Appendix – A

Limited Technical Info for Troubleshooting (NO Prod Data)			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has processes in place to permanently erase SBI data from all environments (LIVE/ archived or data in external media), immediately after the need or clearly defined retention period as per the business engagement? Whether mechanism is in place to monitor the same?	Data Security	Self-certificate from the Third Party.

Lead Data Shared Acknowledgement Sent including CO-lending and NBFCs (where data originates from Third Party)			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
2	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Software Development and secured usage of Open-Source Tools.	Security Assessment	Regulator/ Gov approved or CERT empanelled auditors report on assessment of the security practices at third party environment (or) Evidence for implementation of the Control Objective

Data Shared for fetching (enquiry) – Sync API calls. No data Stored at Third Party			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
2	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Secure Software Development in terms of the Production Code but also	Security Assessment	Regulator/ Gov approved or CERT empanelled auditors report on assessment of the security practices at third party environment (or) Evidence for implementation of the Control Objective

	addressing vulnerabilities in the Open-Source Tools used in Software Development		

Software Procurement (IPR not with the Bank)			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Software Development and secured usage of Open-Source Tools.	Security Assessment	Regulator/ Gov approved or CERT empanelled auditors report on assessment of the security practices at third party environment (or) Evidence for implementation of the Control Objective
2	Assurance from independent third party on security stature of the procured products, indicating that product is free from vulnerabilities.	Application Security	**For Products with Integrations:** Regulator/ Gov approved or CERT empanelled auditors report on the Build deployed in SBI (covering various aspects of security Review like Application Security, Source Code Review, API Security, Authentication. mechanism, Log Review etc **For Stand Alone Products :** Relevant assurance as per the Approved Software Procurement Note

Development Offsite			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point
2	Whether resources deployed by third party for development, are properly skilled /trained in Secure Coding Practices, Secure Data management Practices?	Human Resource Security	ISO27001 certification or Undertaking with Evidence covering the control point

3	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
4	Whether a properly documented Change Management process has been instituted by the 3rd Party/ Vendor?	Change Management	ISO Certification or Change Management Procedures, Release Trackers
5	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e. SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e. 3rd party.
6	Whether the 3rd Party/Vendor/Vendor has (Board/Top Management approved) Information Security Policy and Procedures, in place with periodic reviews (minimum annually) by Top Management? The policy should cover below aspects of Information Security: 1. Human Resource Mgmt 2. Asset Management 3. Cryptographic Controls 4. Access Management 5. Log Management 6. Third Party Cyber Risk Mgmt 7. Network Security Mgmt 8. Application Security Mgmtt 9. End-point Security Mgmt 10. Incident Management 11. Physical Security 12. Change Management	Governance	ISO Certification or Content Table/ Page of IS Policy and review history page

Sensitive Technical Data Shared Offsite			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point

	sufficiency and effectiveness of physical controls is assessed by independent security auditors?		
2	Whether the 3rd Party/Vendor's Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc	Network Security	Evidence for implementation of the Control
3	Whether the third party has a dedicated Incident Management Mechanism to handle Cyber Incidents well within the timelines prescribed as per their internal guidelines?	Incident Management	ISO27001 certification or Evidence showing latest Policy Review and Approval
4	Whether third party has a mechanism in place to ensure that the employees of third party return the assets containing SBI/SBI Customer data after role change or completion/ termination of the project or company?	Human Resource Security	ISO27001 certification or Asset Mgmt Procedures Approved, Asset Issue Register
5	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
6	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e. SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e. 3rd party.
7	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
8	Whether third party has processes in place to permanently erase SBI data from all environments (LIVE/ archived or data in external	Data Security	Self-certification in case of Govt entity and Approved Purging Process & timeline and Evidence of actual implementation for non-Govt entities duly verified by CERT empanelled auditor.

