Cloud Brokering: Cloud Chargeback and Showback

A Cloud Service Customer (CSC) uses the services of a Cloud Broker to select the Cloud Service Provider (CSP) that fulfils its specific requirements. The Broker implements a service catalogue encompassing services from multiple CSPs. In addition, the catalogue clearly outlines charges for the various resources that can be provisioned. The CSC makes a selection and the Cloud Broker seamlessly provisions the requested resource from the appropriate CSP through their API or other interface using their native commands. At the same time, the Broker handles the chargeback to the CSC's organization, if appropriate.

User Type: SME

User Maturity: Novice

Cloud Service lifecycle phase: Acquisition

Cloud usage: App on a Cloud

High priority practices

SLA URL

The Service Level Agreement (SLA) should be publicly available at the CSP's 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 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 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.

Maximum service credits (Euro amount) provided by the CSP

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 CSP, next to improvement commitment for zero-repeat.

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.

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 CSA Open Certification Framework – Level 3 (OCF – STAR Continuous).

General SLOs

Metrics definitions associated to the General Service Level Objectives (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.

Medium priority practices

- Choice of law
- SLA duration
- SLA language
- SLA change notifications
- Unilateral change
- Feasibility of specials & customizations
- General Carve-outs
- Specified SLO metrics
- Cloud Service Performance SLOs
- Service Reliability SLOs
- Data Management SLOs
- Personal Data Protection SLOs

Low priority practices

- Cloud SLA definitions
- Revision date
- Update Frequency
- Previous versions and revisions
- 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