

### Annexure - VII - Due Dilegence Checklist

Sr. No.	Domain	Areas	Check / Observation	Description	Response
1	Asset inventory and configuration management	Asset Inventory	Do you prevent removal of client related assets (storage media, hardware) from the premises? Please provide details.	Assets which are in use to provide services to client should be removed after getting proper approval from client.	
2	Asset inventory and configuration management	Asset Inventory	Do you have an application or process for inventory tracking? If yes, how often is the physical inventory validation performed?	Asset inventory should be tracked and maintained	
3	Asset inventory and configuration management	Asset Security	Do you have controls to safeguard the information during transport? Please describe if the process of loading and unloading is conducted in a controlled environment. Describe the container used for transport	Security controls like, shock proof and fire proof media case should be used to transport sensitive assets, loading unloading areas should be properly protected and guarded.	
4	Asset inventory and configuration management	Asset Security	Do you have documented procedures regarding the movement of assets (both inside and out of your organization)?	Guidelines for movement of assets should be documented	

5	Asset inventory and configuration management	Asset Security	Do you have a documented process to pass the custody of the assets between locations?	Guidelines for movement of assets should be documented	
6	Asset inventory and configuration management	Asset Security	Do the procedures for the disposal, reuse, or repair of electronic media (e.g. end-user devices, tapes, disk drives, multifunction devices, copiers) require degaussing and/or data erasure and/or destruction to ensure that the data cannot be recovered? If so, what standard (beyond simple deletion or formatting) do you use for data destruction?	Low level formatting or data degaussing or destruction should be performed, prior to dispose / reuse / repair of any equipment containing client data	
7	Asset inventory and configuration management	Asset Security	Do you have a documented process for removing physical property, such as hardware, backup tapes, from the premises?	documented process for removing physical property, such as hardware, backup tapes, from the premises	
8	Business Continuity	Continuity of Business Operations	Does a BCP plan guide the continuity of business operations at the time of a disaster?	Continuity of vendor business operations at agreed service levels should be defined by a well-documented BCP / DR policy. The Vendor should have a sound BCP strategy to ensure continued operations.	

9	Business Continuity	Continuity of Business Operations	Does vendor identify the events that cause interruptions to various departments supporting various business activities	Have vendor performed risk assessment to analyze associated threats and vulnerability with the concerned business process.	
10	Business Continuity	Continuity of Business Operations	Have the training plan of Business continuity plan for various department is identified.	BCM training is required to ensure that effective continuity strategy is in place	
11	Business Continuity	Continuity of Business Operations	Do the business continuity plans describe in detail about roles and responsibilities describing who is responsible for executing all aspects of the plan.	The BCP should clearly state the roles and responsibilities of individuals at the time of a disaster.	
12	Business Continuity	Continuity of Business Operations	Are the plans reviewed on periodic basis and on every significant change to environment	Changes in Assets, Business Operations should trigger the changes in the Business Continuity Plan of the Vendor.	
13	Business Continuity	Continuity of Business Operations	Does the Vendor have alternate facilities equipped to resume business operations in case of a disaster?	The Vendor must have alternate processing facilities to resume critical activities in case of a disaster. The vendor could resort to having a hot site, warm site or a cold site arrangement.	
14	Business Continuity	Continuity of Business Operations	Are the Business continuity arrangements are tested and updated regularly? Does vendor regularly test and update business continuity plans to ensure their effectiveness	Testing business continuity plan is required to analyze effective recovery strategy is in place	

15	Business Continuity	Continuity of Business Operations	Are the provisions made for the periodic transfer of backup media to a secure offsite storage facility?	Necessary backup media and restoration procedures should be ensured to ensure resumption of operations at the vendor facility.	
16	Business Continuity	Continuity of Business Operations	Are services provided to SBI Life covered under scope of BCP	Services provided to SBI Life should covered the scope of BCP.	
17	Business Continuity	Continuity of Business Operations	Issues faced during testing and the action taken for the same are documented?	Issues faced during the BCP testing and the action taken should be documented.	
18	Business Continuity	Continuity of Business Operations	Evacuation drills conducted - Observations & action taken Report are maintained?	Evacuation drills conducted - Observations & action taken should be placed.	
19	Change Management	Change Management Process	Do you have a documented change control policy or program that has been approved by management? If yes, please describe it.	The vendor must follow a well documented, management approved change management process. The change management process should include necessary approvals.	
20	Change Management	Change Notification	Has the vendor documented detailed procedure for identifying of changes to be notified to SBI Life, sending an approval request & communication process	Vendor should maintain necessary documents for communication of changes and obtaining the approvals from SBI Life	
21	Change Management	Change Management Process	Is there an established SPOC for notifying these changes and ensuring documentation?	The Vendor SPOC should be responsible for communicating the changes and maintaining an updated list of changes.	

22	Change Management	Change Management Process	Do you follow your standard change control policies and procedures for changes required throughout the Software Development Lifecycle (SDLC) process? If not, please explain how you control changes in the different SDLC phases.	Vendor must plan and test all the changes prior moving to production to ensure effective change management procedure. Development and production environment must be separate to ensure confidentiality of production data, continuity of application as development may lead to downtime and unauthorized access to production data may lead to compromise with integrity	
23	Change Management	Change Management Process	Do you perform a security review for any changes as part of the overall change approval process?	After applying every change, security review should be carried out to analyze whether any new vulnerabilities are arise due to the applied change	
24	Change Management	Change Management Process	Are logs maintained , capturing all relevant details, whenever a change is effected.	Logs are required to analyze what all steps performed for any change moved to production	
25	Change Management	Change Management Process	Does the vendor organization maintain Audit Trail of all the change requests?	Audit trails are required to analyze what all steps performed for any change moved to production	
26	Change Management	Change Management Process	Is the change management process reviewed on periodic basis and on every significant change to environment	The change management process should be reviewed on a periodic basis. Inclusion of Assets, Changes in Location, modification in system configurations trigger the initiation of the Change management routine.	

