

## Scope of Work for Audit & IT Security Compliance Management Services for Desktop/Laptop

### Objective

To achieve 99% compliance in regards to SBIL IT Security policy & various standards adopted by SBIL. It helps SBI Life to comply with software & other audits conducted by internal as well as external auditors.

### Responsibilities

- Adherence to SBI Life's IT & IS policy as well as Acceptable Usage Policy. Testing and implementing the Secured Configuration Document (SCD) of Desktop operating system as published by SBIL Information Security Team (IST) periodically. (SCD documents will be provided by SBIL)
- Testing of the newly Launched Windows 11 version by Microsoft with the required software, agents and drivers of the hardware used by SBIL. Ensuring that the new version installation complies with the SCD requirements and preparing ISO for the same to be deployed in the SBIL Laptops and desktops.
- Testing and fine tuning of all the new desktop /Laptop hardware purchased with latest approved version of Windows 11 and preparing a ISO for the same.
- Adherence to IT Standards accepted by SBI Life for IT security.
- Installation of windows OS version with appropriate windows security patches approved by competent authority of SBI Life.
- Installing version upgrade of existing approved software's.
- To ensure all endpoints to be part of Active Directory (AD).
- To maintain all agents like BMC remedy, Symantec Antivirus, MacAfee DLP, NAC etc. online on all the endpoints.
- To maintain local administrator password policy and make sure to do not disclose with end users.
- Group Update Provider (GUP) or any Distribution Server (DS) or Relay machines (Local Desktop) in branches are to be connected and updated with centralized servers. On site engineer to be arranged if in case it is not connected to centralized server or not resolved through remote.
- Preventive Maintenance (PM) of all desktops/laptops in branches are need to be done **Physically** once in a quarter at all locations, the list of activities to be carried out during Preventive Maintenance is provided.
- Activities to be carried out in Preventive Maintenance are prepared in the form of checklist and it has to be 100% adhered. Checklist is enclosed along with RFP under section Annexure D.2.
- It is mandatory to complete PM for all assets within 90 day's cycle hence lapses for uncompleted PM will attract penalties as mentioned in RFP.
- PM schedule to be confirmed and intimated to respective SBIL branch & Belapur office.

### Deliverables

- Installation, configuration, troubleshooting of following agents:

Symantec, BMC Remedy, NAC, DLP, TITUS, Trelix, zscaler and any other agents approved by SBIL as mandatory for desktop /laptops time to time during contract period.

- Installation of Operating Systems at least once in a year if the existing version of OS declared End of Support by OEM.
- Implementation of Secured Configuration as per SBIL’s SCD guidelines.
- Monthly windows security patches to be installing in all desktops & laptops.
- Regional audit & inter audit findings about the non-compliance to be targeted as Zero day findings.
- Any audit finding reported by auditor should be closed within the stipulated time given towards closure. Usually closure timing for desktop/laptop is within one week.
- Submission of checklist of PM dully filled & signed off obtained by end user on IT portal form or physical form.
- Any unauthorized software / tool found to be removed immediately & inform to SBIL Belapur Office ASAP in writing.
- Any unauthorized access / user found to be removed immediately & inform to SBIL Belapur Office ASAP in writing.
- Any noncompliance found to be corrected & reported to SBIL CPC Office ASAP in writing.
- Review the end point patch compliance on monthly basis, get the noncompliance report from BMC ITAM system and send the mail to respective employees, management services team and RDs office, risk manager and ensure that system is connected to network and compliance is achieved.
- On quarterly basis Inspection and Audit team carry out the branch audits and verifies below tabulated compliance points, compliance team to ensure that all the below point mentioned point should be address before the audit and no finding should reported with this respect. Coordinate with branch / region team for closure of any open points on top priority.
- In BMC ITAM system compliance related rule and auto remediation is configured, compliance team to monitor these parameters on daily basis and act on any noncompliance points

SR. No.	Function	SUBFUNCTION	AUDIT CHECKPOINTS
1	Branch Sales and Administration	Adherence to Information Security Guidelines	Check the following (i) Unauthorized USB Drive access (ii) Unauthorized software/content installation with respect to the approved s/w list
2	Branch Sales and Administration	Adherence to Information Security Guidelines	Check the availability of Shared folder (if yes then check for approval).
3	Branch Sales and Administration	Adherence to Information Security Guidelines	Check Whether Windows security patches are updated within last 90 days.
4	Branch Sales and Administration	Adherence to Information Security Guidelines	Check Availability of (i) Trelix (DLP) Agent on desktop/laptop( for data leakage prevention) (ii) BMC Client Management Agent is installed and status should be ‘Running’.

