| | | | | |
|---|---|---|---|---|
| | (c) = (a) + (b) | | | |
| **Total Post Go-Live Support Cost (D)** | | | | |

**^Note: Bidder to provide go-live support as mentioned in the section 3 Service Contract – Post Go-Live Support**

**D. Total Cost of Ownership (TCO):**

| | |
|---|---|
| **Total Cost of Ownership (TCO) without taxes=**<br>**Table[A] + Table[B] + Table[C] + Table D (Exclusive of Taxes): (X)** | **Rs. ……………………………………….** |
| **Total Taxes (Y) = (Tax of A + Tax of B + Tax of C + Tax of D)** | |
| **Total Cost with taxes(H) = (X+Y)** | |
| **In words (inclusive of taxes): Rupees ……………………………..** | |

**PRICE STATEMENT:**

Bank reserves the right to re-negotiate the price for any of the line items furnished above, in case the rates offered are arbitrary and not as per market prices. Costs include all applicable charges (license, infra, integration, support, etc.). Any additional cost not mentioned shall not be charged separately

Total Cost of Ownership (TCO) for propped solution is for the entire contract period (inclusive of all duties, levies, freight, insurance, warranty, etc., is Rs. ……………………………..………….. (in figures) Rupees ………………………………………………………………… (in words). (Octroi/ Entry Tax if any, will be reimbursed on submission of original receipts.)

We submit that we shall abide by the details given above and the conditions given in your above tender.

For

Office Seal

Place:

Date:

Authorized Signatory

Name:

Designation:

Mobile Number:

Business Address:

Telephone No.:

Official E-Mail ID:

**(LIST OF ANNEXURES)**

**<u>ANNEXURE-I - Bid Form</u>**

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

Date: ___________________

To

General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

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

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

If our bid is accepted, we will obtain the Guarantee of a Bank in a sum equivalent to 5% per cent of the Contract Price for the due performance of the Contract, in the form prescribed by the Bank.

We agree to abide by this for the bid validity period specified and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We agree to extend the Bid Validity Period, if required.

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

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

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

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

Dated this ..........................day of ......................…. 2026

Signature ............................................

.................................................................
(In the Capacity of)

Duly authorized to sign bid for and on behalf of

(Name & Address of Bidder)

...........................................................…...........

..........................................................................

..........................................................................

Mobile:

Official Email

## ANNEXURE-II - Self-Declaration – Blacklisting

To,
General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sir,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

We hereby certify that, we have not been blacklisted by any Government Dept. / PSUs / Banks/ PSBs / Financial Institutions at the time of bid submission.

We hereby certify that, we are not insolvent at the time of bid submission.

**Signature of Authorized Official**

**Name and Designation with Office Seal**

**Place:**

**Date:**

**ANNEXURE–III - Contract Form**

**(To be submitted on Non - Judicial Stamp Paper)**

**THIS AGREEMENT** made the .......day of..................................2026 Between Indian Bank, having its Corporate Office at 254-260, Avvai Shanmugam Salai, Royapettah, Chennai 600 014 (hereinafter "the Purchaser") which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and ………………………………… (Name of Supplier) having its Registered Office at ………………………………………………… (City and Country of Supplier) (hereinafter called "the Supplier") which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

**WHEREAS** the Purchaser invited bids vide RFP No. **GEM/2026/B/7823086** for certain Goods and services viz., .................................... (Brief Description of Goods and Services) and has accepted a bid by the Supplier for the provision of those goods and services in the sum for ......................................................................................... .............................. (Contract Price in Words and Figures) (hereinafter called "the Contract Price").

**NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:**

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

   (a) the Bid Form and the Price Schedule submitted by the Bidder;
   (b) the Schedule of Requirements;
   (c) the Functional & Technical Specifications;
   (d) the Conditions of Contract;
   (e) the Purchaser's Notification of Award/Purchase Order.
   (f) the RFP including Addendum/s & corrigendum/s.

3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

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

| Sl. No. | Brief description of goods & services | Quantity to be supplied | Unit price | Total price |
|---|---|---|---|---|
| | | | | |

**TOTAL VALUE:**

**DELIVERY SCHEDULE:**

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

Signed, Sealed and Delivered by the

said ..................................................... (For Indian Bank)

in the presence of: ......................................

Signed, Sealed and Delivered by the

said ..................................................... (For the supplier)

in the presence of: ......................................

