

The case is simple, and will happen to all CSCs: an SME wished to terminate the MSA with a CSP, and then starts thinking about whether and to what extent the CSP will delete its data, after the SME has extracted and exported that data as much as possible. This SME, as will others, finds out that nothing is arranged for, and is left in the dark.

## High priority practices

### Choice of Law

Getting to agreement with applicable law where the 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 ISO/IEC 17789.

### Data Management SLOs

The SLA may specify related SLOs contained in additional documents like the EC's "SLA Standardisation Guidelines". In particular, the Cloud Service Provider 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 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.

**User Type:** SME

**User Maturity:**

Novice, Basic,  
Experienced

**Cloud Service  
lifecycle phase:**

Acquisition, Operation

**Cloud usage:**

Processing Sensitive  
Data, Data Integrity

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 SLA-Ready Common Reference Model 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.

## Personal Data Protection SLOs

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 URL
- » Findable
- » Cloud SLA definitions
- » SLA change notifications
- » Unilateral change
- » Feasibility of specials & customizations
- » General Carveouts
- » Specified SLO metrics
- » General SLOs

[Click and download your tailored tips on Cloud Service Level Agreements](#)



## Low priority practices

- » Revision date
- » Update Frequency
- » Previous versions and revisions
- » SLA duration
- » SLA language
- » Machine-readable format
- » Nr. of pages
- » Contact details
- » Contact availability
- » Service Credit
- » Service credits assignment
- » Maximum service credits (Euro amount) provided by the CSP
- » Service Levels reporting
- » Service Levels continuous reporting
- » Cloud Service Performance SLOs
- » Service Reliability SLOs