Cloud-based Development and Testing

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

An online retailer needs to develop a new Web 2.0 storefront application, but does not want to burden its IT staff and existing resources. The company chooses a cloud provider to deliver a cloud-based development environment with hosted developer tooling and a source code repository. Another cloud provider is chosen to provide a testing environment so that the new application can interact with many different types of machines and huge workloads.

User Type: SME

User Maturity: Experienced

Cloud Service lifecycle phase: Acquisition, Operation

Cloud usage: App on a Cloud, Data Integrity, Cloud Bursting, 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.

Service Credit

Discussing and agreeing on reasonable terms of remedies, including without limitation the right to claim full damages, except to the extent non-insurable by the Cloud Service Provider (CSP), next to improvement commitment for zero-repeat.

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.

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 Cloud Service Customer (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 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.

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.

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/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

- Revision date
- Update frequency
- SLA duration
- Contact details
- Contact availability
- Service Credit
- Service credits assignment
- Maximum service credits (Euro amount) provided by the CSP
- Cloud Service Performance SLOs
- Service Reliability SLOs

Low priority practices

- SLA URL
- Findable
- Choice of law
- Previous versions and revisions
- SLA language
- Machine-readable format
- Nr. of pages
- Service Levels reporting
- Service Levels continuous reporting
- 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