5	Branch Sales and Administration	Adherence to Information Security Guidelines	Check whether (i) All users (employees / outsourced) are using their own NT Login ID. (ii) Check whether outsourced staff are using NT login ID of SBIL employees. (Login Id not found should be taken up with Branch or location head) (iii) Only SBILSUADM and NETADMIN local login should be Active and Other user should be disabled.
6	Branch Sales and Administration	Adherence to Information Security Guidelines	Check whether (i) N-1 version of Antivirus software is installed. (ii) Definition of Anti-virus should be one day less than system date (iii) Anti-virus full scan is done once in every week.
7	Branch Sales and Administration	Adherence to Information Security Guidelines	Check Whether N-1 Version of Browser: (a) google chrome (b)Mozilla Firefox (c) Microsoft edge is installed
8	IT Infra best practices	Adherence to Information Security Guidelines	Handy Escalation matrix of IT dept with branch ( print copy pasted on easily readable near to switch/server/UPS room).
9	IT Infra best practices	Adherence to Information Security Guidelines	Check whether Preventive Maintenance activity is carried on quarterly basis and report maintained for all systems (verify the exact count of laptops / desktops from fixed asset register of the respective branch)
10	IT Infra best practices	Adherence to Information Security Guidelines	Availability of GUP machine in each branch and it should be switched on. GUP machine should be tagged for the easy identification.
11	IT Infra best practices	Adherence to Information Security Guidelines	Every system should be shutdown at EOD
12	IT Infra best practices	Adherence to Information Security Guidelines	Availability of physical register with details of person (IT Vendors) visited for services and entered in server room/Network Rack/UPS room as per availability in branch/RO Location.

## **Mandatory ‘Information Security Requirements’**

### **Overview:**

The services, processes and solutions deployed for SBI Life shall follow a standard configuration/customization process and shall meet the functional, security, performance, legal, regulatory and statutory requirements of SBI Life. The participant(s) shall comply to “Guidelines on Information and Cyber Security for insurers”, published by IRDAI on 7th April, 2017 and any subsequent changes in this document. The participant(s) shall also comply with SBI Life IT Policy, Information Security Policy and Procedures, SBI LIFE Policy on Information Security Requirements for Third Party in key concern areas as under:

- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of SBI Life being managed by or assigned to the Vendor
- Physical Security of the facilities
- Incident response and reporting procedures
- Server hardening, security policies and Secure Configuration Documents
- Sharing of Background Verification of its personnel, working on SBI Life project

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

### **Detailed:**

The Bidder shall adhere to IRDAI Information & Cyber Security Guidelines, Information Technology Act 2000, its amendments and rules published by Government of India as well as SBI Life Information Security Requirement for Third Party and any equivalent standard in line with The Service Receiver’s information security policies, procedures and standards. The Bidder shall ensure that they have information security organization in place to implement the provisions of The Service Receiver’s information security requirements.

1. The Bidder shall adhere to IRDAI Information & Cyber Security Guidelines, Information Technology Act 2000, its amendments and rules published by Government of India as well as SBI Life Information Security Requirement for Third Party and any equivalent standard in line with The Service Receiver’s information security policies, procedures and standards. The Bidder shall ensure that they have information security organization in place to implement the provisions of The Service Receiver’s information security requirements.
2. Information security requirements such as controls for maintaining confidentiality, integrity and availability of the SBI Life's data shall be considered at all stages throughout third party/vendors having access/handling the organizational system/data.



Apne liye. Apno ke liye.

