State Bank of India
Human Resources Department
16th Floor, Corporate Office, Nariman Point,
Mumbai-4000 021
Telephone No: 022-22741620-04
E-mail: dgm.ir@sbi.co.in
Website: https://sbi.bank.in

RFP No.: **SBI/IR(HR)/RFP/2026-27/01** **Dated: 28.07.2026**

Corrigendum:01

Please refer RFP for Selection of Service Provider for Employee Assistance Program (EAP) dated 28.07.2026. Corrigendum and Bank's response to the Pre-Bid Queries are uploaded and can be accessed under Procurement News on the Bank's website https://sbi.bank.in. Sr. No.6&8 of Schedule of Events at page number 6 of RFP dated 28.07.2026 stands amended as,

Last date and time for submission of bids: **20.08.2026 upto 05:00 PM**.
Date and time of opening of Technical Bids**: 21.08.2026 at 05:00 PM.**

The following corrigendum/clarifications are hereby issued and shall form an integral part of the aforesaid RFP. All bidders are advised to take note of the changes contained herein while preparing and submitting their proposals.

1. Letters of Intent (LoIs) will be issued to L1 bidder and the selected bidder will be required to undergo IT & Security review, also called as ISD review. Selected bidder will be required to submit the documents, duly certified by CERT-IN Auditors, for getting clearance from IS Dept. of the Bank as mentioned in **Schedule 3** as well as mentioned any other place in the RFP document. The bidder/ vendor shall have obligation to comply with Bank's IS policy, Cyber Security Policy and IT Policy and regulatory requirements and implement all the recommendations/ close all the vulnerabilities reported in the various information security reviews, IS audit, UAT etc conducted by the Bank, bank appointed third party professionals, Regulators during the contact period without any additional cost to the Bank.

2. Supply Chain Cyber Risk Assessment (SCCRA) Checklist is placed as Annexure R to be submitted by the bidders along with the evidence.

3. Clarifications/Quantifying the **Scope of Work** as sought in the pre-bid query meeting –

Module No.	Module Name	Clarification
1.4	Pan-India Webinar Programme	The Service Provider shall conduct a minimum of one hundred (100) webinars during each Programme Year. All webinars shall be recorded and made available on the platform for a period of one (1) quarter from the date of the webinar.
1.6 (e)	Physical Wellbeing Activities	The Service Provider shall deliver one (1) live virtual instructor-led session during each week, resulting in a minimum of fifty (50) sessions during each Programme Year. Each activity shall be hosted online and made available through live broadcast or virtual streaming to employees and their dependents for the duration of one quarter.
3	Colony and Residential Community Wellbeing Programme	Monthly one (1) offline program to be conducted across twenty-five (25) designated locations, resulting in a minimum of three hundred (300) offline sessions during each Programme Year.
4.1	Mandatory New Joiner Holistic Wellbeing Induction Module	The induction programme shall be delivered through two (2) live virtual instructor-led sessions per quarter, up to a maximum of ten (10) sessions during each Programme Year. Each session shall be recorded and made available on the platform for a period of one (1) quarter from the date of the live session.
5	Maternity and Parental Wellbeing Programme	The programme shall be delivered through one (1) live virtual instructor-led session per quarter. Each session shall be recorded and made available on the platform for a period of one (1) quarter from the date of the live session.
6.1	Champion Certification	The Service Provider shall ensure the certification of a minimum of five (5) Champions per AO within six (6) months from the Programme Commencement Date. Based on one hundred and seven (107) AOs, the Service Provider shall certify approximately five hundred and thirty-five (535) Champions over the certification period.
7.3	Life-Stage Transition Support	The programme shall be delivered through one (1) live virtual instructor-led session per quarter. Each session shall be recorded and made available on the platform for a period of one (1) quarter from the date of the live session.
9.1.1	Platform and Accessibility	The application shall maintain a separate user profile and separate authentication credentials for each registered dependent. The Service Provider shall ensure complete profile-level confidentiality and logical segregation of data. Information relating to a dependent, including service usage, assessments, counselling interactions, appointments and personal information, shall not be visible to or accessible by the primary employee user or by any other dependent.

		Such information may be accessed only by the respective dependent and by specifically authorised personnel of the Service Provider on a strict need-to-know basis for service delivery, supervision, safeguarding, quality assurance or compliance with applicable law. For dependent users who are minors, registration, consent, confidentiality and information-sharing arrangements shall be governed by applicable legal, parental-consent and safeguarding requirements. The Service Provider shall clearly disclose these arrangements before registration and commencement of services.

Other terms and conditions of the tender will remain the same.

Dated: 10.08.2026

Deputy General Manager
Industrial Relations Department (HR)

Annexure R

Supply Chain Cyber Risk Assessment (SCCRA) CHECKLIST

Customer Data Shared for Processing / Storage Offsite

Sno	Control	Domain	Evidence Requirement
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point
2	Whether third party conducts security Assessment of all their applications (SBI related) covering activities (including not limited to) Appsec, API Testing, Source Code Review, DFRA, Process Review, Access Control, Vulnerability Assessment, Penetration Testing etc through regulator/ government (CERT empanelled or others) approved auditors. Any device hosted by Third party in SBI environment should also be covered	Security Assessment	Evidence of latest CERT In empanelled auditors report along with Scope
3	Whether the 3rd Party/Vendor's Servers are suitably protected from external threats by way of security solutions like firewall, IDS/IPS, AV, DLP etc.?	Network Security	Evidence for controls in place
4	Whether the 3rd Party/Vendor's Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc	Network Security	Evidence for controls in place
5	Whether the 3rd Party/Vendor follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT	Network Security	CERT empanelled auditor's Report on verification of its implementation.
6	Whether the Third party periodically monitors/ reviews the firewall rules including that of Open Vulnerable Ports to ensure that only need based rules are in place.	Network Security	Approved Process of Firewall Rules and self-certification (signed by IS Head of the company) for non-presence of overly permissible such as Any-Any Rules or generic rules/evidence for latest FW