## ANNEXURE-IV - Performance Security Format

Bank Guarantee No. Date:

To: INDIAN BANK,
Chennai,
INDIA:

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

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

**AND WHEREAS** we have agreed to give the Supplier a Guarantee:

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

This guarantee is valid until the ........day of..................20__

Signature of Authorized Official with Seal

..................................................................

Date...................................................2026

Address: ...................................................

..................................................................

..................................................................

NOTE:

1. Supplier should ensure that seal and code number of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee issued by Banks located in India and shall be on a Non-Judicial Stamp Paper of requisite value.

**ANNEXURE-V - Manufacturers' Authorization Form (MAF)**

(To be provided on Letterhead of OEM duly signed & stamped by their Authorized Signatory)

No.
Date:

To
General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai – 600001

**MAF for your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

Dear Sir,

We who are established and reputable manufacturers/ developer of ……………………………………… *(name of product offered)* do hereby authorize M/s………………………………...*(name and address of Agent)* to submit a Quote, and sign the contract with you for the solution offered by us against the above RFP (Supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform).

We hereby extend our full warranty/support as per Conditions of Contract for the goods and services offered for supply by the above firm against this RFP (Request for Proposal). We duly authorize the said firm to act on our behalf in fulfilling all installation, integration, technical support and Annual maintenance obligations required by the Contract.

In case the bidder i.e. M/s ________ is not able to perform obligations as per RFP during the contract period (like if bidder ceases to exist, stops services or support to the Bank, terminates contract due any reasons with Bank or due to any other reason), we will perform the said obligations, as per given scope of work of RFP, either directly or through mutually agreed third party/any other authorized Partner of ours.

Yours faithfully,
(Name)
(Name of OEM)
Designation:
Official Email ID:
Telephone/Mobile No:

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

## ANNEXURE-VI - Pre-Contract Integrity Pact

**(To be submitted on Non - Judicial Stamp Paper)**

**PRE-CONTRACT INTEGRITY PACT**

**Between**

**Indian Bank hereinafter referred to as "The Bank''**

**and**

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

### Preamble

The Bank intends to award, under laid down organizational procedures, contract/s for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023**.**.The Bank values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidders(s) and / or Contractor(s).

In order to achieve these goals, the Bank 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 Bank

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

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

The Bank will, during the tender process treat all Bidder(s) with equity and reason. The Bank will in, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution. The Bank will exclude from the process all known prejudiced persons. If the Bank obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Bank will inform the Chief Vigilance Officer(CVO) and in addition can initiate disciplinary actions.

**Section 2 – Commitment of the Bidder(s)/ Contractor(s)**1. The Bidder(s) / Contractor(s) commit themselves to take all measures necessary to prevent corruption. They commit themselves to observe the following principles during their 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 Bank's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract. The Bidder(s) / Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process. The Bidder(s) / Contractor(s) will not commit any offence under the relevant IPC/PC Act: further, the Bidder (s) / Contractor (s) will not use improperly, for purpose of competition or personal gain, or pass on to others, any information or documents provided by the Bank as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically. The Bidder (s) / Contractor (s) of foreign origin shall disclose the name and address of the Agents/Representatives in India, if any. Similarly, the Bidder(s)/Contractor (s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further, as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers'' shall be disclosed by the Bidder (s) / Contractor (s). Further as mentioned in the Guidelines, all the payments made to the Indian Agent/Representative have to be in Indian Rupees only. Copy of the ''Guidelines on Indian Agents of Foreign Suppliers'' is placed at Annexure. The Bidder (s) / Contractor (s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract. The Bidder (s) / Contractor (s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

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

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

**Section 4 – Compensation for Damages**

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

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

**Section 5 – Previous Transgression**

1. The Bidders declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprises in India that could justify his exclusion from the tender process.
2. The Bidder agrees that if he makes incorrect statement on this subject, bidder is liable to be disqualified from the tender process or the contract, if already awarded, is liable to be terminated for such reason.
3. The imposition and duration of the execution of the bidder will be determined by the bidder based on the severity of transgression.

4. The Bidder/Contractor acknowledges and undertakes to respect and uphold the Bank absolute right to resort to and impose such exclusion.
5. Apart from the above, the Bank may take action for banning of business dealings/holiday listing of the Bidder/ Contractor as deemed fit by the Bank.
6. If the Bidder/Contractor can prove that he has resorted/recouped the damage caused by him and has implemented a suitable corruption prevention system, the Bank may, at its own discretion, as per laid down organizational procedures, revoke the exclusion prematurely.

