ASP Audit checklist

Sr. No.	Audit Parameters	
1.	The communication between ASP and ESP should be Digitally Signed and encrypted	
2	Communication line between ASP and ESP should be secured. It is strongly recommended to have leased lines or similar secure private lines between ASP and ESP. If a public network is used, a secure channel such as SSL should be deployed	
3	ASP should have a documented Information Security policy in line with security standards such as ISO 27001	
4	Compliance review of controls as per Information security policy	
5	ASPs should follow standards such as ISO 27001 to maintain Information Security	
6	Compliance to prevailing laws such as IT Act 2000 should be ensured	
7	Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional network security controls and end point authentication schemes may be put in place.	
8	Resident consent process must be implemented to obtain consent for every transaction carried out. The user must be asked for willingness to sign it and consent form should be stored	
9	Application Security Assessment of the ASP by Cert-in empanelled auditor /IS Auditor	
10	ASP data logging for audit purposes provisioned.	
11	ASP should not delegate any obligation to external organizations or applications.	
12	ASP integrate with ESPs through standard eSign APIs only	
13	Provision for providing/accessing the copy of the signed document to the signer	
14	ASP shall display (and allow download/print) the document that is to be signed clearly for subscribers to read before signing	
15	ASP shall protect the document URL (available within eSign request) from anyone or any system accessing it using URL and also from virus, malware, etc.	
16	Indemnify both ESP and CA for integrity related discrepancies arises at ASP end	