INTERNATIONAL STANDARD

ISO/IEC 19086-4

First edition
2019-01

Cloud computing — Service level agreement (SLA) framework —

Part 4: Components of security and of protection of PII

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

Partie 4: Eléments de sécurité et de protection des PII

Reference number
ISO/IEC 19086-4:2019(E)

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

Published in Switzerland

Contents

Page

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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document can be used by any organization or individual involved in the creation, modification or understanding of a cloud service level agreement which conforms to ISO/IEC 19086 (all parts). The cloud SLA accounts for the key characteristics of a cloud service and aims to facilitate a common understanding between cloud service providers (CSPs) and cloud service customers (CSCs).

This document builds on the foundational concepts and definitions described by ISO/IEC 19086-1.

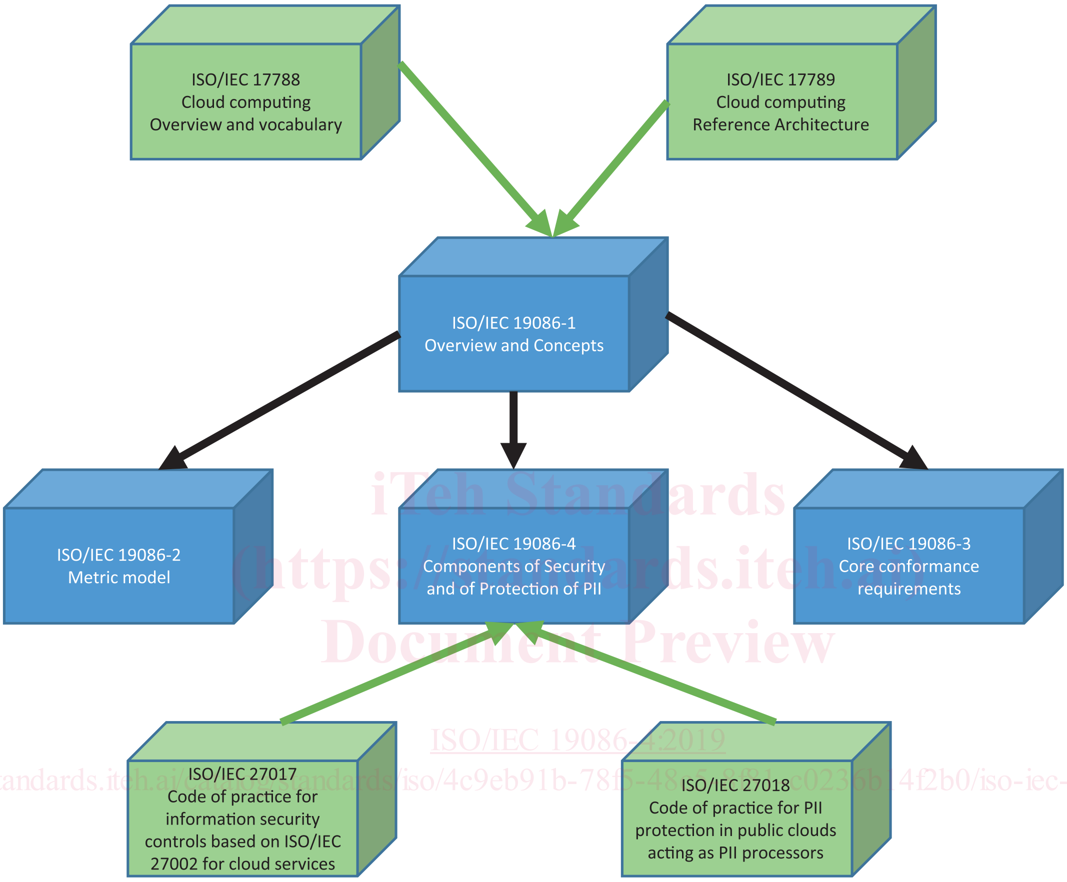

Figure 1 — Relationship of parts of ISO/IEC 19086 (all parts) and other cloud computing standards

Figure 1 presents an overview of the content of the ISO/IEC 19086 series and the relationships between the parts of ISO/IEC 19086 and other key International Standards relating to cloud computing.

Cloud computing — Service level agreement (SLA) framework —

Part 4: Components of security and of protection of PII

1 Scope

This document specifies security and protection of personally identifiable information components, SLOs and SQOs for cloud service level agreements (cloud SLA) including requirements and guidance.

This document is for the benefit and use of both CSPs and CSCs.