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

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all sub-contractors a commitment in conformity with this Pre-Contract Integrity Pact, and to submit it to the Bank before contract signing. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the principles laid down in this agreement/Pact by any of its Sub-contractors/Sub-vendors.
2. The Bank will enter into agreement with identical conditions as this one with all Bidders/Contractors.
3. The Bank will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

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

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

**Section 8 – Independent External Monitor / Monitors**

1. The Bank appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
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 Authority designated by the Bank. The Bidder(s)/Contractor(s) accept that the Monitor has the right to access without restriction to all Project documentations of the Bank including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidders)/Contractors(s)/Subcontractors(s) with confidentiality. The Bank will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Bank and the Contractor. The parties offer to the Monitor the option to participate in such meetings. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Bank and request the Management to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that

they act in a specific manner, refrain from action or tolerate action. The Monitor will submit a written report to the Authority designated by the Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Bank and, should the occasion arise submit proposals for correcting problematic situations. If the Monitor has reported to Authority designated by the Bank, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Authority designated by the Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner. The word **'Monitor'** would include both singular and plural. **Section 9** – **Pact Duration**. This pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded on whomsoever it may be. If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by the Bank.

**Section 10 – Examination of Books of Accounts**

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

**Section 11 – Other provisions**

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Corporate Office of the Bank, i.e. Chennai.
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. In case of a Company, the Pact must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. In the event of any contradiction between the Pre-Contract Integrity Pact and its Annexure, the Clause in the Pre-Contract Integrity Pact will prevail.
6. Any dispute or difference arising between the parties with regard to the terms of this Agreement/Pact, any action taken by the Bank in accordance with this Agreement/Pact or interpretation thereof shall not be subject to arbitration.

The parties hereby sign this Pre-Contract Integrity Pact at ……………………on ……………………..

| | |
|---|---|
| (For & On behalf of the Bank) | (For & On behalf of Bidder/Contractor) |
| (Office Seal) | (Office Seal) |

Place ________________ Place ________________
Date ________________ Date ________________

Witness 1:

Witness 1:

(Name & Address) ____________________ (Name & Address) ____________________
___________________________________ ___________________________________
___________________________________ ___________________________________

Witness 2:

Witness 2:

(Name & Address) ____________________ (Name & Address) ____________________
___________________________________ ___________________________________
___________________________________ ___________________________________

**ANNEXURE-VII - Non-Disclosure Agreement**
**(To be submitted on Non - Judicial Stamp Paper)**

**THIS AGREEMENT** made and entered into at …………………on this the ……day of………2026 between **INDIAN BANK**, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having its Corporate Office at No.254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600 014, hereinafter called the "**BANK**" which term shall wherever the context so require includes its successors and assigns

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

WHEREAS
The Bank is inter-alia engaged in the business of banking and intends to procure for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and Rules 2025.

M/s……………………………. Limited has been engaged in the business of providing the services for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and Rules 2025.

The parties have entered into agreement dated ________________ for providing the services for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and Rules 2025 (herein after referred to as "purpose")" and have established business relationship between themselves. In course of the said purpose, it is anticipated that each party may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information. The parties have agreed that disclosure and use of such confidential information shall be made and on the terms and conditions of this agreement.

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

**1. Confidential information**

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

**2. Use of Confidential Information**

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

The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived there from, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. The Receiving Party may disclose confidential information to consultants only if the consultant has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement.
Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to this agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party. Upon written request by the Bank, the Supplier shall:

(i) cease using the Confidential information,

(ii) return the Confidential Information and all copies, notes or extracts thereof to the Bank within seven (7) business days of receipt of request and

(iii) confirm in writing that the Receiving Party has complied with the obligations set forth in this paragraph."

**3. Exemptions**

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

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

**4. Term**

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the disclosing party, the receiving party shall promptly return or destroy all written, graphic or other tangible forms of the confidential information and all copies, abstracts, extracts, samples, note or modules thereof.

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

**5. Title and Proprietary rights**

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

**6.Return of confidential information**

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

**7. Remedies**

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

**8. Entire agreement**

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

**9. Severability**

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

**10. Dispute resolution mechanism**

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

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

**11. Jurisdiction**

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

**12. Indemnity clause**

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

**13. Governing laws**

The provisions of this agreement shall be governed by the laws of India.
In witness whereof, the parties hereto have set their hands through their authorized signatories

BANK ………………………………….

M/s ………………………………….

