SME for using SaaS

SLA - Ready
Making Cloud SLAs readily usable in the EU private sector

ConsultLess is a small consultancy firm in the EU that has 20 employees (mostly legal and management experts). One of the employees is partner and also the Chief Information Officer (CIO) of the firm. ConsultLess decides to procure office software as a service (SaaS) for use by its employees: the cloud service offers document storage/editing, email and calendar. This cloud service should replace an internal mail-server and office software installed on computers.

User Type: SME

User Maturity: Novice, Basic

Cloud Service lifecycle phase: Acquisition

Cloud usage: App on Cloud, Processing Sensitive Data, Data Integrity

High priority practices

Roles and Responsibilities

Roles and responsibilities should be specified in the cloud Service Level Agreement (SLA), and aligned to the definitions in standards like ISO/IEC 17788 and ISOIEC 17789.

Cloud SLA definitions

Term and definitions should be specified in the cloud SLA, and aligned to EU guidelines and international standards.

SLA change notifications

The information provided by the Cloud Service Provider (CSP), specialized support, and notification period should be sufficient enough in order to give Cloud Service Customer (CSC) the chance to evaluate the severity of the planned SLA changes. The CSP should allow renegotiation of the SLA, and it should be feasible for the CSC to initiate termination of the SLA.

Unilateral change

Have any clause on unilateral change deleted or been declared not applicable, and arranged that any changes of the services itself that are beneficial and non-detrimental for the CSC need to be discussed and agreed upon with the CSC in advance.

Feasibility of specials & customizations

Always assess, prepare and negotiate. The default cloud SLAs initially made available by providers may be less hard-coded, fixed and non-negotiable as customers may think, and the CSPs may wish to make them believe. This is especially applicable now, as the cloud services market is still maturing.

General Carve-outs

Read the small print as good as any other part of the applicable documentation, try to identify where the risks are and what kind of impact such incidents may have on your business, discuss these with your CSP, and negotiate our those that the CSC finds unreasonable and unacceptable for its intended use and possible impact.

Specified SLO metrics

For all Service Level Objectives (SLOs) contained in the SLA, the CSP should provide a metric specification based on a well-known standard e.g., ISO/IEC 19086-2, or NIST SP 500-307.

Data Management SLOs

The SLA may specify related SLOs contained in additional documents like the European Commission's "SLA Standardisation Guidelines". In particular, the CSP is expected to clearly define the used data classification scheme, data deletion mechanism, data portability format, and relevant links to the personal data protection SLOs (e.g., in relationship to the data deletion SLOs). Metrics definitions associated to these SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Security SLOs

This good practice improves the accountability level of the CSP. Beyond a list of applicable security certifications, as part of the SLA the Cloud Service Provider is expected to present a set of quantitative/qualitative SLOs in areas like:

- Organisation of Information Security;
- Human Resources Security;
- Asset Management;
- Access Control;
- Cryptography;
- Physical and Environmental Security;
- Operations Security;
- Communications Security;
- Systems Acquisition;
- Development and Maintenance;
- Supplier Relationships;
- Information Security Incident Management;
- Business Continuity Management;
- Compliance.

It is important to note that in this case the structure/classification of the specified security SLOs should be consistent with that used in the security certifications the provider refers to. For example security SLOs in ISO/IEC 19086-4, along with their corresponding implementation guidance, are structured according to ISO/IEC 27002 and 27017.

Specified security SLOs/Service Quality Objectives (SQOs) should make reference to the verifiable evidence associated to the corresponding and agreed metrics. The security SLOs, and more in general the cloud SLA, should be specified in compliance with ISO/IEC 19086-1, ISO/IEC 19086-2, and ISO/IEC 19086-3. This will provide the CSC with details related to topics like SLO/SQO monitoring, applicable remedies, metrics specification, and core requirements.

Furthermore, for highly important security SLOs it is a good practice for customers to obtain from the CSP the information/tools required for monitoring the agreed security commitments continuously.

Particular attention should be paid to the "Information Security Incident Management" component, where it is expected for the Cloud Service Provider to notify consumers of the occurrence of any breach of its system, regardless of the parties or data directly impacted.

Metrics play an important role in critical CRM security components. Metrics and standards for measuring performance and effectiveness of information security management should be established prior to agreeing on the cloud SLA. As a minimum, customers should understand and document their current metrics and how they will change when operations are moved into the cloud and where a provider may use different metrics. Agreed metrics should be compliant with a relevant standard like ISO/IEC 19086-2.

Personal Data Protection SLOs

The SLA may specify related SLOs contained in additional documents like the EC's "SLA Standardisation Guidelines". Metrics definitions associated to these SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Medium priority practices

- Revision date
- Update frequency
- SLA duration
- Contact details
- Contact availability
- Service Credit
- Service credits assignment
- Maximum service credits (Euro amount) provided by the CSP
- Cloud Service Performance SLOs
- Service Reliability SLOs

Low priority practices

- SLA URL
- Findable
- Choice of law
- Previous versions and revisions
- SLA language
- Machine-readable format
- Nr. of pages
- Service Levels reporting
- Service Levels continuous reporting
- General SLOs

Click and download your tailored tips on Cloud Service Level Agreements

SLA Ready has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644077