3. SBIL may update from time to time, security related policies, guidelines, standards and requirements. SBIL will incorporate such updates by reference which shall be notified in writing by SBIL to The Bidder promptly. The Bidder is deemed to accept all the updates.
4. The Bidder shall have documented policies and procedures to discharge the security requirements detailed within the Agreement.
5. Prior to finalization of order, the Bidder shall allow SBI Life Security Team or its empaneled vendors to inspect and check the designated setup proposed for SBI Life and undertakes necessary corrective actions as may be suggested by SBI Life prior to or during the implementation.
6. All arrangements with external party/vendors shall have a well-defined service level agreement (SLA) that shall specify information security requirements and controls, service levels and liability of suppliers in case of SLA violations, non-mitigation of IS vulnerabilities, IS incidents etc.
7. The Bidder shall ensure that methods of collecting PII/ SPDI are reviewed by its management before they are implemented to confirm that PII/SPDI is obtained
  - a. Fairly, without intimidation or deception and,
  - b. Lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of PII/SPDI.
8. External party shall demonstrate compliance with all SLA requirements such as validating security arrangements for each vendor, handling termination of a relationship with a vendor etc.
9. The Bidder shall provide right to SBI Life or its empaneled vendors to audit / conduct security review of the application, its interfaces with other SBI Life systems, hosting data center facility & its IT infrastructure, security in business processes & operations etc. as well as locations from where the SBI Life application will be maintained.
10. The Bidder shall be subject to a relationship assessment (sometimes referred to as due diligence review) which shall cover:
  - a. Dealing with the said party (e.g. details of provider history, previous and current business arrangement and dispute information)
  - b. The Bidder shall have process of background check on its employees prior to their induction into SBIL project. Level of background checks should meet the sensitivity of information associated with the project.
11. The Bidder shall have process of background check on its employees prior to their induction into SBIL project. Level of background checks should meet the sensitivity of information associated with the project.
12. The contract requirements shall include non-disclosure agreements, roles and responsibilities, and termination clauses and right to inspect/audit by Organization, Law enforcement agencies and regulating agencies including IRDAI.
13. The Bidder shall have a demonstrable level of maturity in relation to information security and their degree of commitment to information security.
14. The Bidder shall record and maintain detailed information of all Personnel who are authorized to access SBI Life Systems or SBI Life Information. All access requirements shall follow Access Control procedure of SBI Life.
15. The list of security controls shall be determined to be implemented based on the type of engagement and nature of information sharing requirement.
16. The data shall be shared with the third party ONLY on “Need to know” basis.
17. The Bidder shall comply with data retention and purging requirements of SBI Life. Compliance certificate for data retention and purging shall be sent to SBI Life as per stipulated time agreed with SBI Life.
18. Confidentiality and non-disclosure agreements with third parties shall be reviewed periodically and whenever the service terms and conditions are changed.
19. Access management for third parties including granting access, review of user access rights shall be periodically assessed and changed as applicable.

20. Personnel who are allowed access to SBIL Information, IT resources and network should have their individual user accounts for authentication and accountability purposes. Access rights granted to the user accounts should be based on job needs, approved by the system owner and reviewed on a regular basis.
21. Logging mechanisms should be enabled on the user accounts. If privileged accounts - like administrator, auditor etc. are used, then the logs should be set up to capture all activities carried out using these accounts. In addition, all necessary logs should be periodically reviewed. The review reports should be produced on request.
22. A consistent method for securely handling the termination of relationships with Parties shall be established which shall include:
  - a. Designating individuals responsible for managing the termination
  - b. Revocation of physical and logical access rights to the organization's information
  - c. Return, transfer or secure destruction of assets (e.g. 'back-up media storage' documentation, hardware and data.)
23. The Bidder shall adhere to SBI Life's license agreements and intellectual property rights
24. The Bidder shall implement Security Incident Event Management (SIEM) software for SBI Life systems/applications/databases/Information and the logs & alerts shall be sent to SBI Life, as per our requirement and use cases
25. 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.
26. In case SBI Life decides to monitor the systems/applications/database/Information through its own SIEM or PIM or any other methodology then the Bidder needs to provide required access and support for integration.
27. Independent security assessments (VAPT, Configuration Review, Network Security Review etc.) as applicable shall be performed by the Bidder for the application(s) and related infrastructure components (collectively referred as 'Information Processing Facility') used to provide service to SBIL through a Cert-In Empaneled Information Security Service provider by the bidder at least annually by the selected participant. Bidder on selection shall submit periodic (annually/bi-annually) integrity & compliance statements of information processing facility used for accessing/processing data or providing services to SBIL (Customer), providing for reasonable level of assurance that the setup is free of malware & viruses, free of any obvious bugs, free of any covert channels in the code and free of any known vulnerabilities and the same should be fulfilled through Cert-In empaneled vendor as appointed by the selected bidder without any additional commercials.
28. As per applicability Mechanisms shall be implemented by the Bidder for vulnerability and threat 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. SBIL (Customer) may ask selected Bidder for submission of security review reports (VAPT, Application Security, Configuration Review, Gray box, Secure Code Review Network Security Review etc.) on a half yearly basis or from time to time through a Cert-In empaneled vendor as appointed by the selected participant. In case of any vulnerabilities detected during the security review, selected bidder is expected to close the high-risk vulnerabilities within one day and other vulnerabilities within one month, or as per mutually agreed timelines with SBI Life without any additional commercials.
29. As a part of pre-engagement due diligence and also as part of a yearly activity, the selected bidder needs to undergo 'Third Party Security Control Checklist' or also known as the controls to be implemented by third party checklist of SBIL Life and the same should be validated by a CERT-In empaneled information security service provider for each time and the report of same needs to be submitted to SBILife without any additional commercials. The SBIL shall reserve the right to verify this validation report and ask for additional evidences, if any, or visit the site to verify the controls.