**ANNEXURE-VIII - Declaration For MSE Benefits**

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

To,

General Manager,
Indian Bank, Head Office
IT Department, 3rd Floor
66, Rajaji Salai, Chennai - 600001

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

Dear Sir,

This has reference to our bid submitted in response to your Request for Proposal (RFP) Ref No **GEM/2026/B/7823086** dated 23/07/2026 floated for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023.

We have carefully gone through the contents of the above referred RFP and hereby undertake and confirm that, as per the Govt. of India guidelines, we are eligible to avail the following MSE benefits in response to your RFP floated, as referred above.

a) Issue of Tender Documents to MSEs free of Cost
b) Exemption on submission of bid security

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

Yours Sincerely

For M/s ______________________

Signature
Name:
Designation: Director/Company Secretary
Place:
Date:
Seal & Stamp

**ANNEXURE-IX - Declaration On Procurement from a Bidder of a Country which shares a land border with India**

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

To, Date

General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sir,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

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

**Signature of Authorized Official**

**Name and Designation with Office Seal**

**Place:**

**Date:**

## ANNEXURE-X - Certificate of Local Content as per Make in India Guidelines

To, Date

General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sir,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

This is to certify that proposed ______________ **<product details>** is having the local content of___________ % as defined in the above mentioned RFP.

The details of location(s) at which the local value addition is made are as under

| S.No. | Make and Model | Name of Place |
|---|---|---|
| | | |

This certificate is submitted in reference to the Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion order number P-45021/ 2/2017-B.E.-II dated 15th June 2017 for the Public Procurement (Preference to Make in India), Order 2017, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 28th May 2018, revision order no. P-45021/ 2/2017-PP (B.E.-II) dated 29th May 2019 and subsequent revision order no DPIIT Order No. P-45021/2/2017-PP(BE-II) dated June 04, 2020 and subsequent revision order no. P-45021/2/2017-PP (B.E.-II) dated 16th Sept 2020 & its amendment (if any) referred to hereinabove.

For Bidder

Signature of authorized signatory
Name and Designation:
Seal:
Date:

For OEM

Signature of authorized signatory
Name and Designation:
Seal:
Date:

**ANNEXURE-XI - Declaration of Customized Source Code (related to Bank) Audit**

To,
Date

General Manager,
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Dear Sir,

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

We further declare that if we become successful bidder, we will submit the proof of customized Source Code Audit by CERT-IN empaneled auditor, to the Bank, **as per timeline and periodicity defined by the Bank.**

**Signature of Authorized Official**

**Name and Designation with Office Seal**

**Place:**
**Date:**

**ANNEXURE-XII - Checklist for the RFP**

| Bidder Criteria | | | | |
|---|---|---|---|---|
| **S. No** | **Eligibility Criteria** | **Yes / No** | **List of Documents (to be filled by Bidder)** | **Page Number** |
| 1. | The bidder must be a registered Company (Public / Private) / PSU / PSE / Partnership Firm / LLP in India and has been in operation in India for at least 5 years as on date of publishing RFP. | | | |
| 2. | The average annual turnover of the Bidder should be Rs.75 crore or above in last three fiscal years (2023-24, 2024-25 & 2025-26). This must be the individual company turnover (the company which is bidding) and not that of any group of companies.<br><br>Relaxation only for MSE/ Start-up:<br>The average annual turnover of the MSE/Start-up Bidder should be Rs.50 crore or above in last three fiscal years (2023-24, 2024-25 & 2025-26). | | | |
| 3. | The net worth of the Bidder firm should be positive in last three fiscal years (2023-24, 2024-25 & 2025-26).<br>and<br>should not have eroded by more than 30% (thirty percent) in the last three fiscal years 2023-24, 2024-25 & 2025-26. | | | |
| 4. | The Bidder should have experience in supplying, implementation, integration, installation, maintenance and support of Enterprise Data Privacy & Governance Solutionduring the last 3 years till the date of release of this RFP for at least one organization in the BFSI sector / Government / PSU in India (The experience must be in the capacity of a solution implementer. Experience limited to consultancy, advisory, assessment, gap analysis, audit, or similar services shall not be considered as qualifying implementation eligibility). This must include at least the modules below:<br>3 Consent Management<br>4 Data Discovery and Classification. | | | |