27	Change Management	Emergency Changes	Has provider documented a process for handling emergency changes to ensure that these types of changes are carried out in controlled & timely manner	In addition to conventional changes, the vendor has to have procedures for emergency changes.	
28	Change Management	Emergency Changes	Does the process mandate the implementer to document a post implementation report detailing reason for change, steps involved and implementation results	Unlike conventional change processes, Emergency changes are not preceded by approvals and communication process prior to implementation but has to be documented.	
29	Change Management	Emergency Changes	Does the process mandate change management committee to review the implementation report & ask implementer to roll-back the change if it doesn't meet the desired objective	There must be a procedure to monitor the implications of the change and a roll back strategy.	
30	Change Management	Change Management Process	Does your formal change control process ensure that systems are tested in an environment with production quality & security controls?	Changes should be tested in production equivalent environment to ensure that change will work properly in actual production environment, without any issue	
31	Change Management	Change Management Process	Are your third parties required to notify you of any changes that might affect services rendered? If yes, please describe.	Any changes to third-party systems, which serves to SBILife, should be notify to SBILife to take necessary action at SBI Life	
32	Change Management	Change Management Process	Do you have a change process that ensures your production and back up environments (technology) remain in sync? If yes, please describe.	Production and Backup environment should be in sync with minimum gap, keeping in mind the RPO and RTO of SLA with clients and company requirement.	

33	Compliance and Legal	Agreements	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards	Monitoring of compliance	
34	Compliance and Legal	Internal Audit	Do you have an internal department (i.e. Audit, Compliance, etc.) who is responsible for testing/auditing against legal and regulatory requirements related to your business?	Team / personnel should be identified to perform various legal / contractual / regulatory related assessment	
35	Compliance and Legal	Internal Audit	If yes, how does your internal audit function determine the scope and frequency of your internal audits?	Describe the function of internal audit team.	
36	Compliance and Legal	Internal Audit	If yes, to which most senior level or role in your organization are audit reports issued?	Internal audit / assessment should be carried out as per legal / regulatory / contractual requirements and reports should be communicated to concerned parties	
37	Compliance and Legal	Compliance Framework	What framework / standard for internal control (e.g. COSO, ISO 27001) have you adopted? Do you have a process for independent validation of the design and operating effectiveness of your internal controls specifically related to the proposed services?	Standard / Framework should be adopted to implement effective internal control and processes.	
38	Compliance and Legal	Compliance Framework	Have you had any external audits in the last 18 months (e.g. ISO 27001)? If yes, please provide results.	External Audit against standards like ISO 27001	

39	Data Governance	Backup Management	Are back-up copies of essential business information and software taken regularly?	Backup operations are necessary during the restoration operations in case of a system outage.	
40	Data Governance	Backup Management	Is there a backup and recovery document?	Backup and recovery document should be maintained	
41	Data Governance	Handling Backup Media	How is access to backup media controlled?	Access to backup media should be controlled to prevent leakage of information stored in them.	
42	Data Governance	Handling Backup Media	Is backup media stored in fireproof environment?	Backup media should be protected with requisite controls to prevent environmental damage.	
43	Data Governance	Handling Backup Media	Is there a procedure for media rotation?	Reusability criteria for media should be well established and must be within the limits for media type.	
44	Data Governance	Handling Backup Media	What are the precautions taken for media (aged/unused) disposal?	Careless disposal / re-use of media could result in leakage of bank's sensitive information. Storage devices containing bank's information should be physically destroyed or securely overwritten, prior to disposal.	
45	Data Governance	Handling Backup Media	Is back-up of confidential data protected by means of encryption?	Encryption ensures confidentiality of backup data .	
46	Data Governance	Handling Backup Media	Are the back-ups stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site?	Appropriate backup management Procedure are in place and followed.	



47	Data Governance	Handling Backup Media	Is the back-up information( at off-site) given an appropriate level of physical and environmental protection consistent with the standards applied at the main site?	Appropriate backup management Procedure are in place and followed.	
48	Data Governance	Retention and Restoration	Does the backup policy identify the period for backup data retention?	The data retention period for backup data must be communicated to the vendor and must be followed.	
49	Data Governance	Retention and Restoration	What are the steps followed in restoring backup? Are the steps documented and available to the authorized personnel?	Procedures for restoration testing should be documented and followed adequately.	
50	Data Governance	Retention and Restoration	Is the media and back up restoration tested periodically?	In addition to the backup of data and system files, adequate testing for restoration must be performed to ensure that the backup data is usable.	
51	Data Governance	Data classification	Does your organization have a clearly-defined and documented information/data classification scheme?	Approved Data classification scheme should be communicated and available to all	
52	Data Governance	Data classification	Are your data labeling and handling procedures aligned with your information/data classification scheme?	data labeling should be done as per the approved data classification scheme	
53	Data Governance	Data classification	Do you have a documented records retention policy or program that has been approved by management? If yes, please attach or describe it.	Describe the record retention policy	

54	Data Governance	Data classification	Do you separate SBIL data logically or physically from other client data? If yes, please describe your process	SBIL data should be protected for unauthorized access	
55	Data Governance	Data ownership, stewardship, and data transfer	Do you have data loss prevention (DLP) / data rights management (DRM) controls for managing client data? If yes, please describe. If no, SBIL may implement DLP / DRM solution for at your processing facilities, where SBIL data is being processed and you need to provide necessary support.	Client data should be protected against unauthorized access/modification/disclosure by means of DLP or DRM controls	
56	Disposal, eradication, and destruction management	Data Governance	Do you have a process to remove data prior to decommissioning equipment that housed, stored, processed, controlled or accessed confidential information?  Describe your procedures for the decommissioning process. Describe if the same procedure is utilized for non-repairable equipment.	Low level formatting or data degaussing should be performed, prior to decommissioning of any equipment containing client data	
57	Email Security	Information exchange policies and procedures	Have vendor defined Email security policy or Email policy?	Email security policy is required to define safe acceptable email usage by employees.	