7	Whether internal servers are exposed to direct Internet access?	Network Security	Evidence of purpose/need of this and verification of controls in place by CERT empanelled auditors.
8	Whether the privilege access activities are logged, (traceable to a specific user id with no default admin or root id used), monitored, controlled, and governed as per best security practices?	Log Management and Monitoring	Evidence of Privileged access logs and PIMS implementation
9	Whether Sufficient logs for Forensic Assessments are generated, stored securely, and reviewed regularly through a SOC	Log Management and Monitoring	Log generation, storage and review process certified by CERT empanelled auditor.
10	Whether the third party has a dedicated Incident Mgmt. Mechanism to handle Cyber Incidents well within the timelines prescribed as per their internal guidelines?	Incident Management	ISO27001 certification or Evidence showing latest Policy Review and Approval
11	Whether resources deployed by third party for development, are properly skilled /trained in Secure Coding Practices, Secure Data management Practises?	Human Resource Security	ISO27001 certification or Undertaking with Evidence covering the control point
12	Whether third party has a mechanism in place to ensure that the employees of third party return the assets containing SBI/SBI Customer data after role change or completion/ termination of the project or company?	Human Resource Security	ISO27001 certification or Asset Mgmt. Procedures Approved, Asset Issue Register
13	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
14	Whether the 3rd Party/Vendor/Vendor has (Board/Top Management approved) Information Security Policy and Procedures, in place with periodic reviews (minimum annually) by Top Management? The policy should cover below aspects of Information Security: 1. Human Resource Management 2. Asset Management 3. Cryptographic Controls 4. Access Management 5. Log Management 6. Third Party Cyber Risk Management 7. Network Security Management 8. Application Security Management 9. End-point Security Management 10. Incident Management 11. Physical Security 12. Change Management	Governance	ISO Certification or Content Table/ Page of IS Policy and review history page

15	Whether suitable Security certifications (ISO, PCI-DSS, SOC1 and SOC2 etc) of the security posture at vendor environment are in place?	Governance	Certificate with validity period, if available.
16	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e., SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e., 3rd party.
17	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
18	Whether the key management system of the third party ensures segregation and uniqueness of keys for SBI vis-à-vis other clients?	Data Security	Approved Process for Key Mgmt. and Evidence of actual implementation of Key Sharing
19	Whether SBI data, stored at 3rd party, is appropriately segregated from other clients at least through logical isolation at database level?	Data Security	Evidence of logical segregation
20	Whether third party has processes in place to permanently erase SBI data from all environments (LIVE/ archived or data in external media), immediately after the need or clearly defined retention period as per the business engagement? Whether mechanism is in place to monitor the same?	Data Security	Self-certification in case of Govt entity and Approved Purging Process & timeline and Evidence of actual implementation for non-Govt entities duly verified by CERT empanelled IS auditor.
21	Whether Data at Rest encryption is ensured for both Live and archived data/ backup in external media etc? Are encryption keys sored in HSM.	Data Security	Evidence of encryption techniques implemented
22	Whether the third Party has a mechanism to delete all SBI data when consent is revoked by SBI Customer or when the relationship ceases.	Data Security	Regulator/ Govt approved or CERT empanelled auditors report on the secured mechanism implemented for deleting the data.
23	Whether the application and database (containing SBI data) are hosted in Public Cloud? If yes, whether Cloud Security aspects including but not limited to the following are ensured: - a. Is there a Secure Migration Process	Cloud Security	(CERT-In/ Govt/ Regulatory approved Auditors report on the Cloud Control checks provided under section “Critical Data Processed

	b. Is there a Secure Deletion Process c. Is Cloud Security Review performed on regular basis		or Stored in Multi-tenant Cloud"
24	Whether a properly documented Change Management process has been instituted by the 3rd Party/ Vendor?	Change Management	ISO Certification or Change Management Procedures, Release Trackers
25	Whether the Vendor performs periodic DR Drills	Business Continuity	ISO27001 Certification or Evidence of conducting DR drills, and lessons learnt and their detailed recordings.
26	Whether third party has a Patch Management process for all systems is in place and the same is meticulously adhered to as per defined timelines?	Application Security	Evidence of latest patch applied, Patch Mgmt. Procedures
27	Whether the 3rd Party/Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?	Access Management	Role Conflict Matrix and evidence of following the same.
28	Whether third party permits remote access to internal systems/ applications? If yes whether they are secured by MDM and/or VPN through Hardened Mobile devices like Laptop/ Desktop or Mobiles	Access Management	Evidence for implementation of the Control
29	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Software Development and secured usage of Open-Source Tools.	Security Assessment	Regulator/ Govt approved or CERT empanelled auditors report on assessment of the security practices at third party environment
30	Adherence to Continuous Monitoring Clauses in Appendix E of this document	Security Posture Maintenance	Relevant evidence for the Control objectives