Fintech Early Stage Seeking IaaS

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

There are lot of start-ups and SMEs that are active in the Fintech industry (where the financial services meet new technologies and business models) with an operational and business plan to develop and exploit cloud-based services to their customers and end-users. For this, most will consider procuring either IaaS or PaaS from respective Cloud Service Provider (CSPs) that offer these cloud services, which will be used as basis to develop, rely, and exploit their own Platform as a Service (PaaS) respectively Software as a Service (SaaS). This Use Case focusses on a Fintech company procuring Infrastructure as a Service (IaaS) from major IaaS CSP.

User Type: SME

User Maturity: Novice

Cloud Service lifecycle phase: Acquisition

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

High priority practices

Findable

The Service Level Agreement (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 SLA, and aligned to the definitions in standards like ISO/IEC 17788 and ISOIEC 17789.

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.

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.

Service Levels continuous reporting

The CSP should provide a certified form of continuous monitoring-based Service Level reporting. An example of such certification scheme is Cloud Security Alliance (CSA) Open Certification Framework – Level 3 (OCF – STAR Continuous).

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.

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.

Data Management SLOs

The SLA may specify related SLOs contained in additional documents like the EC'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

» Cloud SLA definitions

» SLA language

» Feasibility of specials & customizations

Low priority practices

» SLA URL

» Revision date

» Update Frequency

» Previous versions and revisions

» Machine-readable format

» Nr. of pages

» Service Credit

» Service credits management

» Maximum service credits (Euro amount) provided by the CSP

» Specified SLO metrics

» 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