58	Email Security	Information exchange policies and procedures	Are the users aware of their responsibilities with regards to information protection that is exchanged using all types of communication facilities	User responsibilities are generally highlighted in Acceptable usage policy to define what is expected from users/employees which is in line with Organization policies and procedures	
59	Email Security	Provision of e-mail access to users	Are user e-mail accounts at the Vendor facility created after necessary management / HR approvals?	E-mail accounts for communication with SBI Life should be created after necessary approvals and must be commissioned on a need only basis.	
60	Email Security	Provision of e-mail access to users	Are there well-documented procedures for disabling or removing e-mail accounts after the employee leaves?	There must be a defined procedure for disabling/removal of user e-mail accounts on employee termination / transfer.	
61	Email Security	Provision of e-mail access to users	Are the e-mail accounts shared between users?	Sharing of e-mail ids between users obviates accountability for the communication.	
62	Email Security	Secure Configuration of the E-mail infrastructure	Is the e-mail systems are configured for sending mails to non-SBI Life ids?	Access rules have to be configured on the e-mail system to ensure that the same is used for communication with SBI Life only.	
63	Email Security	Secure Configuration of the E-mail infrastructure	Are the mail backups encrypted at the time of storage?	The PST backup of the e-mails should be encrypted during storage.	
64	Email Security	Secure Configuration of the E-mail infrastructure	Is the retention period defined for backed up mails? Is email data purged after the retention period is complete?	The retention and purging procedures should be followed as per defined policy.	
65	Email Security	Secure Configuration of the E-mail infrastructure	Are the mail attachments scanned for Virus and other malicious content?	Virus and malicious content may affect the systems at the Vendor premises and e-mails received/sent have to be scanned for suspicious content.	

66	Email Security	Secure Configuration of the E-mail infrastructure	Do you encrypt emails that contains SBI Life information before it leaves the organization? If you encrypt information, describe the encryption mechanisms you use.	Mail attachments should be encrypted before sending as the traffic could be sniffed in transit, leading to unauthorized disclosure and modification of information.	
67	Email Security	Secure Configuration of the E-mail infrastructure	Does e-mail communication from the vendor include a standard disclaimer as a part of the contents?	Standard disclaimers should be a part of all e-mail communication with SBI Life.	
68	Email Security	Secure Configuration of the E-mail infrastructure	Does the Vendor have an e-mail administrator with defined responsibilities for secure configuration and maintenance?	The e-mail administrator should have the responsibility of configuration and maintenance of e-mail related activities of the Vendors. This responsibility may be shared by a system administrator.	
69	Encryption management	Encryption requirements	Do you have a documented encryption policy or program that has been approved by management? If yes, please provide or describe.	Encryption policy should detailing type of encryption methodology allowed, in line with regulatory / legal / contractual requirement should be documented and approved	
70	Encryption management	Encryption requirements	Does your encryption policy dictate when and how encryption should be employed?	Encryption policy should clearly dictates that what, when and how of the use of encryption	
71	Encryption management	Encryption requirements	Are laptops, mobile devices, or removable media, encrypted with a strong industry standard algorithm?	information assets / endpoints should be encrypted with approved strong encryption mechanism	

72	Encryption management	Device Inventory	In instances where a hardware token or smartcard is used to access an application or system, are the token devices inventoried in a secure system that manages the lifecycle of the token or smartcard?	Inventory of devices should be reviewed periodically to prevent any kind of misuse	
73	Encryption management	Encryption requirements	Is SBIL data/information encrypted while at rest (i.e. stored in databases, applications, disk storage, or backup media)? If yes, please name the encryption algorithm you use to protect the data in storage and backup files.	SBIL data should be stored securely and protected against unauthorized access / modification / disclosure	
74	Encryption management	Encryption requirements	Do you encrypt data transmission on external networks? If yes, which network segments are involved and where is encryption terminated?	All communication should be protected by means of encryption	
75	Encryption management	Encryption requirements	Do you encrypt data transmission on internal networks? If yes, on which network segments? Where is encryption terminated on the internal segments?	All communication should be protected by means of encryption	

76	HR	Pre-employment	Do you perform background checks on employees? Please describe what all check program / procedure includes during screening procedures.	Extensive background checks on the employees / vendor being hired by the vendor will serve as a good preventive control. Any history of suspicious incidents for the employees to be hired has to be analyzed, verified and must influence the selection process. Typical checks included under employee background checks would include Criminal, Academics, Credit and Reference verifications.	
77	HR	Pre-employment	Are any employees or officers of your company exempt from background screening?	If a screening criterion is not required for all employees, please describe the circumstances under which such screening is required.	
78	HR	Pre-employment	Does the aforementioned screening process apply in its entirety to non-employees (e.g. contractors, temp labor, and subcontractors)? If not, please describe the variance.	Extensive background checks on the employees / vendor being hired by the vendor will serve as a good preventive control. Any history of suspicious incidents for the employees to be hired has to be analyzed, verified and must influence the selection process.	
79	HR	Pre-employment	What criteria does your company use to fail or reject a candidate and/or employee based upon the results of a background check?	Describe the criteria / circumstances in which background check could be excused	
80	HR	During Employment	Are your employees required to sign a Non-Disclosure (NDA)/Confidentiality Agreement?	The vendor should apprise its employees on the criticality of data being handled at the premises and sign a NDA at the time of employment	

81	HR	During Employment	Are security roles and responsibilities of employees, contractors and third party users defined and documented in accordance with the organization's information security policy?	Vendor's Management shall ensure that its employees and contractors are properly briefed on their information security roles and responsibility prior to being granted access to confidential information or information system of SBI Life	
82	HR	During Employment	Do you have a well defined process for assigning a "need to do" access to its employees?	Is the access to Client data to employees available on a "need-to-know" and "need-to-do" basis?	
83	HR	During Employment	Do you have a documented, acceptable-use policy that has been approved by management, published, executed, and communicated? If so, please attach or describe it.	An acceptable usage policy document highlighting the recommended information handling guidelines should be circulated to the employees.	
84	HR	During Employment	Does the you have a well defined formal disciplinary process for employees who have committed a security breach?	The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security.	
85	HR	Termination of Employment	Describe the disciplinary action for violations of company policies and procedures?	An effective employee termination process should be available with the Vendor to avoid the loss of SBI Life related information and the restriction/removal of access rights to users who are handling SBI Life data.	

