

The Ultimate SaaS SLA Checklist

Migrating to the cloud is a big decision, and not just any provider will do. After all, **not all clouds are created equal**, and the differences aren't always easy to see. To help dig a little deeper, we've compiled a checklist of what to look for when evaluating SaaS offerings and their respective service level agreements. Insurity provides complete transparency in its SLAs, furnishing every client with full details during discussions of migration. So whether you're evaluating software as a service in general, or ready to choose a provider, check out our top 10 list of critical SLAs to explore.

✓ Availability

The SaaS provider should include a system availability commitment that clearly states the percentage of time the application (which supports your business-critical workflows) will be available. This measurement of availability should also incorporate critical access to third-party services made available from the SaaS provider's platform. The percentage of system uptime and number of scheduled maintenance windows should be included. The SaaS provider should also be able to provide its historical availability performance to support their commitment.

✓ Security

The SaaS provider must be able to provide its documented security policies, along with evidence that these policies are being followed.

✓ Compliance and Audit

The SaaS provider should clearly state how and when its infosec controls are audited and make the audit results available to clients. A standard such as SOC and or NIST should be used for the basis of the audit which is conducted by a reputable third party on an annual basis.

✓ Performance

The SaaS provider must clearly state its system response time objective (RTO) and should have a monitoring solution that can objectively measure performance commitments outlined in their availability SLA.

✓ Privacy

The SaaS provider should clearly state how client data is secured, including encryption algorithms, and how each client's data is isolated from other clients and third parties.

✓ Business Continuity

The SaaS provider must outline its disaster recovery plan, explicitly stating the geographic locations of their primary and secondary hosting environments, and the associated recovery time objective (RTO) and recovery point objective (RPO) commitments, ensuring adequate protection in case of a disaster. The disaster recovery model should be included as part of the SaaS provider's standard offering.

✓ Client Support

The SaaS provider should outline its client support model and clearly outline how it will be able to support the client's specific business and technical needs.

✓ Data Residency

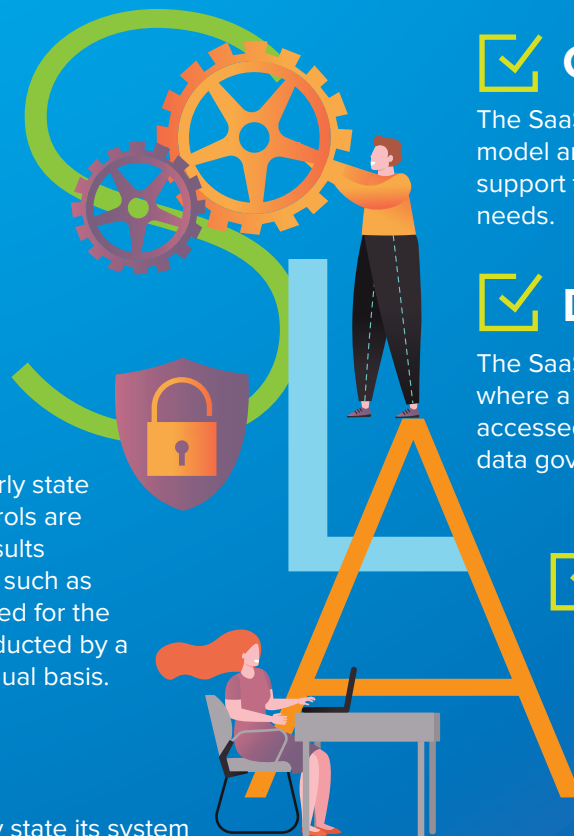
The SaaS provider must be able to clearly identify where a client's data is stored and how it is accessed, and demonstrate that the applicable data governance requirements are met.

✓ Maintenance

The SaaS provider should clearly outline the types of maintenance tasks it performs (service-impacting and non-service-impacting), the frequency and duration of these activities, and the associated annual maintenance window schedule.

✓ Geographic Presence

The SaaS provider must ensure that its cloud operations and client support organizations are available to support the client's business needs in all relevant geographies.



Insurity is a leading provider of cloud-based core system solutions and data analytics for the world's largest insurers, brokers, and MGAs. Through its best-in-class digital platform and with unrivaled industry experience and thought leadership, Insurity is uniquely positioned to deliver exceptional value, empowering clients to focus on their core businesses, optimize their operations, and provide superior customer experiences. With users worldwide and more cloud-based deployments than any other core system provider in the insurtech space, Insurity is trusted by 15 of the top 25 property/casualty carriers in the US.