SME migrating from one SaaS CSP to the other

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

The SME is already using certain Software as a Service (SaaS). At the time of procuring it, it was not felt to be that mission critical for the SME's business. Upon the plans made to shift from the existing SaaS Cloud Service Provider (CSP) to a new SaaS CSP the cloud services used and to be used, the SME founds out that the use of this SaaS has become quite mission critical for the survival and success of the SME.

User Type: SME

User Maturity: Experienced

Cloud Service lifecycle phase: Termination, Consequences of Termination

Cloud usage: App on a Cloud, Processing Sensitive Data, Data Integrity, High Availability

High priority practices

Findable

The SLA should be easy to find directly at the CSP's home page.

Choice of law

Getting to agreement with applicable law where the Cloud Service Customer (CSC) has its offices or where is active with its end-user.

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.

Revision date

The revision date, along with a log of changes, should be included in the SLA.

Previous versions and revisions

Besides providing public access to its SLA repository, the CSP is expected to diligently provide integrity/authenticity protection to the stored SLAs, along with a summary of the relevant changes in each version/revision.

SLA duration

Besides specifying the SLA validity period, the CSP is expected to clearly communicate the conditions under which the SLA may be changed (please refer to "high importance" good practices in 18 - SLA Change Notifications and 19 Unilateral Change below), or become invalid before its expiration.

Contact details

The CSP should provide the contact information for SLA-related questions. Furthermore, it is expected that the CSP provide more than one communication channel e.g. email, telephone, live-chat, etc.

Contact availability

Contact availability for SLA-related questions should be continuously provided by the CSP, therefore covering the complete SLA life cycle.

SLA change notifications

The information provided by the CSP, specialized support, and notification period should be sufficient enough in order to give 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.

General SLOs

Metrics definitions associated to the General SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Data Management SLOs

The SLA may specify related Service Level Objectives (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 CSP 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 CSP 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 CSCs 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 CSP 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, CSCs should understand and document their current metrics and how they will change when operations are moved into the cloud and where a CSP may use different metrics. Agreed metrics should be compliant with a relevant standard like ISO/IEC 19086-2.

Personal Data Protection SLOs

The CSP needs to make clear in a documented way that it complies to the applicable laws. Furthermore, 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

- SLA URL
- Cloud SLA definitions
- Update Frequency
- SLA language
- General Carve-outs

Low priority practices

- Machine-readable format
- Nr. of pages
- Service Credit
- Service credits assignment
- Maximum service credits (Euro amount) provided by the CSP
- Service Levels reporting
- Service Levels continuous reporting
- Feasibility of specials & customizations
- Specified SLO metrics
- Cloud Service Performance SLOs
- Service Reliability 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