86	HR	Termination of Employment	Do you have procedures to manage access by employees and contractors who have been terminated, transferred, or whose status has changed? If yes, please describe.	There should be an effective communication mechanism to apprise the system admits to manage employee access rights at the time of termination and the user access profile lest should be updated.	
87	HR	Termination of Employment	Do termination procedures include the return of all corporate assets and media?	Vendor shall establish the procedure for user termination and returning of asset on termination of employment.	
88	HR	Employee Awareness and Training	Do you have an Information Security training curriculum? If yes, please describe.	An information security awareness program should aim to make employees and, where relevant contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged during induction training	
89	HR	Employee Awareness and Training	How often is the curriculum updated? Please describe.	An information security awareness program should aim to make employees and, where relevant contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged during induction training	



90	HR	Employee Awareness and Training	Do you organize periodic trainings and awareness programs to convey the criticality of data being handled at the premises?	Emphasis on the criticality of SBI Life specific information should be highlighted in the training sessions. The training sessions should be periodically conducted by the vendor. The programs in addition to focusing on the technical competencies should also focus on the security aspects of the SBI Life information being handled.	
91	HR	Employee Awareness and Training	Do you have appropriate metrics for measuring and monitoring the effectiveness of the SBI Life related trainings imparted to the members?	Appropriate metrics should be available with the Vendor for the monitoring the effectiveness of the Awareness and Training Programs undertaken. Typical evidences would be the periodic tests conducted through quizzes and the employee responses in terms of scores.	
92	HR	Employee Awareness and Training	Do you have controls to ensure that employees complete required training? If yes, please describe.	Appropriate tracking mechanism should be implemented to track the employees who has not attended and completed the training / awareness program.	
93	HR	Employee Awareness and Training	Is action taken on non-performers in the SBI Life related training sessions?	Is the performance of the employees in the awareness sessions monitored and is ensued by appropriate actions for non-performers? Failure to do so might send wrong signals across the organization and might reflect in the work environment too.	

94	HR	Malicious insider risk	Does your company have documented policies or procedures relating to segregations of duties, the use of dual controls, and employee tracking and observation protocols, including logging and supervision? If yes, please provide or describe.	conflicting roles / duties should be identified and accordingly segregation of duties should be done	
95	Incident Management	Incident Notification	Do you have a documented information security incident management policy or program that has been approved by management? If yes, please attach or describe it.	Incident security policy should be well documented, approved, circulated to all concerns and should be at least reviewed on yearly basis.	
96	Incident Management	Incident Management	Do you have a process to notify clients of instances of non-compliance impacting them (including, but not limited to, privacy breaches and legal and regulatory-related incidents)? If yes, please describe.	SBI Life should be informed of all security incidents at the Vendor premises.	
97	Incident Management	Incident Management	Are all users informed of formal procedures for reporting the different types of security incident? Is escalation matrix readily available with users?	The vendor should inform the formal procedure of security incident reporting mechanism and escalation matrix for the same to all users	
98	Incident Management	Learning from Incidents	Do you document and test your information security incident management and response procedures at least annually?	Adequate incident management procedure should be in place.	

99	Incident Management	Learning from Incidents	Do you have an information security incident management process that tracks, analyzes, and determines details, including root cause and corrective actions for all reported incidents?	Adequate incident management procedure should be in place.	
100	Incident Management	Learning from Incidents	Do you conduct a postmortem review after an information security incident to identify the root cause and decrease the likelihood of a similar incident in the future?	Adequate incident management procedure should be in place.	
101	Information Security Management Systems	ISMS Documentation	Do you have a documented information security policy or program that has been approved by management? If yes, please attach or describe it.	Approved Information Security Policy should be in placed	
102	Information Security Management Systems	ISMS Documentation	Do you publish and communicate your information security policy or programs to employees and contractors? If yes, please describe how you communicate them.	Information Security Policy should be available to all concerned stakeholders, any changes / revisions should be communicated to stakeholders.	
103	Information Security Management Systems	ISMS Documentation	Do you publish and communicate information security policies and standards to your Third Parties? If yes, please describe how you communicate them.	Information Security Policy should be available to all concerned stakeholders, any changes / revisions should be communicated to stakeholders.	

104	Information Security Management Systems	ISMS Documentation	Do you review your information security policies and standards annually and update them as needed? If yes, please describe the process.	Information Security Policy should be reviewed, updated and approved at-least annually	
105	Information Security Management Systems	ISMS Documentation	Have you appointed an owner to manage and maintain your information security policies, standards, and initiatives, as well as related activities? If yes, please provide the name and position/title of the owner.	Individual / team should be identified to manage information security program	
106	Information Security Management Systems	ISMS Documentation	Do you have a documented process to approve exceptions to the established security policies? If yes, please describe the process.	Exception management process should be documented and implemented	
107	Information Security Management Systems	SOD	Do you have an mechanism to segregate the duties of information security roles from operational roles?	conflicting roles / duties should be identified and accordingly segregation of duties should be done	
108	Information Security Management Systems	Compliance	Are processes in place to ensure compliance with local, state, and national information security regulations?	Compliance requirement with regulatory / laws / contractual obligations should be identified and all processes should be in line with these requirements	

109	Information Security Management Systems	Compliance	Do you have documented information security risk assessment, remediation, and acceptance policy(ies) or program(s) approved by management? If yes, please attach or describe it.	Information security program should be approved and implemented	
110	Information Security Management Systems	Compliance	Do you monitor the results of your information security risk assessment programs and address gaps, threats and vulnerabilities in a timely manner?	Tracking of gaps, identified during various assessment should be done and implementation should be monitored	
111	Logging and Monitoring	Logging Requirements	Do you have a documented logging and monitoring policy or program that has been approved by management? If yes, please provide or describe.	The provider should ensure that there are adequate requirements for the logging of events on the service. Requirements should be defined and documented.	
112	Logging and Monitoring	Logging Requirements	Have you enabled logging for applications, OS platforms, and network devices in accordance with security best practices to track user activity?	logging should be enabled for all available environment / device / application	
113	Logging and Monitoring	Logging Requirements	Do you periodically review the event logs (e.g. unsuccessful logons, access violations, privileged access)? If yes, please describe.	A process for regular review of security logs must be established to identify relevant information contained within, alarms for preventative and corrective actions, and significant security incidents.	