| | | | | |
|---|---|---|---|---|
| 5. | The bidder shall be the OEM / System Integrator / Certified or authorized agent / reseller / partner for supply of Licenses and solution implementation and maintenance support under warranty/ AMC of the proposed solution. No consortium is allowed for the scope of the RFP.<br>The bidder needs to submit the MAF from the OEM proposed components of enterprise data privacy governance & compliance platform (as mentioned in section 3 of this RFP) and the related hardware components. | | | |
| 6. | The bidder shall have a valid partnership with the proposed OEM as on the date of issuance of the RFP, for supply, implementation, warranty, and maintenance support of the proposed solution and related hardware. The bidder shall ensure continuation / formalization of such arrangement for minimum three (3) years from the date of go-live Order, if selected. | | | |
| **OEM Criteria** | | | | |
| 8. | The proposed enterprise data privacy governance & compliance platform by OEM must have been implemented in at least one organization in the BFSI sector / Government / PSU in India within the last five (5) years as on the date of RFP release.<br>This must include at least the below modules:<br>3. Consent Management<br>4. Data Discovery and Classification<br><br>The Bank reserves the right to assess equivalence of functionalities provided under different nomenclatures. | | | |
| 9. | The hardware OEM must have successfully supplied and implemented hardware infrastructure in any organization within the BFSI, Government, or Public Sector Undertaking (PSU) sectors in India within the last five (5) years as on the date of this RFP release.<br>Note: The proposed hardware components need not be specific to privacy solutions. For the purpose of eligibility, the bidder may submit experience of similar hardware implementations by OEM. | | | |
| 10. | The proposed OEM of the enterprise data privacy governance & compliance platform must have a fully operational development and | | | |

| | | | | |
|---|---|---|---|---|
| | support center in India for at least one (1) year prior to the RFP release date. | | | |
| **Bidder - OEM Criteria** | | | | |
| 11. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017.<br>(or)<br>The Bidder and proposed OEM is from such a country and has been registered with the Competent Authority i.e., the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade, as stated under Annexure to the said Office Memorandum / Order and to submit the proof of registration herewith. | | | |
| 12. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform to provide information that any of its subsidiaries or associate or holding company or companies having common director/s or companies in the same group of promoters/ management or partnership firms/ LLPs having common partners has not participated in the bid process. | | | |
| 13. | The Bidder and proposed OEM of the enterprise data privacy governance & compliance platform should not have been debarred/ blacklisted for corrupt and fraudulent practices by the Govt. of India / State Governments / Regulatory Agencies / PSU/other institutions at the time of submission of bid. | | | |
| 14. | Bidder and proposed OEM of the enterprise data privacy governance & compliance platform should not be insolvent, in receivership, Bankrupt, or being wound up. | | | |

## ANNEXURE-XIII - Pre-Bid Query Format

(to be provided in MS-Excel format)

Bidder's request for Clarification - to be submitted as per the date mentioned in the RFP for submission of pre-bid queries

If, bidder, desiring to respond to RFP (**GEM/2026/B/7823086 dated 23/07/2026**) for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and its Rules 2025 and requires any clarifications on the points mentioned in the RFP, it may communicate with Bank using the following format.

All questions received till the last date & time of query receivable as mentioned in RFP will be formally responded to and questions/points of clarification and the responses will be circulated to all participating bidder if required. The source (identity) of the bidder seeking points of clarification will not be revealed. Alternatively, Bank may at its discretion, answer all/any/no such queries in the Pre-bid meeting.

Bidder's Name:

| S. No | Page No | Para No. | Description | Query details |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

## ANNEXURE-XIV - Experience Details

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

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

| S.No. | Name of Organization for whom services rendered | Nature of Work | Team size | PO Issue Date | Contract Value (In Rs.) | Project Details | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Period (No. of Months) | Start Date | Date of Completion/ expected completion |
| | | | | | | | | |

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

## ANNEXURE-XV - Turnover, Net Worth and P&L Details

*(To be signed by Statutory Auditor/Chartered Accountant)*

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

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

(Amount in Rs.)

| *F Y* | *Turnover* | *Net Profit and Loss* | *Net worth* |
|---|---|---|---|
| **2023-24** | | | |
| **2024-25** | | | |
| **2025-26** | | | |

Signature of CA/Statutory Auditor:

Name of CA/ Statutory Auditor:

Designation:

Seal:

Date:

**ANNEXURE – XVI - Undertaking Letter on the vendor's letterhead for Central Minimum Wages Act & Labour Laws**

General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Phone: +91-44-25269703 / 25269701

