

License and Cloud Questionnaire

Sr. No.	Brief Description of Requirement	Vendor Responses
ERS_166	Can you host your application on any of the cloud provider recommended by SBI Life	
ERS_167	What is the maximum number of years of your Cloud Delivery Model and Service Contract?	
ERS_168	Are you also into On Premise Cloud delivery Model	

Mandatory Security / Cloud Security Criteria

The Service provider and/or the Cloud Service Provider (CSP) shall provide following but not limited to security controls:

Overview:

The solution deployed should follow a standard configuration/customization process and shall meet the functional, security, performance, legal & regulatory requirements of SBIL.

The Vendor shall comply with SBIL Information Security Policy and Procedures in key concern areas as under:

- Responsibilities for data and application privacy and confidentiality
- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of SBIL being managed by or assigned to the Vendor
- Physical Security of the facilities
- Incident response and reporting procedures
- Password Policy of SBIL
- Data Encryption/Protection requirement of SBIL
- Server hardening, security policies and Secure Configuration Documents
- Sharing of Background Verification of its personnel, working on SBIL project

The Outsourced vendor's access to IT infrastructure of SBI Life shall be managed as per Third Party Access Standard & Procedure of SBI Life. If required, SBIL Policy on Information security requirement for third-party document will be shared with the successful bidder. SBIL shall carry out Gray Box, White Box and Black Box, VA/PT of the application and underlying infrastructure components through their empanelled information security service provider. In case of any observations or vulnerabilities reported during these testing, the successful Bidder and CSP shall close the observation and mitigate the risk within one month without any additional commercial levied to SBIL. Failure to close the vulnerabilities within one month will attract penalty.

Detailed:

Parameter	Complied (Y/N/NA)	Remarks
1. Service Provider(SP) and/or CSP (Cloud Service Provider) shall provide right to SBIL or its empanelled service providers to audit / conduct security review of the application, its interfaces with other SBIL systems, hosting data centre facility & its IT infrastructure, processes etc. as well as locations from where the SBIL application will be maintained.		

<p>2. SP and CSP shall adhere to Information Technology Act 2000, its amendments and rules published by Government of India as well as SBIL Information Security Policy, Procedures, Guidelines. The SP and CSP shall ensure that they have information security organization in place to implement the provisions of SBI Life's information security requirements and protection of intellectual property.</p>		
<p>3. SP and CSP shall adhere to applicable legal, statutory, contractual and regulatory compliance including Insurance Regulators' obligations for all elements of the information systems, processes and services.</p>		
<p>4. Data centre location for hosting the system and SBIL data shall be at a minimum certified with latest ISO 27001 standard.</p>		
<p>5. Data centre, Disaster Recovery and Business Continuity locations for hosting SBIL systems/application/database with personally identifiable information (PII) shall be with in India.</p>		
<p>6. SP and CSP shall provide data privacy for all the business critical data while at rest as well as during transit. Strong encryption algorithms like RC4, AES-256 shall be used and key exchange shall happen in a secure manner during data transmission.</p>		
<p>7. SP and CSP shall have Backup and network failover systems to maintain availability of network services and shall have DOS & DDOS protection/mitigation technique.</p>		
<p>8. SP and CSP shall have DR site and Business Continuity with Disaster Recovery (DR) Drills periodically to test functionality after getting approval from approving authority of SBIL.</p>		
<p>9. SP and CSP shall implement controls to protect SBIL confidential information, determine who shall access the data, what their rights and privileges are, and under what conditions these access rights are provided. Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis.</p>		
<p>10. Intrusion detection system (IDSs) / Intrusion prevention system (IPS) shall be deployed at the network level for Cloud environment to detection / prevention threats.</p>		
<p>11. SP and CSP shall follow change management system for any change. Mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and product vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.</p>		
<p>12. SP and CSP shall have an effective Incident Management System including Incident Response mechanism to take action when ever any incident takes place. Capability of provider to manage the incident of real world network attacks. Should have Breach strategy in place. All incidents occurred at cloud data enter and LMS service provider's premises shall be informed to SBIL.</p>		
<p>13. SP and CSP shall have multi levels of monitoring, logging and reporting. Audit logs consisting user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.</p>		

