SME using IaaS/PaaS

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

EasyAgriSelling is a small tech start-up in the EU, which developed an online web shop software (as a service) for farmers who would like to start direct-selling their vegetables and other products. Their slogan is: "Selling your agricultural produce to consumers, made easy". Farmers can set up an online shop in a few clicks - customizing their shop with a logo, colours and a description of their farm. EasyAgriSelling operates a pay-as-you-go model, charging no monthly fee, but only charging their customers when products are sold. EasyAgriSelling is a SaaS provider and they are a cloud services customer building services on a cloud provider who offers them IaaS and PaaS on which to build their product. The SaaS platform runs on top of the IaaS/PaaS platform.

User Type: SME

User Maturity: Experienced

Cloud Service lifecycle phase: Acquisition, Operation

Cloud usage: App on a Cloud, High Availability

High priority practices

SLA URL

The Service Level Agreement (SLA) should be publicly available at the Cloud Service Provider's (CSP) home page, with an easy to remember URL e.g., https://www.csp_name.com/SLA.

Findable

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

Roles and responsibilities

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

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.

Service credits management

Discussing and agreeing on continuous monitoring as well as pro-active incident management notification, with incurred damages being paid out in financial funds.

SLA change notifications

The information provided by the 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.

Service Levels reporting

The CSP should provide the CSC with the tools, training and support to directly measure the achieved Service Levels, and evaluate them with respect to the agreed Service Level Objectives (SLOs). Measured Service Levels should be integrity- and authenticity-protected, so the CSC can use them to demonstrate potential violation of the SLA by the CSP.

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.

Cloud Service Performance SLOs

The CSC should be able to request changes to the capacity SLO limits for the consumed service(s). Furthermore, the SLA may specify related SLOs contained in additional documents like the European Commission's "SLA Standardisation Guidelines". Metrics definitions associated to the General SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Service Reliability SLOs

All reliability information should be found on the SLA. The CSP may also refer to reliability SLOs in the Data Management section of the SLA. Furthermore, the SLA may specify related SLOs contained in additional documents like the EC's "SLA Standardisation Guidelines". The reliability SLOs specified by the CSP should assist the CSC in putting in place Recovery Point Objective and Recovery Time Objective when using the cloud service. 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/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

- Choice of law
- SLA duration
- SLA language
- Service Credit
- Maximum service credits (Euro amount) provided by the CSP
- Unilateral change
- Service Levels continuous reporting
- General Carve-outs
- Specified SLO metrics
- General SLOs

Low priority practices

- Cloud SLA definitions
- Revision date
- Update Frequency
- Previous versions and revisions
- Machine-readable format
- Nr. of pages
- Data Management 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