SME video storage and streaming from the Cloud

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

A financial investment company is launching new investment products to its agents and affiliates. A number of videos have been created to teach the company's agents and affiliates about the benefits and features of the new products. The videos are very large and need to be available on-demand, so storing them in the cloud lessens the demands on the corporate infrastructure. However, access to those videos needs to be tightly controlled. For competitive reasons, only certified company agents should be able to view the videos. An even stronger constraint is that regulations require the company to keep product details, including the videos, confidential during the quiet period before the launch of the product. The company's decision is to use a public cloud storage provider to scale the secure hosting and streaming of the videos. The cloud solution must control the videos with an auditable access control mechanism that enforces the company's security policies.

User Type: SME

User Maturity: Novice, Basic

Cloud Service lifecycle phase: Acquisition, Operation

Cloud usage: App on a Cloud, High Availability

High priority practices

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.

Contact availability

Contact availability for SLA-related questions should be continuously provided by the Cloud Service Provider (CSP), therefore covering the complete Service Level Agreement (SLA) life cycle.

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.

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.

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.

Medium priority practices

- SLA URL
- Findable
- SLA language
- Contact details
- Service Credit
- Service credits assignment
- Maximum service credits (Euro amount) provided by the CSP
- SLA change notifications
- Unilateral change
- Service Levels reporting
- Service Levels continuous reporting
- General Carve-outs
- General SLOs
- Data Management SLOs
- Personal Data Protection SLOs

Low priority practices

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

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