114	Logging and Monitoring	Protection of Logs	Are information systems audit tools (e.g. software, data or log files used for security, audit, compliance) protected and separated from development and operational systems and not held in tape libraries or user areas?	Information Systems audit tools should be protected by appropriate access control and security controls	
115	Logging and Monitoring	Protection of Logs	Are security audit logs copied to a separate and secure environment?	Audit logging procedure should be documented and Administrator logs should not be accessed / altered / deleted by themselves.	
116	Logging and Monitoring	Logging Requirements	How long do you retain system event and audit logs, both in on-line and off-line storage?	Audit log should be stored as per contractual / legal / regulatory requirements	
117	Logging and Monitoring	Monitoring of Logs	Are you correlating log information from divergent devices, such as firewalls, IDS, and system logs? If yes, how are you aggregating and correlating the information?	Unsuccessful attempts to gain access to systems and applications should also be logged and analyzed for irregularities. Patterns in the logs can be used to detect and plug unauthorized attempts.	
118	Logging and Monitoring	Logging Requirements	Do systems and network devices utilize a common time synchronization service?	There should be time synchronization between network elements for logs to be used for incident management.	
119	Logging and Monitoring	Monitoring of Logs	Do you have a control or process to review or detect unauthorized changes to files/logs/systems/web pages on production systems (e.g. file integrity monitoring software)? If yes, please describe.	Log monitoring should be done for critically identified commands / events for various systems	

120	Logging and Monitoring	Monitoring of Logs	Do you set thresholds for normal activity on systems, networks, databases, and applications to better monitor and detect suspicious or abnormal activity and behaviors?	Threshold limits should be set for at-least critically identified commands / events / activities	
121	Logging and Monitoring	Monitoring of Logs	Do you monitor for security incidents on a 24/7 basis?	do you have team to monitor alerts / incidents raised round the clock	
122	Logical Access Control	User Account Management	Do you have a documented access control policy or program that has been approved by management? If yes, please provide or describe.	Access control policy should be approved by top management and all accesses should be regulated as per the approved policy.	
123	Logical Access Control	User Account Management	Is the access to systems and data on a "need-to-do" basis?	The access to applications and systems should be provided on a "need to do" basis to avoid unauthorized/unrestricted access to SBI Life data.	
124	Logical Access Control	User Account Management	Is there a well defined process for creation of New user accounts?	New user accounts in the Operating System and the Application should be created at the directive of the HR and the SPOC should be apprised of the same. The administrators should obtain necessary approvals before user account creation and allocation of privileges to the users.	

125	Logical Access Control	User Account Management	is there formal user registration process include using unique user ID's so that users can be linked to and made responsible for their actions and the use of group ID's should only be permitted where they are suitable for the work carried out.	All user id must be unique to define accountability and group id must be assigned to a user as an owner	
126	Logical Access Control	User Account Management	Do all accounts (e.g. user, service, privileged, test) have a designated owner?	Ownership of the all logical accounts should be defined and documented.	
127	Logical Access Control	User Account Management	Do you identify all system users by a unique User ID?	Sharing of user ids between users obviates accountability for the communication.	
128	Logical Access Control	User Account Management	Are there procedures to verify or identity a user prior to providing a new, replacement or temporary password	Procedure to verify or identify user prior to handing over the temporary password if user is calling over phone for password change or reset.	
129	Logical Access Control	User Account Management	Are users required to authenticate prior to changing their password?	Procedure to verify or identify user prior to handing over the temporary password if user is calling over phone for password change or reset.	
130	Logical Access Control	User Account Management	How are temporary passwords communicated to users? Is a secure password distribution mechanism in place?	Process for communicating temporary passwords to requested user.	
131	Logical Access Control	User Account Management	Does a System shall prompt for forceful changing of password after the first login	Changing of password on first logon ensures that confidentiality of password is maintained	



132	Logical Access Control	User Account Management	Is there a well-defined process for removing the user account and access rights at the time of an employee leaving the vendor facility?	There should be established process to handle employee termination and the deletion of user accounts and access profiles. User accounts existing in the systems after the termination of the employee could be misused.	
133	Logical Access Control	User Account Management	Is there a periodic audit of the user access profile by the system administrator?	The user access profile of the vendor should be periodically monitored and updated.	
134	Logical Access Control	User Account Management	Is there an automatic lockout for predefined number of unsuccessful attempts?	Unrestricted systems and applications are prone to Brute-force attack to gain access into the system to gain unauthorized access to application and data.	
135	Logical Access Control	User Account Management	After how many consecutive failed log-in attempts are user IDs disabled?	Failed log-in attempts should be defined to avoid rainbow / dictionary attack on user accounts	
136	Logical Access Control	User Account Management	Are different accounts and passwords used for applications and OS level access?	The SBI Life specific applications should be managed by different user IDs and passwords.	
137	Logical Access Control	User Account Management	Do you have established password requirements? If yes, please attach or describe.	Password policies mandate the requirement of a strong password policy for gaining system access.	
138	Logical Access Control	User Account Management	Does the system prompt the change of user passwords at predefined intervals?	User Passwords should be changed at periodic intervals and must be managed by system administrators.	
139	Logical Access Control	User Account Management	Do you enforce a password management policy for access to all platforms, applications, and databases?	Password policies, common for all platform, should be defined, approved and implemented.	

140	Logical Access Control	User Account Management	Do you have a policy regarding the storing and/or sharing of access credentials? If yes, please describe.	Access credentials, if stored / shared, can be misused and accountability cannot be established in case of any security breach.	
141	Logical Access Control	User Account Management	Do you prevent passwords from being displayed in clear text during user authentication or in electronic/printed reports?	User access credentials should not be explicitly displayed at the user work-stations as they could provide easier way to gain access for other personnel.	
142	Logical Access Control	User Account Management	Please indicate how long the initial/temporary password will last before it expires if not used.	Temporary passwords should be communicated securely and it should have defined life period after which it cannot be used. Also it should be allowed to use only one time .	
143	Logical Access Control	User Account Management	Do you have processes and controls for privileged access?	Privileged accesses should be granted after due authorization and it should be monitored and tracked.	
144	Logical Access Control	User Account Management	Do the users have unrestricted access to auxiliary devices like printers and scanners?	Access to auxiliary devices like printers, copiers etc. should be controlled with the help of passwords.	
145	Logical Access Control	User Account Management	Do you conduct a periodic access-level review that includes entitlements? If yes, please describe.	User access review should be performed periodically	
146	Logical Access Control	User Account Management	Do you have a segregated administration function to manage privileged accounts? If yes, please describe.	administration function to manage privileged accounts should be segregated and access should be with few identified individuals only	
147	Logical Access Control	User Account Management	Are there any instances in which employees would use a shared account? If yes, please explain.	Accountability could not be established, if shared user accounts are being used	