	media), immediately after the need or clearly defined retention period as per the business engagement? Whether mechanism is in place to monitor the same?		
9	Whether Data at Rest encryption is ensured for both Live and archived data/ backup in external media etc? Are encryption keys stored in HSM?	Data Security	Evidence of encryption techniques implemented
10	Whether the application and database (containing SBI data) are hosted in Public Cloud? If yes, a. Is there a Secure Migration Process b. Is there a Secure Deletion Process c. Is Cloud Security Review performed on regular basis	Cloud Security	Cloud Controls reviewed by CERT-In auditors. Or ISO27018 and SOC 2 certification
11	Whether the 3rd Party/ Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?	Access Management	Role Conflict Matrix and evidence of following the same.
12	Whether third party permits remote access to internal systems/ applications? If yes whether they are secured by MDM and/or VPN through Hardened Mobile devices like Laptop/ Desktop or Mobiles	Access Management	Evidence for implementation of the Control

Production Support from Offsite Location			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point

2	Whether the 3rd Party/Vendor's Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc	Network Security	Evidence for controls in place
3	Whether the Third party periodically monitors/ reviews the firewall rules including that of Open Vulnerable Ports to ensure that only need based rules are in place.	Network Security	Approved Process of Firewall Rules and self-certification (signed by IS Head of the company) for non-presence of overly permissible such as Any-Any Rules or generic rules/evidence for latest FW
4	Whether the privilege access activities are logged IN PIM, (traceable to a specific user id with no default admin or generic id used), monitored, controlled and governed as per best security practices?	Log Management and Monitoring	Evidence of Privileged access logs and PIMS implementation
5	Whether the third party has a dedicated Incident Mgmt Mechanism to handle Cyber Incidents well within the timelines prescribed as per their internal guidelines?	Incident Management	ISO27001 certification or Evidence showing latest Policy Review and Approval
6	Whether resources deployed by third party for development, are properly skilled /trained in Secure Coding Practices, Secure Data management Practices?	Human Resource Security	ISO27001 certification or Undertaking with Evidence covering the control point
7	Whether third party has a mechanism in place to ensure that the employees of third party return the assets containing SBI/SBI Customer data after role change or completion/ termination of the project or company?	Human Resource Security	ISO27001 certification or Asset Management Procedures Approved, Asset Issue Register
8	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
9	Whether suitable Security certifications (ISO, PCI-DSS, SOC1 and SOC2 etc) of the	Governance	Certificate with validity period, if available.

	security posture at vendor environment are in place?		
10	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e. SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e. 3rd party.
11	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
12	Whether the 3rd Party/Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?	Access Management	Role Conflict Matrix and evidence of following the same.
13	Whether third party permits remote access to internal systems/ applications? If yes whether they are secured by MDM and/or VPN through Hardened Mobile devices like Laptop/ Desktop or Mobiles	Access Management	Evidence for implementation of the Control

Customer Data Shared for Processing / Storage Offsite			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Whether third party has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	Physical Security	ISO27001 certification or any other equivalent Audit Certificate covering the Control Point
2	Whether third party conducts security Assessment of all their applications (SBI related) covering activities (including not limited to) Appsec, API Testing, Source Code Review, DFRA, Process Review, Access	Security Assessment	Evidence of latest CERT In empanelled auditors report along with Scope

	Control, Vulnerability Assessment, Penetration Testing etc through regulator/ government (CERTempanelled or others) approved auditors. Any device hosted by Third party in SBI environment should also be covered		
3	Whether the 3rd Party/Vendor's Servers are suitably protected from external threats by way of security solutions like firewall, IDS/IPS, AV, DLP etc.?	Network Security	Evidence for controls in place
4	Whether the 3rd Party/Vendor's Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc	Network Security	Evidence for controls in place
5	Whether the 3rd Party/Vendor follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT	Network Security	CERT empanelled auditor's Report on verification of its implementation.
6	Whether the Third party periodically monitors/ reviews the firewall rules including that of Open Vulnerable Ports to ensure that only need based rules are in place.	Network Security	Approved Process of Firewall Rules and self-certification (signed by IS Head of the company) for non-presence of overly permissible such as Any-Any Rules or generic rules/evidence for latest FW
7	Whether internal servers are exposed to direct Internet access?	Network Security	Evidence of purpose/need of this and verification of controls in place by CERT empanelled auditors.
8	Whether the privilege access activities are logged, (traceable to a specific user id with no default admin or root id used), monitored, controlled and governed as per best security practices?	Log Management and Monitoring	Evidence of Privileged access logs and PIMS implementation
9	Whether Sufficient logs for Forensic Assessments are generated, stored securely and reviewed regularly through a SOC	Log Management and Monitoring	Log generation, storage and review process certified by CERT empanelled auditor.