30. In case of any VPN connectivity or Leased Line connectivity with SBIL by the selected participant/bidder, hardening of desktops/Laptops as per SBILife provided hardening/SCD document to be carried out along with deployment of Antivirus, EDR, DLP solutions, monthly security patch updation to be deployed on the desktops/Laptops. The SCD/Hardening review to be carried out through a CERT-In empaneled information security service provider and the report to be submitted to SBI Life. The SBIL shall reserve the right to verify this validation report and ask for additional evidences, if any. This process should be repeated every year through a CERT-In empaneled information security service provider and the reports to be submitted to SBI Life.
31. The operating systems, web servers, database etc. used for processing SBIL's information shall be hardened in line with CIS (Center for Internet Security) Benchmarks and configuration review of these systems shall be performed at least yearly.
32. In case of renewal, the security considerations in line with the Prior to engagement scenario shall be considered.
33. There shall be formal, documented standard/procedures for performing information risk assessments, which apply across the organization. Standards procedures to cover types of target environment that would be assessed for information risks, e.g. IT Applications, hardware and software, vendors, etc.
34. SBI Life may obtain periodic integrity & compliance statements, for application and related infrastructure components used for SBI Life project, in writing from the selected Bidder providing for reasonable level of assurance about the setup being free of malware & viruses, free of any obvious bugs, free of any covert channels in the code, and free of any known vulnerabilities.
35. SBI Life's Information Security Team/ Inspection Audit department shall conduct audit for third party /vendors handling critical data on planned and ad hoc basis to measure the effectiveness of the third-party security controls implemented.
36. The Bidder shall be ISO Certified for the designated line of business e.g. ISO 27001, ISO 22301 preferably etc. If the Bidder is not certified, then they should adhere to the requirement of these aforesaid standards.
37. The Bidder should ensure that appropriate technology measures are in place to protect the storage and exchange of information. These measures may include the following, but not limited to:
  - i. The Bidder shall maintain integrity of the software in use, including patch upgrades, operating systems and applications.
  - ii. Mail attachments should be encrypted before sending as the traffic could be sniffed in transit, leading to unauthorized disclosure and modification of information.
  - iii. The connectivity between the Bidder and SBI Life shall be encrypted and data transfer shall be via Secure FTP
  - iv. The Bidder shall have secure connectivity to the SBI Life's central data center in active fail-over mode and to disaster recovery center.
38. Prior to finalization of order, the Bidder shall allow SBI Life Security Team or their representative to inspect and check the designated setup proposed for SBI Life and undertakes necessary corrective actions as may be suggested by SBI Life prior to or during the implementation.
39. The Bidder is required to disclose the method of data storage in their proposed solution. If the Bidder chooses to store the SBI Life data on cloud, the Bidder shall be subject additional security assessment in alignment with SBI Life Cloud Security Requirements
40. Bidder should have defined Business Continuity Management and Disaster Recovery (BCM-DR) procedures in place for effective handling of critical business processes in situations of any incident disrupting the business including
  - i. Backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans.
  - ii. Bidder should have proper updating of the procedures in regular intervals to ensure effective and smooth functioning of such procedures.



Apne liye. Apno ke liye.

iii. Business recovery time frames supported by setup should meet SBIL's the business requirements.

41. The Bidder shall comply with all legal, regulatory and statutory requirements.

Type	Severity	Response TAT	Resolution TAT
Incident	Critical	5 min	15 min
	High	10 min	30 min
	Medium	15 min	45 min
	Low	30 min	2 hr
Work Order	2 hrs		