148	Logical Access Control	Logging Requirements	Are unsuccessful attempts to gain access to the work stations being logged and periodically analyzed by the system administrator?	Unsuccessful attempts to gain access to systems and applications should also be logged and analyzed for irregularities. Patterns in the logs can be used to detect and plug unauthorized attempts.	
149	Logical Access Control	Logging Requirements	Are the system administrator activities on firewall and other network elements being logged and monitored?	Logging should be defined for administrator activities on firewall and other critical network elements like routers. The changes should be traceable to a business requirement / change request.	
150	Logical Access Control	Logging Requirements	Are the timings between network devices synchronized for the logs to be useful?	There should be time synchronization between network elements for logs to be used for incident management.	
151	Logical Access Control	User Account Management	What is the process for dormant id deactivation? Are inactive accounts disabled and/or deleted for all systems (including, but not limited to, servers, routers, databases, switches, firewalls)? If yes, please describe.	Users id should be reviewed and monitored on periodically basis. Dormant id deactivation procedure should be defined and dormant id should be deleted from the system and documented.	

152	Logical Access Control	Logging Requirements	Do employees/contractors ever use their own PCs not managed by your company to store confidential data or connect to your network? Does the company allow BYOD?	1-Specify What Devices Are Permitted. 2-Establish a Stringent Security Policy for all Devices. 3-Define a Clear Service Policy for Devices Under BYOD Criteria. 4-Make It Clear Who Owns What Apps and Data 5-Decide What Apps Will Be Allowed or Banned. 6-Integrate Your BYOD Plan With Your Acceptable Use Policy. 7-Set Up an Employee Exit Strategy.	
153	Media Handling	Management of Removable Computer Media	Do you have a documented policy or program for use and management of removable media? If yes, please describe it.	Clear guidelines should be documented in form of policy for media handling and should be available to all concerns	
154	Media Handling	Management of Removable Computer Media	Is an authorization required for all media to be removed from the organization?	Appropriate authorization should be taken for all media to be removed from the organization	
155	Media Handling	Management of Removable Computer Media	Do you have documented requirements for securely storing removable media? If yes, please describe it.	Clear guidelines should be documented in form of policy for media handling and should be available to all concerns	
156	Media Handling	Management of Removable Computer Media	Do you have controls to safeguard and retrieve any physical SBIL's documents during storage? Please describe the controls.	SBIL document should be not be retrieved without prior approval from appropriate authority	

157	Media Handling	Management of Removable Computer Media	Do you retain a Third Party to deliver media to an off-site facility? If yes, please describe what kind of security controls are identified and implemented.	Security controls like, encryption of data, shock proof and fire proof media case should be used.	
158	Media Handling	Management of Removable Computer Media	Do you have documented procedures for the disposal, destruction, and/or re-use of physical media, removable media, and paper documents? If yes, please describe.	Clear guidelines should be documented in form of policy for media handling and should be available to all concerns	
159	Media Handling	Management of Removable Computer Media	Is the record of all authorized removals maintained?	Records for authorization should be maintained for all media to be removed from the organization	
160	Media Handling	Management of Removable Computer Media	Does vendor performs classification of information according to the SBI Life's classification scheme?	information classification must be in line with SBI information classification policy	
161	Media Handling	Management of Removable Computer Media	Does backup media tapes move to offsite location?	Offsite movement of backup tapes ensure availability of data in adverse situation	
162	Media Handling	Management of Removable Computer Media	Is the formal procedures established for media tape movement to offsite location	Adequate media tape movement procedure should be in place.	
163	Media Handling	Management of Removable Computer Media	Is the disposal of sensitive items logged to maintain an audit trail?	Appropriate media disposal procedures should be followed.	

164	Media Handling	Management of Removable Computer Media	Is SBIL data sent or received via physical media and How is physical media tracked?	Media handling officer should monitored or track the process of media while carrying the media during business hour. Physical media handling standard policy should be defined and documented.	
165	Media Handling	Management of Removable Computer Media	Is the movement of removable storage media / physical documents secured as agreed with the SBIL?	The standards policy and procedures should be defined and documented to restricted end users who have legitimate business requirements to connect portable removable media within internal networks.	
166	Media Handling	Management of Removable Computer Media	Are the servers processing SBIL data hardened as per policy?	All the servers processing SBIL data should be hardened and secure as per the SBIL policy.	
167	Network Security	Internet Access	Is the internet access to users controlled by a central gateway and routed through a proxy server?	Access should be routed through a proxy server so that the machines in the SBI Life user segment are anonymous and their IP's are not visible to external parties.	
168	Network Security	Internet Access	Is the internet access secure through a firewall?	Any access to or from the vendor network should be restricted through a firewall. The firewall should be adequately configured to prevent unauthorized access to the network.	

169	Network Security	Internet Access	Are your network devices configured to prevent communications from unapproved networks (e.g. the network devices deny all access by default, and only allow the minimum communication needed to support business and security objectives)?	The firewall should be adequately configured to prevent unauthorized access to the network.	
170	Network Security	Internet Access	Do you have a dedicated group or individual(s) to administer the firewall rules? If yes, please identify the individuals, and describe how you grant permissions to access the firewall.	There must be firewall administrator responsible for secure configurations and managing the changes made in the firewall.	
171	Network Security	Network Segregation	Do you use firewalls to define a logical network perimeter, security zones, and enclaves?	Network zone should be segregated using firewall to protect unauthorized access	
172	Network Security	Network Segregation	Do you have a process to certify and authorize firewall rules on a periodic basis? If yes, please describe your process.	All firewall rules should be implemented on the firewall only after the defined approval process	
173	Network Security	Remote Access	Are remote access (via Internet, Intranet, Extranet, etc.) connections to the network allowed? If yes, please describe the controls you use to secure network connectivity (e.g. firewall terminations, VPNs).	Remote access should be granted to only authorized and identified personal after due approval persons	