14. Servers over cloud shall be hardened as per SBIL secure configuration document.		
15. SP and CSP shall provide data retention as per SBIL policy.		
16. SP and CSP shall provide segregation among multiple client setups with multiple client data.		
17. Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications, OWASP for mobile applications etc.).		
18. The service provider shall adopt a secure software development life cycle during development, deployment, change etc. of the application		
19. Privilege Identity Management (PIM) software shall be used to log, monitor and manage all the activities of system administrators e.g. Operating System, Web server, Application server, Database, Network device, Network security device etc. and shall be integrated with SIEM		
20. SIEM software shall be implemented for SBIL systems/applications/databases and the logs & alerts shall be sent to SBIL, as per our requirement and use cases		
21. DLP (Data Loss Prevention) and Database Activity Monitoring tools shall be deployed for SBIL systems/applications and the logs & alerts shall be sent to SBIL, as per our requirement		
22. SBIL Data shall be shared with us and then on confirmation from us, it shall be permanently destroyed using physical or digital means at all locations, which cannot be retrievable, after expiry of the contract or at termination of the contract. The service provider and the Cloud service provider shall submit a certificate to SBIL in this regard.		
23. Ensure that logs are in tamper resistant stores for accurate legal and forensic analysis. The use of write-once devices, separation of servers used to storage logs from application servers and access controls to servers storing logs are critical aspects of this requirement.		
24. In case SBIL like to monitor the systems/applications/database through its own SIEM or PIM or any other methodology then the service provider needs to provide required access and support for integration.		
25. SBI Life may update from time to time, IT and Information security related policies, guidelines, standards and requirements and will incorporate such updates by reference which shall be notified in writing by SBI Life to SP promptly. SP and CSP is deemed to accept all the updates.		
26. CSP shall have a documented policies and procedures to discharge the information security requirements detailed within this RFP		
27. Internal Audits shall be performed bi-annually by SP and CSP's Internal Audit department/Corporate Governance team/ SP and CSP appointed third party/ External Auditors in order to verify the strength of information security and to validate the compliance with SBI Life's information security policies and standards. Compliance certificate shall be issued in the format as specified by SBI Life and submitted to SBIL on bi-annually basis from an authorized signatory.		

28. SP & CSP shall implement adequate measures to provide access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers) as per SBI Life Protection of Information on BYOD Policy.		
29. The information security responsibilities of all SP and CSP employees working for SBI Life shall be defined by SP and CSP. SP and CSP shall ensure that all information security requirements of SBIL are communicated, to all its employees in relation to their role.		
30. The CSP (Cloud Service Provider) and SP shall provide an undertaking separately to comply with all SBIL requirements related to security, technical and functional.		
31. The SP and CSP shall agree for Escrow of information systems source code for and end of support / proprietary technologies (e.g.' application source code and cryptographic keys) using a trusted external party, such as a legal representative, lawyer or equivalent, as selected by SBIL		

Compliance Statement

DECLARATION BY CLOUD SERVICE PROVIDER & SERVICE PROVIDER

Terms & Conditions

We hereby undertake and agree to abide by all the terms and conditions stipulated by SBIL in the RFP document under Mandatory Security / Cloud Security Criteria. We hereby also agree to comply with all the requirements of SBIL, Deliverables, related addendums, appendices and other documents including any changes, if any, made to original tender documents issued by SBIL.

The cost of service, process, resources, training, documents, rate contract, tools etc finally arrived and accepted by SBIL will be binding on us for period of the contract.

We accept that we, the Bidder, will not levy any other charges on SBIL, in any form to meet the obligations as per scope of this RFP including all deliverable, requirements, terms & conditions etc.

We certify that the services offered by us in response to the bid conform to the security, technical and functional specifications stipulated in the RFP.

Signature &

Designation Seal of

Company