Small Public Administration using Governmental Cloud

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

In 2013, the Government of Estonia took the first steps to deploy a Governmental Cloud with three main principles guiding its development:

» Using Cloud solutions located within Estonia's national borders,

» Using international private Cloud resources, and

» Using Data Embassies (cloud storage).

The Estonian government has built the foundation of a highly developed information society, and its ICT development has taken Estonia to a stage where many registers and services only exist in digital form. This development requires a flexible and secure Governmental Cloud solution. Sufficient flexibility has to be planned in advance. The State Infocommunication Foundation leads the Governmental Cloud development, which is responsible for the consolidation of server resources and provision of high-quality server hosting services within Estonia's national borders. The Estonian Public Administration (PA) is the main cloud customer of the national Governmental Cloud. In some cases, PAs are provisioned with IaaS resources (e.g. virtual machines), but also PAs provision Governmental cloud-based services to citizens. The Governmental Cloud system does not store personal identifiable data.

User Type: Government

User Maturity: Experienced

Cloud Service lifecycle phase: Operation

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

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.

Cloud SLA definitions

Term and definitions should be specified in the cloud SLA, and aligned to EU guidelines and international standards.

Contact details

The Cloud Service Provider (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.

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.

Cloud Service Performance SLOs

The Cloud Service Customer (CSC) should be able to request changes to the capacity Service Level Objective (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

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.

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

- SLA duration
- Service Credit
- Service credits assignment
- SLA change notifications
- Unilateral change
- Service Levels reporting
- Service Levels continuous reporting
- Feasibility of specials & customizations
- General Carve-outs
- Specified SLO metrics

Low priority practices

- SLA URL
- Findable
- Choice of law
- Revision date
- Update Frequency
- Previous versions and revisions
- SLA language
- Machine-readable format
- Nr. of pages
- Maximum service credits (Euro amount) provided by the CSP

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