174	Network Security	Remote Access	Do you allow Third Parties to connect remotely to your environment? If yes, please describe your solution for Third Party remote access.	Vendor / third parties should only be granted remote access on need-to-know & need-to-have basis after due approval process	
175	Network Security	Remote Access	Does the remote access client prohibit split tunneling, thus preventing the device from accessing two separate networks simultaneously?	Split tunneling should not be allowed, it may lead to malware infection or data leakage issue.	
176	Network Security	Remote Access	Is multi-factor authentication required for remote network access?	passwords can be shared by remote users and it can be misused, to avoid that 2-factor authentication should be used.	
177	Network Security	Remote Access	Are all your remote access sessions recorded in an audit log? If yes, please describe.	To establish audit trail, all remote sessions should be recorded	
178	Network Security	Remote Access	Have you defined and configured remote access time limits and inactivity time limits? If yes, please describe.	Idle remote connection should be terminated after predefined inactivity time limit	
179	Network Security	Remote Access	Do you require your remote or non-console administrative access to systems (e.g. servers, network and wireless devices) go through an encrypted session?	Remote connection should be accessed through only encrypted channels to maintain the confidentiality and integrity of data.	



180	Network Security	Network Segregation	Do you have a current network diagram depicting the environment of services provided? Please indicate if your network diagram includes firewalls, routers, network servers, applications, critical databases, and workstations. Please provide a copy of your current network diagram.	High level & Low level network diagram should be readily available with concerned team, which can be used for trouble shooting.	
181	Network Security	Network Segregation	Do you have a data flow diagram that defines and documents all data interfaces (including remote and third parties) for secure data transmissions? Please provide a copy of your current data flow diagram.	High level & Low level data flow diagram should be readily available with concerned team, which can be used for trouble shooting.	
182	Network Security	Network Segregation	Are system components that store or process data (such as a database and application servers) in an internal network zone, segregated from the DMZ and other untrusted networks?	Access to internal network should be restricted using LAN segregation to avoid any unauthorized access / intrusion from outside to internal critical component / servers / database / application.	
183	Network Security	Wireless Security	Do you have a documented wireless communications and wireless networks policy or program that has been approved by management? If yes, please provide or describe.	Wireless policy should be well documented, approved and available with the concern for implementation.	

184	Network Security	Wireless Security	Are your wireless network segments segregated from the network using VLANs or other appropriate technologies?	Wireless network segments should be segregated to protect sensitive LAN zones (e.g. Production/UAT/Development)	
185	Network Security	Wireless Security	Which wireless protocols do you use at your organization, and how are they configured?	Secure protocols should be used to protect wireless device from getting compromise	
186	Network Security	Wireless Security	Do you ensure that only authorized users are allowed to access wireless devices? If yes, please describe how the users are monitored and tracked.	Authorized users list should be available with wireless admin and only these users should be able to access the wireless network.	
187	Network Security	Network Segregation	Is the network used for providing service to SBI Life, logically and physically segregated	The SBI Life environment at the service provider premises must be compartmentalized, separating it from the rest of the provider's environment to ensure no penetration is possible from other client environments or from the provider's wider network.	
188	Network Security	Secure Configuration and Patch Management	Is FTP / SFTP to users granted on a need only basis and is restricted?	The FTP facility should be provided based on business requirement and not be made available to all users.	
189	Network Security	Secure Configuration and Patch Management	Are the FTP sessions for communication with SBI Life encrypted?	The FTP sessions with SBI Life should be encrypted as the communication could be sniffed.	
190	Network Security	Secure Configuration and Patch Management	Is there a process for implementing security patches?	All network elements should be updated with the latest patches and application of patches should be established.	

191	Network Security	Authorized devices	Does your company have a policy or documented controls over devices that connect to the network, so that only authorized devices are allowed to connect to the network or to devices that connect to the network?	security controls like, port mapping, should be used to allow white listed / authorized devices to connect network	
192	Physical Security	Vendor Site Assessment	Is your information processing facility in a location that is externally obvious?	The vendor's information processing facility should not be in a externally obvious location with indications of SBI Life related operations explicitly displayed at their premises.	
193	Physical Security	Vendor Site Assessment	Whether SBI Life information processing facilities are in close proximity to potentially harmful installations?	Information Processing facilities near places where explosive materials are operated (e.g.; Kitchen) are subjected to associated risks.	
194	Physical Security	Physical Access to processing facilities	Is the access to your facility restricted to employees and authorized personnel only?	The access to the Vendor's facility should be made available to employees and authorized support personnel only.	
195	Physical Security	Physical Access to processing facilities	Is the access to the employees / vendors restricted by means of strong physical access control mechanisms?	Strong physical access controls (like Access IDs, Smart Cards) need to be deployed to ensure that the access is restricted to employees. Access cards mechanisms are prone to impersonation and might necessitate other controls like biometric access to ensure traceability and accountability.	

196	Physical Security	Physical Access to processing facilities	Is there a mechanism that informs the security personnel of the lost access cards (if available) or termination of access rights to personnel?	If access cards are used by personnel and visitors to gain access into the premises, there should be a mechanism to report lost access cards and a procedure to disable the access rights from the cards that were reported.	
197	Physical Security	Physical Access to processing facilities	Is the access to the Vendor's facility to employees / authorized personnel / visitors regulated by guards / receptionist?	Even if there is a deployment of an access card mechanism to gain access into the facility, there must be a security guard / receptionist to guide the visitors to the intended place. Third Party Personnel who may not be familiar to the location have to be provided guidance by them.	
198	Physical Security	Physical Access to processing facilities	Is an updated log maintained to track / monitor the movement of employees and authorized personnel?	There should be an updated log that captures the movement of authorized personnel into the Vendor site. The log may be physical or electronic, but must be present to ensure tracking. The movement of personnel visiting the Vendor's facility may also be monitored with the help of CCTV setup.	
199	Physical Security	Physical Access to processing facilities	Is a separate log maintained to track / monitor the visit of other personnel?	In addition to monitoring of employees and support personnel, a separate log is to be maintained to monitor the visit of other personnel to the site.	

