DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19086-1

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2016-01-04

Voting terminates on:
2016-04-04

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

Part 1:
Overview and concepts

Titre manque

ICS: 35.020

Reference number
ISO/IEC DIS 19086-1:2015(E)

COPYRIGHT PROTECTED DOCUMENT

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 Symbols and abbreviated terms 4

5 Overview of SLAs for cloud services 5

6 Relationship between the cloud service agreement and SLAs 6

7 Cloud SLA management best practices 7
7.1 General 7
7.2 Design 7
7.3 Evaluation and acceptance 7
7.4 Implementation and execution 8
7.5 Changes to the cloud SLA 8

8 The role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the SLA 8
8.1 General 8
8.2 Metrics 8
8.3 Service levels 9
8.3.1 Cloud service level objectives 9
8.3.2 Cloud service qualitative objectives 9
8.4 Remedies 10
8.4.1 Claims process 10
8.5 Exceptions 10

9 Cloud SLA components 10
9.1 General 10
9.2 Covered services component 10
9.2.1 Description 10
9.2.2 Relevance 11
9.3 Cloud SLA definitions component 11
9.3.1 Description 11
9.3.2 Relevance 11
9.4 Service monitoring component 11
9.4.1 Description 11
9.4.2 Relevance 11
9.4.3 Cloud service qualitative objectives 11
9.5 Roles and responsibilities component 11
9.5.1 Description 11
9.5.2 Relevance 12

10 Cloud SLA content areas 12
10.1 General 12
10.2 Accessibility content area 12
10.2.1 Accessibility component 12
10.3 Availability content area 13
10.3.1 Availability component 13
10.4 Cloud service performance content area 13
10.4.1 General 13
10.4.2 Cloud service response time component 13

10.4.3 Cloud service capacity component....14
10.4.4 Elasticity component....15
10.5 Protection of personally identifiable information (PII) content area....16
10.5.1 Protection of PII component....16
10.6 Information Security content area....17
10.6.1 Information Security component....17
10.7 Termination of service content area....18
10.7.1 Termination of service component....18
10.8 Cloud service support content area....20
10.8.1 Cloud service support component....20
10.9 Governance content area....22
10.9.1 Governance component....22
10.10 Changes to the cloud service features and functionality content area....23
10.10.1 Changes to the cloud service features and functionality component....23
10.11 Service reliability content area....24
10.11.1 General....24
10.11.2 Service resilience/fault tolerance component....24
10.11.3 Customer data backup and restore component....24
10.11.4 Disaster recovery component....26
10.12 Data management content area....27
10.12.1 General....27
10.12.2 Intellectual property rights (IPR) component....27
10.12.3 Cloud service customer data component....28
10.12.4 Cloud service provider data componen....28
10.12.5 Account data component....29
10.12.6 Derived Data component....29
10.12.7 Data portability component....30
10.12.8 Data deletion component....30
10.12.9 Data location component....31
10.12.10 Data examination component....31
10.12.11 Law enforcement access component....32
10.13 Attestations, certifications and audits content area....32
10.13.1 Attestations, certifications and audits component....32

Bibliography....34

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 19086-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud Computing and Distributed Platforms*.

ISO/IEC 19086 consists of the following parts, under the general title *Information technology — Cloud computing — Service Level Agreement (SLA) framework*:

— *Part 1: Overview and concepts*

— *Part 2: Metrics*

— *Part 3: Core requirements*

— *Part 4: Security & Privacy*

Information technology — Cloud computing – Service Level Agreement (SLA) framework — Part 1: Overview and concepts

1 Scope

This International Standard specifies an overview of Service Level Agreements (SLA)s for cloud services, identification of the relationship between the cloud service agreement and the SLA, concepts that can be used to build cloud SLAs, and terms commonly used in SLAs for cloud services. This standard is for the benefit and use of both cloud service provider and cloud service customer.

This International Standard does not provide a standard structure that can be used for a cloud SLA or a standard set of cloud service level objectives (SLOs) and cloud service qualitative objectives (SQOs) that will apply to all cloud services or all cloud service providers. Contracts vary between cloud service providers, and in some cases different cloud service customers can negotiate different contract terms with the same cloud service provider for the same cloud service, so this standard seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can then be used to create cloud SLAs that help avoid confusion and facilitates a common understanding between cloud service providers and cloud service customers.

