Distribution of SME Training Material to Mobile Employees

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

A SME must deploy the technical processes and considerations to distribute educational material for new products to their agents. Given the potential network traffic to be generated by this process, it is necessary to rely on Cloud services.

User Type: SME

User Maturity: Basic, Experienced

Cloud Service lifecycle phase: Operation

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

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.

Contact availability

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

Service Levels reporting

The CSP should provide the Cloud Service Customer (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.

Cloud Service Performance SLOs

The customer 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 Cloud Service Provider 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 provider should assist the customer 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 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/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.

Medium priority practices

- SLA URL
- Findable
- Choice of law
- 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 continuous reporting
- Feasibility of specials & customizations
- General Carve-outs
- Specified SLO metrics
- 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