200	Physical Security	Physical Access to processing facilities	Is the movement of assets tracked / monitored and reconciled?	Assets here refer to the replacement assets. For example, desktop PCs and Laptops that are being replaced / serviced at the Vendor's premises. Information like Laptop details, Personal Contact numbers, Persons to contact etc. have to be logged for references. Laptop Sr.no of visitors have to be reconciled on exit.	
201	Physical Security	Physical Access to processing facilities	Are the access logs being reviewed for any suspicious activities?	Logging and tracking are essential and these logs have to be analyzed by the SPOCs for any suspicious activities / deviations.	
202	Physical Security	Physical Access to processing facilities	Does all employees, contractors and third party users and all visitors wear some form of visible identification?	Visitor entry pass/ ID Card, Employee ID card, separate Entry pass/id cards for Vendor, contractors must be available and clearly distinguished	
203	Physical Security	Physical Access to processing facilities	Can personnel carry and use personal storage media devices into the facility?	Personal storage media devices like USB devices, Removable Hard-Disks etc. should be restricted within information processing facilities. They can be mis-handled to transfer SBI Life specific information from the Vendor site.	
204	Physical Security	Physical Access to processing facilities	Is delivery and loading areas controlled and isolated from information processing facilities to avoid unauthorized access?	Delivery and loading area must be separate and with appropriate access control mechanism in place	

205	Physical Security	Security at the vendor Site	Has enough precautions been taken and controls implemented to protect the premise and information assets from external and environmental threats like fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster?	Essential physical security controls for detecting and controlling a fire-outbreak. In addition to installation of the controls, it is essential they are tested regularly.	
206	Physical Security	Security at the vendor Site	Is the fire fighting system tested periodically?	Implemented Fire fighting system must be tested at least half yearly	
207	Physical Security	Security at the vendor Site	Is lightning protection applied to all buildings and lightning protection filters fitted to all incoming power and communications lines?	Lightning protection is required for safe grounding of current which prevents the damage of electric equipment	
208	Physical Security	Security at the vendor Site	Is there an UPS mechanism / Power Generator in place at the Vendor site?	Essential requirement for ensuring continuity in case of a power outage.	
209	Physical Security	Security at the vendor Site	Are there guidelines for movement of equipment within the Vendor's facility?	In case of a shared facility, there should be procedures for movement of user machines and server equipment that contained SBI Life related information. SBI Life specific data has to be removed from the storage repositories in case of movement.'	

210	System Security	Controls against Malicious Software	Is there a formal policy requiring compliance with software licenses and prohibiting the use of unauthorized or unsupported software, including freeware or shareware? If yes, what are the controls related to preventing their use?	There should be a guidance document on the usage of licensed software and the installation and usage of unauthorized software.	
211	System Security	Controls against Malicious Software	Is the appropriate anti-virus software employed and regularly updated?	An AV solution should be installed and regularly updated as control against malicious codes/software.	
212	System Security	Data Security	Do you have controls to prevent individuals from storing any confidential information or data on their desktop? If yes, please describe.	confidential data / information should not be allowed to store on local drives to maintain its availability, confidentiality and integrity. Data should be stored on central file server where security controls, like data backup, access controls are implemented.	
213	System Security	Server Security	Is there a configuration management document for servers and network? Does this document capture the all the secure settings and application specific settings?	Secure configuration document for servers and network element should be available, maintained and updated.	

214	System Security	Server Security	Are the audit and logging settings appropriately configured? Do suspicious activities like Failed logins, Start and stop of services, Modification of user privileges and Denial of Service attempts logged?	Logs on servers and critical equipment should be enabled and periodically monitored to record and identify security incidents.	
215	System Security	Desktop Configuration / Security	Do you prohibit end-users from having administrator access on their desktops? If yes, please describe the controls you use for this purpose.	Desktops should be hardened as per the secure configuration / hardening document. Unauthorized admin access can lead to data breach.	
216	System Security	Desktop Configuration / Security	Are all read/writeable devices controlled at the desktop (e.g. devices, CD burners, DVDs, zip drives, USB drives)? If yes, please describe.	Desktops should be hardened as per the secure configuration / hardening document. Only authorized personnel should have access to USB / CD / DVD drives	
217	System Security	Desktop Configuration / Security	Do you have controls to prevent users from altering security system configurations (e.g. screen saver settings, anti-virus settings)?	Secure configuration / hardening document should be available and implemented on all desktops	
218	System Security	Desktop Configuration / Security	Do you require users' approval before the help desk can take remote control of their desktops?	Without knowledge of end user, help desk or technical support staff should not allowed to take control of users machine.	



219	System Security	Desktop Configuration / Security	Do you use standard security configurations on operating systems, applications, laptops, desktops, and virtual machines? If yes, please provide details of your standard.	Secure configuration document for servers and network element should be available, maintained and updated.	
220	System Security	Desktop Configuration / Security	Do you have set and documented security baselines for all operating systems that are in line with industry practices or minimum security baselines?	Secure configuration document for servers and network element should be available, maintained and updated.	
221	System Security	Desktop Configuration / Security	Are share folders available with insecure permissions?	Access should be restricted to shared folders by specifying granular permissions to the specific users/groups.	
222	System Security	Desktop Configuration / Security	Is time zone setting correctly configured on the machine?	Correlation of logs and identification of the correct time frame for a malicious activity cannot be done if time zone setting is incorrect.	
223	System Security	Desktop Configuration / Security	Is security assessment( VA/PT/ Appsec) of application and systems used for accessing\processing of SBI Life data done?	An intruder can use a vulnerability for gaining unauthorized access to the SBI Life Data.	
224	System Security	Desktop Configuration / Security	Is the screen saver with Password protect option enabled and configured correctly?	An intruder can use an unattended console for gaining unauthorized access to the network / server segments.	

225	System Security	Desktop Configuration / Security	Are guest accounts disabled in the User machines?	Since Guest account is a default account, it is a common target for attackers to get unauthorized access to the user machines.	
226	System Security	Declining technology	Do you have a program that monitors technology products and versions that require third party support to ensure that the products continue to be supported? If yes, please provide documentation or describe.	Monitoring of software's / technology products for end of support by OEM or vendor	

Remarks



[illegible]






[illegible]
























[illegible]