This International Standard does not supersede any legal requirement.

2 Normative references

The following referenced documents are indispensable for the application 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.

Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

Recommendation ITU-T Y.3502 | ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in Rec. ITU-T Y.3500 | ISO/IEC 17788 and the following definitions apply.

3.1
accessibility
usability of a product, service, environment or facility by people within the widest range of capabilities

Note 1 to entry: The concept of accessibility addresses the full range of user capabilities and is not limited to users who are formally recognized as having disability.

Note 2 to entry: The usability-oriented concept of accessibility aims to achieve levels of effectiveness, efficiency and satisfaction that are as high as possible considering the specified context of use, while paying attention to the full range of capabilities within the user population.

Note 3 to entry: It is important in the context of ISO/IEC 19086 to distinguish between the specialized meaning of “accessibility” as defined here and the term “accessible” which is used with its dictionary meaning of “able to be reached or entered”.

[SOURCE: ISO 9241-171:2008, 3.2]

3.2
cloud service agreement
documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)

Note 1 to entry: A cloud service agreement can consist of one or more parts recorded in one or more documents

3.3
failure notification policy
policy specifying the processes by which the cloud service customer and cloud service partner can notify the cloud service provider of a service outage and by which the cloud service provider can notify the cloud service customer and cloud service partner that a service outage has occurred.

Note 1 to entry: The policy may also include the process for providing updates on service outages, who receives notifications and updates, the maximum time between the detection of a service outage and the issuance of a notice of service outage, the maximum time interval between service outage updates and how service outage updates are described

3.4
remedy
compensation available to the cloud service customer in the event the cloud service provider fails to meet a specified cloud service level objective.

3.5
resilience
ability of a cloud service to recover operational condition quickly after a fault occurs

3.6
cloud service level objective
SLO
commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval or ratio scale

Note 1 to entry: an SLO commitment may be expressed as a range

3.7
cloud service qualitative objective
SQO
commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal or ordinal scale

Note 1 to entry: a cloud service qualitative objective may be expressed as an enumerated list

Note 2 to entry: qualitative characteristics typically require human interpretation

Note 3 to entry: The ordinal scale allows for existence/nonexistence

3.8
metric
a standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement.

Note 1 to entry: A metric implements a particular abstract metric concept.

Note 2 to entry: A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific goal.

3.9
disaster recovery
ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disaster

[SOURCE: ISO/IEC 27031:2011, 3.7]

3.10
personally identifiable information (PII)
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.11
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100, 2.12]

3.12
service level agreement (SLA)
part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered service(s)

3.13
business continuity
capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

[SOURCE: ISO/IEC 22301:2012(en), 3.3]

3.14
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.15
PII principal
natural person to whom the personally identifiable information (PII) relates

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.16
nominal scale
scale with unordered labelled categories or ordered by convention

[SOURCE: ISO 3534-2:2006(en), 1.1.6]

3.17
ordinal scale
scale with ordered labelled categories

[SOURCE: ISO 3534-2:2006(en), 1.1.7]

3.18
interval scale
continuous scale or discrete scale with equal sized scale values and an arbitrary zero

[SOURCE: ISO 3534-2:2006(en), 1.1.8]

3.19
ratio scale
continuous scale with equal sized scale values and an absolute or natural zero point

[SOURCE: ISO 3534-2:2006(en), 1.1.9]

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviations apply:

AUP	Acceptable Use Policy
BLOB	Binary Large Object
CSA	Cloud Service Agreement
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IPR	Intellectual Property Rights
IT	Information Technology
KPI	Key Performance Indicator
MBRT	Maximum Batch Response Time
MTTSR	Maximum Time to Service Recovery
PaaS	Platform as a Service
PII	Personally Identifiable Information

RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SCRUD	search, create, read, update and delete
SLA	Service Level Agreement
SLO	Cloud Service Level Objective
SQO	Cloud Service Qualitative Objective
TTSR	Time to Service Recovery
VM	Virtual Machine
WCAG	W3C Web Content Accessibility Guidelines

5 Overview of SLAs for cloud services

A service level agreement (SLA) is a part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered service(s). The cloud SLA should account for the key characteristics of cloud computing as described in Clause 6.2 of Rec. ITU-T Y.3500 | ISO/IEC 17788 that include:

— **Self-service** – A CSC may gain access to cloud services without human interaction with the CSP. The cloud service agreement (CSA) (see Clause 6) and the associated cloud SLA may be presented and agreed through software tools and financial arrangements that are automated.