10	Whether the third party has a dedicated Incident Mgmt Mechanism to handle Cyber Incidents well within the timelines prescribed as per their internal guidelines?	Incident Management	ISO27001 certification or Evidence showing latest Policy Review and Approval
11	Whether resources deployed by third party for development, are properly skilled /trained in Secure Coding Practices, Secure Data management Practises?	Human Resource Security	ISO27001 certification or Undertaking with Evidence covering the control point
12	Whether third party has a mechanism in place to ensure that the employees of third party return the assets containing SBI/SBI Customer data after role change or completion/ termination of the project or company?	Human Resource Security	ISO27001 certification or Asset Mgmt Procedures Approved, Asset Issue Register
13	Whether employee on-boarding process of third party covers background verification of the officials before allowing access to the systems/ data?	Human Resource Security	ISO27001 certification or Undertaking with evidence covering the control point.
14	Whether the 3rd Party/Vendor/Vendor has (Board/Top Management approved) Information Security Policy and Procedures, in place with periodic reviews (minimum annually) by Top Management? The policy should cover below aspects of Information Security: 1. Human Resource Management 2. Asset Management 3. Cryptographic Controls 4. Access Management 5. Log Management 6. Third Party Cyber Risk Management 7. Network Security Management 8. Application Security Management 9. End-point Security Management	Governance	ISO Certification or Content Table/ Page of IS Policy and review history page

	10. Incident Management 11. Physical Security 12. Change Management		
15	Whether suitable Security certifications (ISO, PCI-DSS, SOC1 and SOC2 etc) of the security posture at vendor environment are in place?	Governance	Certificate with validity period, if available.
16	Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security posture of the subsequent Party(ies) are reviewed to ensure that same are equivalent to those of the third Party (i.e. SBI vendor)?	Governance	SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e. 3rd party.
17	Whether the PII/ SPDI data is secured in transit by encryption with best-in-class encryption standards as per global best practises?	Data Security	Evidence of encryption techniques implemented
18	Whether the key management system of the third party ensures segregation and uniqueness of keys for SBI vis-à-vis other clients?	Data Security	Approved Process for Key Mgmt. and Evidence of actual implementation of Key Sharing
19	Whether SBI data, stored at 3rd party, is appropriately segregated from other clients at least through logical isolation at database level?	Data Security	Evidence of logical segregation
20	Whether third party has processes in place to permanently erase SBI data from all environments (LIVE/ archived or data in external media), immediately after the need or clearly defined retention period as per the business engagement? Whether mechanism is in place to monitor the same?	Data Security	Self-certification in case of Govt entity and Approved Purging Process & timeline and Evidence of actual implementation for non-Govt entities duly verified by CERT empanelled IS auditor.
21	Whether Data at Rest encryption is ensured for both Live and archived data/ backup in external media etc? Are encryption keys sored in HSM.	Data Security	Evidence of encryption techniques implemented

22	Whether the application and database (containing SBI data) are hosted in Public Cloud? If yes, a. Is there a Secure Migration Process b. Is there a Secure Deletion Process c. Is Cloud Security Review performed on regular basis	Cloud Security	Cloud Controls reviewed by CERT-In auditors. Or ISO27018 and SOC 2 certification
23	Whether a properly documented Change Management process has been instituted by the 3rd Party/ Vendor?	Change Management	ISO Certification or Change Management Procedures, Release Trackers
24	Whether the Vendor performs periodic DR Drills	Business Continuity	ISO27001 Certification or Evidence of conducting DR drills, and lessons learnt and their detailed recordings.
25	Whether third party has a Patch Management process for all systems is in place and the same is meticulously adhered to as per defined timelines?	Application Security	Evidence of latest patch applied, Patch Mgmt Procedures
26	Whether the 3rd Party/Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?	Access Management	Role Conflict Matrix and evidence of following the same.
27	Whether third party permits remote access to internal systems/ applications? If yes whether they are secured by MDM and/or VPN through Hardened Mobile devices like Laptop/ Desktop or Mobiles	Access Management	Evidence for implementation of the Control
28	Whether the Third Party has a Secure Software Development Lifecycle Environment that includes both Software Development and secured usage of Open-Source Tools.	Security Assessment	Regulator/ Gov approved or CERT empanelled auditors report on assessment of the security practices at third party environment

Data Shared with Govt./ Statutory/ Regulatory Bodies through any Mode (SFG/API etc)			
Sno	**Control**	**Domain**	**Evidence Requirement**
1	Security of the Data stored and processed at Govt / Regulator end.	Data Security	Self Certificate from competent authority of the Govt / Regulator Entity.

Appendix – C

Description for Nature of Services	
Term	**Description**
Limited Technical Data for Troubleshooting	Limited Technical / Non-Technical data (Exclusive of Customer Information or Internal Sensitive Information), shared with OEM for technical troubleshooting purpose.
Lead Data Shared Acknowledgement Sent including CO-lending and NBFCs	Data is originated at third-party and received at SBI for further action or internal consumption. However, acknowledgement / confirmation is sent to third party without any SBI identifiable data/ information.
Data Shared for fetching (enquiry) - Sync API calls. No data Stored at Third Party	Data is shared for fetching some info about existing SBI customer to third-party like CIBIL. Sync API calls where there is no offline processing or Storage of data sent (except for any reference number for such communication)
Software Procurement (IPR/ source code not with the Bank)	Software procured directly where IPR for Source code is not with Bank
Development Offsite	Where Software development is done offsite, and Source Code is shared with Bank for review at our end.
Sensitive Technical Data Shared Offsite	Technical Data that identifies SBI internal technical information such as IP address etc., is shared at the third party's environment that is outside SBI controlled environment.
Production Support from Offsite Location	Any support services requiring access to Production Servers from offsite location i.e. third party's environment which is outside the SBI controlled environment. This includes handling of Customer/ Production data as well.
Customer Data Shared for Processing / Storage Offsite	Customer Data means any data that Singly or jointly identifies SBI Customer. Sharing means any Such data shared by Bank for Storing or Processing (exclusive of Sync API Call Processing), at the third party's environment that is outside SBI controlled environment.
Data Shared Onsite	When any data is shared to Onsite third-party resources either for Development, Production Support or otherwise.
Services without any data sharing	Any Services obtained from Third Party without data sharing. (e.g. Software or Hardware Procurement)
Data Received from Merchants/ Third Parties/ through any Mode (SFG/API etc)	Data received from Third Parties (by any mode like API, SFG etc)

APPENDIX – E

CONTROL POINTS FOR CONTINUOUS MONITORING BY IT AOs

(at least half-yearly)

1. Status of observations for Vulnerability Assessment scanning and Penetration Testing for assets and resources controlled by at vendor (deployed on-premises or offsite).
2. Status of security patch implementation for assets and resources controlled by at vendor (deployed on-premises or offsite)
3. Changes implemented during the relevant period by vendor in the IT environment under their control. The change reports should also be accompanied by security assessment report from a regulator approved independent security auditor.
4. Reporting of incidents impacting the IT systems (deployed on-premises or offsite) controlled by the vendor, for the relevant period.

NOTE:

Any other control points that the IT AO may consider relevant in view of criticality of data and/ or service, may also be included as part of continuous monitoring process.