**Dear Sir,**
**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: RFP No. GEM/2026/B/7823086 dated 23/07/2026**

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

**(Proof of compliance and labour license needs to be submitted along with the quotation)**

**Signature of Authorized Official**

**Name:**
**Designation:**
**Office Seal:**
**Place:**
**Date:**
**Name:**

**ANNEXURE-XVII - Bid Security Format**

(to be submitted on non-judicial stamp paper)

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai – 600001

Whereas.......................... *(Hereinafter called "the Bidder")* who intends to submit its bid for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and its Rules 2025 through GeM Portal against GeM Bid Number **RFP No. GEM/2026/B/7823086 dated 23/07/2026** (Hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that We.................... *(name of bank)* of ................. (name of country), having our registered office at ................. *(address of bank)* (hereinafter called "the Bank"), are bound unto Indian Bank in the sum of ________________________for which payment well and truly to be made to the said Bank, the Bank binds itself, its successors, and assigns by these presents. Sealed with the seal of the said Bank this ____ day of _________.

THE CONDITIONS of this obligation are:

1. If the Bidder
   (a) withdraws its Bid during the period of bid validity specified in the GeM Bid; or
   (b) does not accept the correction of errors in accordance with the GeM Bid terms; or
2. If the Bidder, having been notified of the acceptance of its bid by the Bank during the period of bid validity:
   (a) fails or refuses to execute the Contract Form/NDA/SLA; or
   (b) fails or refuses to furnish the performance security, in accordance with the GeM Bid terms.

We undertake to pay the Bank up to the above amount upon receipt of its first written demand, without the Bank having to substantiate its demand, provided that in its demand the Bank will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including forty-five (45) days after the period of the bid validity (i.e. 165 days from last date of bid submission) and any demand in respect thereof should reach the Bank not later than the above date. (Signature of the Bank)

NOTE:

1. Bidder should ensure that the seal and CODE No. of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee issued by banks located in India and shall be on a Non-Judicial Stamp Paper of requisite value

## ANNEXURE-XVIII - Compliance Statement

**Ref**: **Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**
(**RFP No. GEM/2026/B/7823086)**

**DECLARATION**

Bank reserve the right to reject the bid, if bid is not submitted in proper format as per RFP and if any deviations are observed. Annexure-XXII Compliance Statement enclosed

| Compliance | Description | Compliance (Yes / No) |
|---|---|---|
| Terms and Conditions | We hereby undertake and agree to abide by all the terms and conditions including all annexure, corrigendum(s) etc. stipulated by the Bank in this RFP. (Any deviation may result in disqualification of our bid).<br>We understand & agree that in event of being successful in the bid and being awarded, we shall comply to the terms & conditions of RFP in future and shall not attempt to get the same changed from Bank later on in process of execution, contract signing, and extension of contract and / or subsequent purchase order/s from Bank. We understand and agree that such attempts and non-compliance to RFP terms may lead to cancellation of our agreement and suitable penal action may be taken by Bank against us including invoking the EMD and/ or PBG and black-listing. | |
| Scope of work, Technical and Functional Specification | We certify that the systems/services offered by us for tender conform to the Scope of work, technical and functional specifications stipulated by you. (Any deviation may result in disqualification of our bid). | |
| RFP, Clarifications & subsequent Corrigendum/s, if Any. | We hereby undertake that we have gone through RFP, clarifications & Corrigendum/s issued by Bank and agree to abide by all the terms and conditions including all annexure, corrigendum(s) etc. stipulated by the Bank in this RFP. (Any deviation may result in disqualification of our bid). | |

Date: ____________
Place: ____________

Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.: Seal of Company

**<u>ANNEXURE-XIX- Certificate of Solution/Software being deployed</u>**

(On Letter-Head of OEM)

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001
Phone: 044-25269703 / 25269701

**Dear Sir,**

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

Rules, 2025

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

We M/s________________________________________________, the OEM for the Solution(s)/Software(s) which is/are being supplied as a part of 'RFP for the supply, installation, implementation, integration and maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023 and Rules 2025 through our authorized partner M/s ____________________(name of bidder) hereby certify that all the software(s)/solution(s) to be deployed are latest bug free version and is free from all known vulnerabilities, malware and any covert channels in the code. We also confirm that the all the Licenses proposed as part of the solution are supported by an OEM and not community version.

We further certify that the Solution and Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to

a) Inhibit/ alter/ disable essential functions / critical settings, rending the application unusable or unreliable
b) Block communications or data flow, isolating the application from networked systems and preventing updates or controls
c) Tap information resident or transient in the equipment/network.