— **Resource pooling** – The public cloud deployment models allow sharing resources across many CSCs that do not have a relationship. The private cloud models allow users to share resources within the same organization. The hybrid cloud models allow users to share some resources within the same organization and some resources across many CSCs that do not necessarily have a relationship. The community cloud deployment models allow sharing resources across CSCs that have some relationship.

— **Multi-tenancy** – Cloud environments are enabled through the use of large-scale virtualization of servers, storage and networks. Overall system usage is typically spread over many CSCs. Cloud environments typically have no persistent relationship between particular physical resources and their use by CSCs. The CSCs are assigned virtual resources, and logging of usage is done at this level of abstraction.

— **Rapid elasticity and scaling** – A characteristic of cloud computing where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources.

— **Tradeoff between cost and control** – Large-scale, standardized cloud services may be provided on a low unit cost, utility basis, in conjunction with standardized contracts and cloud SLAs. If a CSC requires more control and customization of cloud services than is available from a standard utility service model, then this may be provided at additional cost and with a specific cloud SLA.

— **Measured service** - A feature where the metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered cloud service. The focus of this key characteristic is that the CSC may only pay for the resources that they use.

— **Broad network access** – The capabilities of cloud services are made available over the network and are typically accessed through standard mechanisms that promote use by heterogeneous client platforms (for example, access through mobile phones, laptops and workstations).

Details of cloud SLAs, SLOs and SQOs can vary for different cloud service categories, cloud capabilities types and different cloud deployment models (see Rec ITU-T Y.3500 | ISO/IEC 17788). Cloud SLAs in this standard are intended to be useful for CSCs and CSPs across the variety of cloud service categories and cloud deployment models. As the definition of cloud SLOs and SQOs is intended to be technology and business model neutral, so not all of these SLOs or SQOs will apply to every cloud service, and those that do apply may be structured and applied in different ways to specific cloud services. For example, service availability can be measured in different ways, some of which depend on the specific cloud service; a computational cloud service is different than an email cloud service and service availability for each will be computed differently.

6 Relationship between the cloud service agreement and SLAs

Cloud services, particularly public cloud services, generally involve an agreement between the CSC and the CSP concerning the acquisition and use of the cloud services. For the purposes of this standard, the legal agreement is referred to as the “Cloud Service Agreement” or CSA. The CSA has a number of synonyms such as “Master Service Agreement”, "Customer Agreement", "Terms of Service" or simply "Agreement".

A CSA comprises one or more parts recorded in one of more documents. Contents of each part can appear in more than one document. There is no normative relationship between parts and documents i.e. a part does not have to be in a single document, and a document does not have to contain a whole part. There is neither a standard naming convention for the parts or documents of a CSA, nor a standard structure for the documents or parts.

Examples of common parts of CSAs include

- Cloud Service Level Agreement (cloud SLA).
  The cloud SLA ordinarily contains a collection of SLOs and SQOs relating to the cloud service, covering aspects of the service. This might include availability, reliability, performance, security, data protection, compliance and data handling.
- Acceptable Use Policy (AUP).
  The acceptable use policy usually defines boundaries for the CSC's use of the cloud service. This might include restrictions that prevent the CSC from installing malware on the cloud service or limit the kind of data that can be stored.
- Security Policy.
  The security policy typically describes responsibilities that apply to the CSC and to the CSP, SLOs and SQOs which the CSP applies to the cloud service in security terms and potentially indicates which security certifications or standards are met by the cloud service.
- Data Protection Policy
  The data protection policy typically deals with the handling of personal data or sensitive data by the cloud service, including SQOs for specific data protection measures and privacy certifications or standards that apply to the service.
- Business Continuity Policy.
  The business continuity policy typically deals with the resilience aspects of the cloud service and can include measures that are implemented by the CSP to avoid data loss and to deal with outages, such as backups and redundant components.
- Termination Policy.
  The Termination Policy usually deals with the issues that arise when a CSC terminates their use of one or more cloud services. The termination policy might include SQOs for areas such as notifications, data reversibility and data deletion.