
**Information technology — Cloud
computing — Service level agreement
(SLA) framework —**

**Part 3:
Core conformance requirements**

*Technologies de l'information — Informatique en nuage — Cadre de
travail de l'accord du niveau de service —*

Partie 3: Exigences de conformité essentielles



IECNORM.COM : Click to view the full PDF of ISO/IEC 19086-3:2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	1
5 Conformance	2
6 Relationship between the cloud service agreement and cloud SLAs	2
7 Cloud SLA Management	2
8 Role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA	2
9 Cloud SLA components	3
9.1 General	3
9.2 Covered services component	3
9.3 Cloud SLA definitions component	3
9.4 Service monitoring component	3
9.4.1 General	3
9.4.2 Monitoring parameters	3
9.4.3 Monitoring mechanisms	3
9.5 Roles and responsibilities component	3
10 Cloud SLA content areas and their components	4
10.1 General	4
10.2 Accessibility content area	4
10.2.1 Accessibility component	4
10.2.2 Accessibility standards	4
10.2.3 Accessibility policies	4
10.3 Availability content area	4
10.3.1 Availability component	4
10.3.2 Availability	4
10.4 Cloud service performance content area	4
10.4.1 General	4
10.4.2 Cloud service response time component	4
10.4.3 Cloud service capacity component	5
10.4.4 Elasticity component	5
10.5 Protection of personally identifiable information (PII) content area	6
10.6 Information security content area	6
10.7 Termination of service content area	6
10.7.1 Termination of service component	6
10.7.2 Data retention period	6
10.7.3 Log retention period	6
10.7.4 Notification of service termination	6
10.7.5 Return of assets	6
10.8 Cloud service support content area	7
10.8.1 Cloud service support component	7
10.8.2 Support hours	7
10.8.3 Service incident support hours	7
10.8.4 Service incident notification time	7
10.8.5 Maximum first response time	7
10.8.6 Maximum incident resolution time	7
10.8.7 Support plans	7
10.8.8 Support methods	7
10.8.9 Support contacts	7

10.8.10	Service incident reporting	7
10.8.11	Service incident notification	8
10.9	Governance content area	8
10.9.1	Governance component	8
10.9.2	Regulation adherence	8
10.9.3	Standards adherence	8
10.9.4	Policy adherence	8
10.9.5	Audit schedule	8
10.10	Changes to the cloud service features and functionality content area	8
10.10.1	Changes to the cloud service features and functionality component	8
10.10.2	Minimum service change notification period	8
10.10.3	Minimum time before feature/function deprecation	9
10.10.4	Service change notification method	9
10.11	Service reliability content area	9
10.11.1	General	9
10.11.2	Service resilience/fault tolerance component	9
10.11.3	Customer data backup and restore component	10
10.11.4	Disaster recovery component	11
10.12	Data management content area	11
10.12.1	Intellectual property rights (IPR) component	11
10.12.2	Cloud service customer data component	11
10.12.3	Cloud service provider data component	11
10.12.4	Account data component	12
10.12.5	Derived data component	12
10.12.6	Data portability component	12
10.12.7	Data deletion component	12
10.12.8	Data location component	13
10.12.9	Data examination component	13
10.12.10	Law enforcement access component	14
10.13	Attestations, certifications and audits content area	14
10.13.1	General	14
10.13.2	Cloud service attestations	14
10.13.3	Cloud service certifications	14
10.13.4	Cloud service audits	14
	Bibliography	15

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

A list of all the parts in the ISO 19086 series can be found on the ISO website.

IECNORM.COM : Click to view the full PDF of ISO/IEC 19086-3:2017

Information technology — Cloud computing — Service level agreement (SLA) framework —

Part 3: Core conformance requirements

1 Scope

This document specifies the core conformance requirements for service level agreements (SLAs) for cloud services based on ISO/IEC 19086-1 and guidance on the core conformance requirements. This document is for the benefit of and use by both cloud service providers and cloud service customers.

This document does not provide a standard structure that would be used for cloud SLAs.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 19086-1, *Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 and ISO/IEC 19086-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

4 Abbreviated terms

CSC	cloud service customer
CSP	cloud service provider
CSA	cloud service agreement
ICT	information and communications technology
IPR	intellectual property rights
PII	personally identifiable information
RTO	recovery time objective

RPO	recovery point objective
SLA	service level agreement
SLO	cloud service level objective
SQO	cloud service qualitative objective

5 Conformance

A cloud SLA that conforms to this document shall implement at least the following components, as described in ISO/IEC 19086-1:

- covered services;
- cloud SLA definitions.