Date: ___________
Place: ___________

Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

**ANNEXURE-XX- Hosting Requirement.**

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001
Phone: 044-25269703 / 25269701

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

The bidder is required to provide detailed infrastructure sizing for hosting the proposed Privacy Management Platform covering the following modules:

1. Consent & Preference Management
2. Cookie Consent
3. Privacy Notice Management
4. Data Principal Rights Management
5. Personal Data Breach Management
6. Data Discovery, Classification & Lineage
7. Data Protection Impact Assessment (DPIA)
8. Records of Processing Activities (RoPA)
9. Third Party Risk Management

| S. No | Component | Server Type | Qty | Rack Unit (RU) required | Kilo Vat Amperes (KVA) Required |
|---|---|---|---|---|---|
| Production - Data Center Environment | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Production – Disaster Recovery Environment | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Non-Production – Development and UAT Environment | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Date: ____________
Place: ____________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

**ANNEXURE-XXI- Sizing Adequacy letter**

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001

Phone: 044-25269703 / 25269701
**Dear Sir,**

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

Dear Sir/Madam,

We ____________________________________________________(Bidder Name & address ) have reviewed the sizing submitted and in agreement with the proposed sizing to maintain the SLA for the contract duration . We confirm that the sizing is adequate and will meet the requirements of the Bank as stated in the RFP.

However, in the instance of the solution not working as per the SLA and response time mentioned in the RFP, we will augment the solution at no additional cost to the Bank

In case of shortfall during the contract period then the bidder is required to provide the shortfall along with the following penalties.

Penalty would be levied as mentioned below:

a) Shortfall between 1% to less than 5% (cost of Hardware, Software, license in the BOM submitted at the time of bid) then penalty would be two times of shortfall
b) Shortfall between 5% to less than 10% (cost of Hardware, Software, license in the BOM submitted at the time of bid) then penalty would be three times of shortfall
c) Shortfall more than 10% (cost of Hardware, Software, license in the BOM submitted at the time of bid) then penalty would be four times of shortfall

Bank Date: ___________
Place: ___________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:

Telephone No.:
Seal of Company

## ANNEXURE-XXII- Hardware End of Life and Support Declaration

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001
Phone: 044-25269703 / 25269701

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref**: **Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

Dear Sir/Madam,

We ______________________________________________________(OEM & address) has supplied ____________________(Hardware & software Make / model and quantity). We confirm that the Supplied device/s will not be end-of-life / End-of-sale within 2 years from the date of delivery and will be under support from the date of Delivery of hardware to next 3 years. The bug/Patches/components/security patches and releases will be available to Bank for above mentioned 5 years duration, the same responsibility shall so survive even after termination or expiry of the contract.

Date: ___________
Place: ___________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

## ANNEXURE-XXIII- Component Mapping

To
General Manager
Indian Bank, Head Office,
IT Department,4th Floor
66 Rajaji Salai, Chennai - 600001

Phone: 044-25269703 / 25269701

**Dear Sir,**

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

We, ______________________________ (Bidder Name & Address), hereby submit the component mapping for the proposed Privacy Management Platform.
We confirm that:

- All components proposed are included in the Bill of Materials
- No additional or hidden components are required for complete solution functionality
- Necessary back-to-back agreements exist with respective OEMs
- Proposed solution fully supports all modules defined in the RFP

| S.No | Component Name | Proposed OEM | Proposed Solution Name | Proposed Solution version/Make & Model |
|---|---|---|---|---|
| 1 | Consent & Preference Management | | | |
| 2 | Cookie Consent | | | |
| 3 | Privacy Notice Management | | | |
| 4 | Data Principal Rights Management (DPRM) | | | |
| 5 | Personal Data Breach Management | | | |

| | | | | |
|---|---|---|---|---|
| 6 | Data Discovery, Classification & Lineage | | | |
| 7 | Data Protection Impact Assessment (DPIA) | | | |
| 8 | Records of Processing Activities | | | |
| 9 | Third Party Risk Management | | | |

**Declaration**

We confirm that the above components are adequate for full implementation, integration and ongoing support of the enterprise privacy governance and compliance platform as per Bank requirements.

Date: ____________
Place: ____________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

**ANNEXURE-XXIV- Know Your Employee (KYE)**

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor
66 Rajaji Salai, Chennai - 600001
Phone: 044-25269703 / 25269701

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**

Dear Sir/Madam,

1. We ______________________ (name of the company) hereby confirm that all the Resource (both on-site and off-site) deployed/to be deployed on Bank's project for ___________________________________________________________________________ _(Name of the RFP) have undergone KYE (Know Your Employee) process and requisite checks have been performed prior to employment of said employees as per our policy.

