ANNEXURE I

#	Points to be covered	
1	• Vulnerability Assessment and Penetration Testing (VAPT) • Network, Router and related interface • Conduct security review of PCs/terminals • Mobile Banking Application (Android / iOS) • Internet Banking • Website	• Broad Areas of Audit • Network Architecture review • Firewall rule base review • Antivirus rule base review • Security Equipment Configurations & Policies
2	• IT Policies review • Cyber Security Policy • IS / IT Policy • The Technology Vision Document 2020-23 • Vendor / Outsourcing Risk Management • Change Management policy • Data Leak Prevention Strategy policy • Cyber Crisis Management Plan (CCMP) • Incident Response and Management policy	• Payment Gateway Audit • Verification of controls for RTGS, NEFT, and SFMS etc. • Privacy and Data Protection • Procedures of erasing, shredding of documents an • Media containing sensitive information after the period of usage. • Gap Assessment Audit of ATMs • Access for Cyber Security Compliance Portal

	Services
1	VAPT Audit – 2 Times in year
2	IS Audit – 1 Time in year
3	24 visits in a year (For timely implementation of RBI, CERT-IN and NPIIC alerts and advisories) and day to day cyber security advice.
4	GAP Assessment Audit and SAR Audit as per RBI Guideline – CERTIN Audit Including **(subject to Cert-in panel on boarding)**
5	Reserve bank of India and other authority compliance support, Support for CERT-IN advisory and alerts CERT-IN Auditor certificate issue as when required for compliance purpose
6	Unlimited support as when required