ISO/IEC 19086-1 includes one or more cloud service level objectives (SLOs) or cloud service qualitative objectives (SQOs) for each cloud SLA component ([Clause 9](#)) or content area ([Clause 10](#)). When using a component from [Clause 9](#) or a content area from [Clause 10](#), a conforming cloud SLA is not required to use the SLOs or SQOs described in those components or content areas. A conforming cloud SLA is recommended to use SLOs and SQOs from ISO/IEC 19086-1, when appropriate. Regardless of whether an SLO or SQO is used, a CSP shall not redefine any term in such a way that it contradicts the terms and definitions in ISO/IEC 19086-1 or this document.

ISO/IEC 19086-2 defines a model for specifying metrics for cloud service level agreements (SLAs). Conforming cloud SLAs are encouraged to use the model in ISO/IEC 19086-2 when specifying metrics for SLOs and SQOs.

A conforming cloud SLA may use a subset of the components ([Clause 9](#)) or content areas ([Clause 10](#)) described in this document or it may include components or content areas outside the scope of this document. However, a conforming cloud SLA shall adhere to the definition of the terms, components or content areas, as stated in ISO/IEC 19086-1 and the requirements as stated in this document. Conformance for a specific component or content area means that the SLA shall adhere to all the requirements for that component or content area. Conformance to this document does not require implementation of any specific technology.

6 Relationship between the cloud service agreement and cloud SLAs

The relationship between the cloud service agreement and cloud SLAs is covered in ISO/IEC 19086-1. There are no conformance requirements for the relationship between the CSA and cloud SLAs.

7 Cloud SLA Management

Cloud SLA management is covered in ISO/IEC 19086-1. There are no conformance requirements for cloud SLA management.

8 Role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA

The role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA is covered in ISO/IEC 19086-1. There are no conformance requirements for role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA.

9 Cloud SLA components

9.1 General

The cloud SLA components in this clause and the cloud SLA content areas in [Clause 10](#) define the requirements of the SLOs or SQOs that may be used within a cloud SLA.

9.2 Covered services component

The covered services component shall identify the cloud service(s) that are covered by the cloud SLA.

A given cloud SLA may cover more than one cloud service and each cloud service may have its own components, content areas, SLOs and SQOs.

9.3 Cloud SLA definitions component

The cloud SLA definitions component shall define terms that are unique to the SLA or that are particularly important to the understanding of the cloud SLA.

Cloud SLAs should use definitions from industry standards, when possible.

A conforming cloud SLA shall not redefine a term defined by ISO/IEC 19086-1, ISO/IEC 19086-3 or ISO/IEC 19086-4 in a manner that contradicts the original meaning.

9.4 Service monitoring component

9.4.1 General

A service monitoring component shall specify the monitoring mechanisms that are available to the cloud service customer.

The service monitoring component shall specify one or more SQOs for cloud service monitoring (see ISO/IEC 19086-1 for SQOs).

For each of the service monitoring SQOs chosen, the SQO shall conform to the requirements listed below for the SQO.

9.4.2 Monitoring parameters

A monitoring parameters SQO shall provide a list of the parameters for the covered services that the CSP monitors and for which it provides data to the CSC.

9.4.3 Monitoring mechanisms

A monitoring mechanisms SQO shall provide a list of monitoring mechanisms available to the CSC, which shall include a description of the monitored parameters and a description of any related terms and conditions.

9.5 Roles and responsibilities component

Roles and responsibilities component is covered in ISO/IEC 19086-1. There are no conformance requirements.

10 Cloud SLA content areas and their components

10.1 General

The cloud SLA content areas clauses define requirements for the SLOs or SQOs that may be used within a cloud SLA.

10.2 Accessibility content area

10.2.1 Accessibility component

An accessibility component shall specify one or more SQOs for accessibility (see ISO/IEC 19086-1 for SQOs).

For each of the accessibility component SQOs chosen, the SQO shall conform to the requirements listed below for the SQO.

10.2.2 Accessibility standards

An accessibility standards SQO shall provide a statement listing any accessibility related standards the CSP supports in the covered services.

10.2.3 Accessibility policies

An accessibility policies SQO shall provide a statement listing the policies and regulations for accessible ICT the CSP supports in the covered services.