2. We undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, educational document, etc.) to Bank before deploying officials in Bank premises for "Request for Proposal (RFP) for Supply, Installation, Implementation, Integration and Maintenance of enterprise data privacy governance & compliance platform to comply with the Digital Personal Data Protection Act, 2023.

Date: ___________
Place: ___________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

## ANNEXURE-XXV- CV Format

| S.No | Header | | | Details |
|---|---|---|---|---|
| 1 | Proposed position in the project | | | |
| 2 | Name of Staff | | | |
| 3 | Date of Birth | | | |
| 4 | Nationality | | | |
| 5 | Education Details | | | |
| i | Name of Institution | From | To | Degree Obtained |
| ii | | | | |
| Iii | | | | |
| Iv | | | | |
| 6. | Certifications and Trainings attended | | | |
| 7 | Area(s) of expertise and no. of years of experience in this area(s) | | | |
| 8 | Total No. of years of experience | | | |
| 9 | Total No. of years with the current firm | | | |
| 10 | Details of Experience | | | |
| | Name of the Organization | From | To | |
| i | <start with the current and go back in chronological order> | | | Designation/ Responsibilities |
| ii | | | | |
| iii | | | | |
| iv | | | | |
| 9 | Detailed Tasks Assigned on the Project [List all tasks to be performed under this assignment] | | | |
| 10 | Relevant Work Undertaken that Best Illustrates the experience as required for the Role (provide maximum of 5 citations of 10 lines | | | |
| i | Name of Assignment or Project | | | |
| ii | Is this project one of the client reference project? | | | <Yes / No> |
| iii | Duration on the project (in months) | | | |
| Year | | | | |
| Location | | | | |
| Employer | | | | |
| Main project Features | | | | |
| Position Help | | | | |
| Value of Project [Approximate value or range value] | | | | |
| Activities performed | | | | |
| Name of Assignment or Project | | | | |
| Is this project one of the Client reference project? | | | | |
| Duration on the project (in months) | | | | |
| Year | | | | |
| Location | | | | |
| Employer | | | | |
| Main project features | | | | |
| Positions held | | | | |

| | |
|---|---|
| Value of Project | |
| Activities performed | |
| <insert rows as relevant> | |

I, the undersigned, certify that to the best of my knowledge and belief, that the CV of the proposed staff above correctly describes qualifications and experience mentioned, and that the proposed staff member is a permanent employee of our organization. I understand that any willful misstatement described herein may lead to our disqualification or dismissal, if engaged

Date: ____________
Place: ____________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No.:
Seal of Company

**Ref: RFP No. GEM/2026/B/7823086** **Date: 23/07/2026**

## ANNEXURE-XXVI- Proposed Hardware Description Details

To
General Manager
Indian Bank, Head Office,
IT Department, 4th Floor.
66 Rajaji Salai, Chennai - 600001

**Sub: Request for Proposal for engagement of vendor for supply, implementation, integration and management of an enterprise data privacy governance & compliance platform, including supply and installation of required hardware, for compliance with DPDP Act, 2023 and DPDP Rules, 2025**

**Ref: Your RFP No. GEM/2026/B/7823086 dated 23/07/2026**
Dear Sir/Madam,

| Description | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **NOTE: The Hardware /appliance costing should be inclusive of web server, Application server, Database Server, OS and any other components** | **Specifications (incl Qty)** | **Model** | **Make** | **Latest Release (Model)** | **Latest Release (Make)** | **No. of Cores/ node** | **No. of RAM/ node (GB)** | **Processor Qty/ Node** | **Processor Frequency** | **Processor Cache** | **Storage Quantity** | **Total Storage Capacity** | **Operating System** | **NIC quantity/ node** | **NIC Make** | **Total Cores** | **Total Memory (GB)** | **Other Details** |
| **Data Centre Hardware (DC)** | | | | | | | | | | | | | | | | | | | |
| **Dev/UAT/SIT Hardware** | | | | | | | | | | | | | | | | | | | |
| **DR Hardware** | | | | | | | | | | | | | | | | | | | |
| **Others** | | | | | | | | | | | | | | | | | | | |
| **Total Hardware** | | | | | | | | | | | | | | | | | | | |

Date: ___________
Place: ___________
Signature of Authorized Signatory
Name of Signatory:
Designation:
Official Email ID:
Mobile No:
Telephone No:
Seal of Company: