Scope of Work for System Integrator & OEM

S.no	Description	Compliance	Remark
1	Conduct an assessment of our existing infrastructure, applications, and systems to determine compatibility and integration requirements for the SSO & IDAM solution		
2	Understand the existing authentication mechanisms and protocols in use		
3	Understand the user existing experience and authentication flows.		
4	Prepare & document a detailed implementation plan that includes pre-requisite for SSO & IDAM, timelines, milestones, and resource requirements.		
5	Design & document the overall architecture(HLD & LLD) of the SSO & IDAM solution. Certification signoff from OEM on finalised HLD and LLD.		
6	Ensure deployment and configuration of the SSO & IDAM solution in SBIL UAT, production & DR environment		
7	Ensure to implement required features of SSO & IDAM solution as mentioned in SSO technical specification documentation.		
8	Implement industry-standard On-premise SSO & IDAM setup with High Availability for seamless integration with our existing applications infrastructure.		
9	Prepare plan based on application priority, timeline, milestone and execute the deployment of the SSO & IDAM solution for SBIL on-prem with API to connect with cloud-based applications.		
10	Integrate SSO & IDAM solutions with Active Directory, LDAP, embedded LDAP & other directory services as a single directory service, to synchronize user information and enable centralized management of user identities to allow users to authenticate once and access multiple applications seamlessly.		
11	Integration of required SSO protocols into intended applications by guiding & hand holding with application developer/teams & vendors, also help to application team for appropriate application code change, re-development etc		
12	Ensure to implement SSO integration with atleast one applications from each application platform working at SBI Life (e.g. platform like weblogic, .net, java, jboss, product based etc.)		
13	Ensure design and implementation of SSO & IDAM solution with High Availability at DC and DR		
14	Conduct comprehensive testing to validate the functionality, performance, and security of the implemented solution		
15	Verify security compliance for an SSO & IDAM solution and mitigate vulnerabilities, security points closure within defined TAT		
16	Validate the user experience and troubleshoot any issues.		

17	Implement logging and monitoring mechanisms to track user access activities, detect suspicious behaviour, and generate audit reports. Ensure compliance with relevant regulations and standards		
18	Implement access review processes and tools to periodically review and certify user access rights		
19	Implement monitoring & reporting & alert mechanisms to track on user access activities, security incidents, and compliance violations. This includes generating audit reports, analysing access logs, and implementing real-time alerts for suspicious activities.		
20	Provide detailed documentation covering the architecture, configuration, and maintenance of the SSO & IDAM solution		
21	Provide Knowledge base documentation, user guides, technical documentation, and SOP to educate users and administrators about SSO & IDAM solution.		
22	Conduct training sessions for our IT staff to ensure they understand the new SSO & IDAM system and its features. Walk through the deliverables.		