10.3 Availability content area

10.3.1 Availability component

An availability component shall specify one or more SLOs for availability (see ISO/IEC 19086-1 for SLOs).

For each of the availability component SLOs chosen, the SLO shall conform to the requirements listed below for the SLO.

10.3.2 Availability

An availability SLO shall provide the amount or percentage of time in a given period that the cloud service is accessible and usable.

10.4 Cloud service performance content area

10.4.1 General

The cloud SLA may include components that can be used to express the performance of a cloud service.

For each of the cloud service performance content area related component SLOs chosen, the SLO shall conform to the requirements listed below for the SLO.

10.4.2 Cloud service response time component

10.4.2.1 General

A cloud service response time component shall specify one or more SLOs for cloud service response time (see ISO/IEC 19086-1 for SLOs).

For each of the cloud service response time component SLOs chosen, the SLO shall conform to the requirements listed below for the SLO.

10.4.2.2 Cloud service maximum response time observation

A cloud service maximum response time observation SLO shall specify a maximum time between a defined stimulus or input to the cloud service and a defined point in the response (see ISO/IEC 19086-2 for metrics).

10.4.2.3 Cloud service response time mean

A cloud service response time mean SLO shall specify the statistical mean over a set of cloud service response time observations (see ISO/IEC 19086-2 for a metric model).

10.4.2.4 Cloud service response time variance

A cloud service response time variance SLO shall describe how far from the mean response times are likely to be within a set of cloud service response time observations.

10.4.3 Cloud service capacity component

10.4.3.1 General

A cloud service capacity component shall specify one or more SLOs for cloud service capacity (see ISO/IEC 19086-1 for SLOs).

The cloud service capacity component shall specify the metric(s) used to state capacities, where appropriate (see ISO/IEC 19086-2 for metrics).

For each of the cloud service capacity component SLOs chosen, the SLO shall conform to the requirements listed below for the SLO.

10.4.3.2 Limit of simultaneous cloud service connections

A limit of simultaneous cloud service connections SLO shall specify the maximum number of simultaneous connections supported by the cloud service.

10.4.3.3 Limit of available cloud service resources

A limit of available cloud service resources SLO shall specify the maximum capacity of available resources.

10.4.3.4 Cloud service throughput

A cloud service throughput SLO shall specify the number of inputs or the amount of sets of inter-dependent inputs that can be processed in every unit of time by the cloud service.

10.4.3.5 Cloud service bandwidth

A cloud service bandwidth SLO shall specify the maximum amount of data that can be transferred over a period of time.

10.4.4 Elasticity component

10.4.4.1 General

An elasticity component shall specify one or more SLOs for elasticity (see ISO/IEC 19086-1 for SLOs).

The elasticity component shall specify the metric(s) used to state elasticities where appropriate (see ISO/IEC 19086-2 for metrics).

For each of the elasticity SLOs chosen, the SLO shall conform to the requirements listed below for the SLO.

10.4.4.2 Elasticity speed

An elasticity speed SLO shall describe how fast a cloud service is able to react to a resource request when the CSC makes a resource re-allocation request or when workload changes take place.

10.4.4.3 Elasticity precision

An elasticity precision SLO shall describe how precise the resource allocation meets the actual resource requirements at a given point in time.

10.5 Protection of personally identifiable information (PII) content area

A protection of PII component shall specify one or more SLOs or SQOs for protection of PII.

For details, refer to ISO/IEC 19086-4 for SLOs and SQOs relating to the protection of PII component.

10.6 Information security content area

An information security component shall specify one or more SLOs or SQOs for protection of PII.

For details, refer to ISO/IEC 19086-4 for SLOs and SQOs relating to the information security component.

10.7 Termination of service content area

10.7.1 Termination of service component

A termination of service component shall specify one or more SLOs or SQOs for termination of service (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the termination of service SLOs or SQOs chosen, the SLO or SQO shall conform to the requirements listed below for the SLO or SQO.

10.7.2 Data retention period

A data retention period SLO shall specify the period of time that the cloud service customer data is retained after a notification of service termination has been issued.

10.7.3 Log retention period

A log retention period SLO shall specify the period of time that cloud service customer related log files are retained after a notification of service termination has been issued.

10.7.4 Notification of service termination

A notification of service termination SQO shall document the process for notifying a CSC that their cloud service agreement is being terminated including the notification period.

10.7.5 Return of assets

A return of assets SQO shall document the responsibilities of the CSP and the CSC in relation to the ownership, use, return and disposal of data objects and the disposal of physical artefacts containing data objects as part of the service termination.

10.8 Cloud service support content area

10.8.1 Cloud service support component

A cloud service support component shall specify one or more SLOs or SQOs for cloud service support (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the cloud service support SLOs or SQOs chosen, the SLO or SQO shall conform to the requirements listed below for the SLO or SQO.

10.8.2 Support hours

A support hours SLO shall specify the hours of operation for each support plan.

10.8.3 Service incident support hours

A support incident support hours SLO shall specify the hours during which CSCs may obtain support specifically for service incidents.

10.8.4 Service incident notification time

A service incident notification time SLO shall include the time interval in which the CSP shall provide a notification of a service incident to specified contacts at the CSC when provided for in the support plan.

10.8.5 Maximum first response time

A maximum first response time SLO shall specify the maximum time between a customer reporting an incident and the cloud service provider's initial response to the report.

10.8.6 Maximum incident resolution time

A maximum incident resolution time SLO shall specify the maximum time for resolving an incident.

10.8.7 Support plans

A support plans SQO shall list the support plans available to the CSCs, including any support costs.

The following SQOs may be included under support plans in the cloud SLA. For each of SQOs chosen, the SQOs under support plans shall conform to the requirements listed below.

10.8.8 Support methods

A support methods SQO shall document the methods the CSC can use to obtain support.

10.8.9 Support contacts

A support contacts SQO shall document the specific contacts for service support if available under the support plan.

10.8.10 Service incident reporting

A service incident reporting SQO shall document the options which the CSC may use to report service incidents to the CSP.

10.8.11 Service incident notification

A service incident notification SQO shall document the terms and conditions (severity, timeframe, etc.) under which the CSP shall disclose the details of a service outage or condition that affects the operation of the service. The terms may also define what constitutes a service incident.

Service incident notification should include:

- the cause of the incident;
- the steps the CSP is taking to resolve the incident;
- the time at which the CSP expects to have the incident resolved;
- any workarounds the CSP may employ while the incident is being resolved.

10.9 Governance content area

10.9.1 Governance component

A governance component shall specify one or more SQOs for governance (see ISO/IEC 19086-1 for SQOs).

For each of the governance SQOs chosen, the SQO shall conform to the requirements listed below for the SQO.

10.9.2 Regulation adherence

A regulation adherence SQO shall document regulations including name, clause, and certification number (if applicable) the CSP attests or has been certified to comply with.

10.9.3 Standards adherence

A standards adherence SQO shall document the standards including name, clause, and certification number (if applicable) the CSP attests or has been certified to comply with.

10.9.4 Policy adherence

A policy adherence SQO shall document the business or governance policies specific to the service that are being adhered to on an ongoing basis.

10.9.5 Audit schedule

An audit schedule SQO shall document the schedule of audits the CSP undertakes using its own or third party resources.

10.10 Changes to the cloud service features and functionality content area

10.10.1 Changes to the cloud service features and functionality component

A change to the cloud service features and functionality content area shall specify one or more SLOs or SQOs for changes to the cloud service features and functionality (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the changes to the cloud service features and functionality SLOs or SQOs chosen, the SLOs or SQOs shall conform to the requirements listed below for the SLO or SQO.

10.10.2 Minimum service change notification period

A minimum service change notification period SLO shall specify the minimum period of time between the issuance of a service change notification and the implementation of the change.

10.10.3 Minimum time before feature/function deprecation

A minimum time before feature/function deprecation SLO shall specify the minimum period between the initial availability of a feature or function and deprecation of that feature or function.

10.10.4 Service change notification method

A service change notification method SQO shall describe the method(s) by which the CSP will notify CSCs of changes to the features and functionality of covered service(s).

10.11 Service reliability content area

10.11.1 General

A service reliability content area shall specify one or more SLOs or SQOs for service reliability (see ISO/IEC 19086-1 for SLOs and SQOs).

10.11.2 Service resilience/fault tolerance component

10.11.2.1 General

The service resilience/fault tolerance component shall specify one or more SLOs or SQOs for service resilience/fault tolerance (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the service resilience/fault tolerance SLOs or SQOs chosen, the SLO or SQOs shall conform to the requirements listed below for the SLO or SQO.

10.11.2.2 Time to service recovery

A time to service recovery SLO shall specify the time elapsed between a cloud service failing and the service returning back to the normal state of operation.

10.11.2.3 Mean time to service recovery

A mean time to service recovery SLO shall specify the average of a series of Time to Service Restoration calculations.

10.11.2.4 Maximum time to service recovery

A maximum time to service recovery SLO shall specify the largest value of a set of Time to Service Restoration calculations over a defined period of time.

10.11.2.5 Number of service failures

A number of service failures SLO shall specify the number of service failures in total or over a period of time.

10.11.2.6 Cloud service resiliency/fault tolerance methods

A cloud service resiliency/fault tolerance methods SQO shall describe the methods employed by the CSP which afford resilience and fault tolerance for the covered service(s) and a statement of the methods available to the CSC to afford resilience/fault tolerance for their workloads.

10.11.3 Customer data backup and restore component

10.11.3.1 General

The customer data backup and restore component shall specify one or more SLOs or SQOs for customer data backup and restore (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the customer data backup and restore SLOs or SQOs chosen, the SLO or SQO shall conform to the requirements listed below for the SLO or SQO.

10.11.3.2 Backup interval

A backup interval SLO shall specify the period of time between data backups or the number of data backups made in a defined period of time.

10.11.3.3 Retention period for backup data

A retention period for backup data SLO shall specify the time period the CSP retains data backups.

10.11.3.4 Number of backup generations

A number of backup generations SLO shall specify the number of backup generations of cloud service customer data retained by the CSP.

10.11.3.5 Backup restoration testing

A backup restoration testing SLO shall specify the number of restoration tests from backups over a specified time period.

10.11.3.6 Backup method

A backup method SQO shall list the cloud service customer data backup methods available to the CSC or employed by the CSP.

10.11.3.7 Backup verification

A backup verification SQO shall list the methods or technologies used to verify the integrity of data backups.

10.11.3.8 Backup restoration test reporting

A backup restoration test reporting SQO shall list the content and availability of reports on backup restoration testing.

10.11.3.9 Alternative methods for data recovery

Alternative methods for data recovery SQO shall list the methods the CSP can undertake to restore cloud service customer data in the event the primary data restoration method is not successful.

10.11.3.10 Data backup storage location

A data backup storage location SQO shall list the geographical location(s) where the data backups are stored.

10.11.4 Disaster recovery component

10.11.4.1 General

A disaster recovery component shall specify one or more SLOs or SQOs for disaster recovery (see ISO/IEC 19086-1 for SLOs or SQOs).

For each of the disaster recovery SLOs or SQOs chosen, the SLO or SQO shall conform to the requirements listed below for the SLO or SQO.

10.11.4.2 Recovery time objective (RTO)

A recovery time objective SLO shall specify the maximum time period required to bring the cloud service back from an outage to a correct operational state.

10.11.4.3 Recovery point objective (RPO)

A recovery point objective SLO shall specify the maximum time period prior to a failure or disaster during which changes to data may be lost as a consequence of recovery.

10.11.4.4 Cloud service provider disaster recovery plan

A cloud service provider disaster recovery plan SQO shall list the procedures adopted by the cloud service provider for restoring the cloud service, as well as the responsibilities for the recovery of CSC resources that have been built on top of the cloud service. These responsibilities will vary depending on the cloud capability type.

10.12 Data management content area

10.12.1 Intellectual property rights (IPR) component

An IPR SQO shall include a statement of any IPRs the CSP claims on the cloud service customer data.

An IPR SQO shall include a statement of any IPR the CSP grants to the CSC on the cloud service provider's data and/or cloud service derived data.

10.12.2 Cloud service customer data component

10.12.2.1 Cloud service customer data

A cloud service customer data SQO shall define the cloud service customer data.

NOTE ISO/IEC 19944 describes a data taxonomy that can be used to define cloud service customer data.

10.12.2.2 Cloud service customer data usage

A cloud service customer data usage SQO shall document all uses of cloud service customer data by the cloud service provider.

NOTE ISO/IEC 19944 defines a data use statement structure that can be used to describe cloud service customer data usage.

10.12.3 Cloud service provider data component

A provider data SQO shall define cloud service provider data.

NOTE ISO/IEC 19944 describes a data taxonomy that can be used to define cloud service provider data.