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*

ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788, ISO/IEC 19086-1, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 29100 apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Symbols and abbreviated terms

CSC	cloud service customer
CSP	cloud service provider
CSA	cloud service agreement
Cloud SLA	Cloud service level agreement

PII	personally identifiable information
SLA	service level agreement
SLO	cloud service level objective
SQO	cloud service qualitative objective
VPN	virtual private network

5 Relationship with other parts of the cloud computing SLA framework

5.1 General

ISO/IEC 19086-1 provides an overview, foundational concepts, and definitions for the cloud SLA framework. In particular, it defines the following fundamental concepts of the cloud SLA framework:

— Cloud Service Agreement (CSA);

— Cloud Service Level Agreement (Cloud SLA);

— Cloud Service Level Objectives (SLO);

— Cloud Service Qualitative Objectives (SQO).

ISO/IEC 19086-1 also describes the content areas and components that consist of a list of SLOs and SQOs.

ISO/IEC 19086-2 provides a metric model to be used for specifying metrics used for cloud SLAs.

ISO/IEC 19086-3 provides the core conformance requirements derived from the SLOs and SQOs defined in ISO/IEC 19086-1.

This document builds on the foundational concepts and definitions described by ISO/IEC 19086-1 to address security and protection of PII components.

ISO/IEC 19086 (all parts) is intended to facilitate a common understanding between CSCs and CSPs. Cloud service agreements and their associated cloud SLAs vary between CSPs, and in some cases different CSCs can negotiate different contract terms with the same CSP for a particular cloud service. This document aims to assist CSCs when they compare cloud services from different CSPs, with respect to material that covers security and protection of personally identifiable information. This document should be used in conjunction with ISO/IEC 19086-1 for a full understanding of a cloud SLA.

5.2 Conformance

ISO/IEC 19086-3:2017, Clause 5 describes conformance for a cloud SLA in the context of ISO/IEC 19086-1. This document follows the same principle regarding a conforming cloud SLA. In each of the components identified in this document in the areas of security (Clause 7) and protection of PII (Clause 8), there are one or more SLOs or SQOs. When using one of the components from Clauses 7 or 8, a conforming cloud SLA is not required to use the SLOs or SQOs described in those components. A conforming cloud SLA should use SLOs and SQOs from this document, 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 in this document.

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

A conforming cloud SLA may use a subset of the components described in this document (Clauses 7 and 8) and it may include components 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 this document and in ISO/IEC 19086-1, and the requirements as stated in this document. Where a cloud

SLA contains a specific component or content area, it shall adhere to all the requirements specified for that component or content area. Conformance to this document does not require implementation of any specific technology.

6 Overview

6.1 General

This document builds on foundational cloud SLA concepts covered in general in ISO/IEC 19086-1. A description of each security or protection of PII component is provided with applicable SLOs and SQOs. As explained in ISO/IEC 19086-1, a CSP can offer more than one SLO, SQO or both.

The specific components and the conformance requirements for SLOs and SQOs in the area of security and protection of PII are detailed in this document. The security components (7.1 to 7.13) follow the structure of ISO/IEC 27002 and the cloud-specific information security controls defined in ISO/IEC 27017. The protection of PII components (8.1 to 8.9) follow the structure of ISO/IEC 29100 and the cloud-specific PII related controls defined in ISO/IEC 27018.

Using the definitions of SLO and SQO stated in ISO/IEC 19086-1 and the metric model described in ISO/IEC 19086-2, CSPs are able to specify their SLOs and SQOs. A CSC can then express its requirements for the covered services using the same SLOs and SQOs as the CSP. This allows the CSC to directly compare its requirements to determine which CSP's capabilities best meet the CSC's requirements. Further guidance on evaluating SQOs and SLOs, and accepting cloud SLAs, is provided in ISO/IEC 19086-1:2016, 7.3.

6.2 Structure of this document

The order of the clauses in this document does not imply their importance or priority. Each component for security and protection of PII should be considered according to cloud service categories, cloud capabilities types and cloud deployment models (see ISO/IEC 17788).

Components are structured as follows:

1) Description: describes the specific component. Description of the core conformance requirements and the guidance on those core requirements for each specific component.

2) List of SLOs and SQOs: describes the relevant SLOs and SQOs.

   The definition of an SLO is provided in ISO/IEC 19086-1 as follows: "commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the *interval scale* or *ratio scale*".

   The definition of an SQO is provided in ISO/IEC 19086-1 as follows: "commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the *nominal scale* or *ordinal scale*". Description of the core conformance requirements and the guidance on those core requirements for each specific component.

3) Guidance: provides more detailed information to support the implementation of the SLO or SQO. It is possible that the guidance is not entirely suitable or sufficient in all situations and does not fulfil the CSP's specific SLO or SQO requirements.

7 Information security components

7.1 Information security policy component

7.1.1 Description

Information security policies describe the policy and/or the process for securing the provision, operation and maintenance of the covered services.

An information security policy component shall specify the information security policy that applies to the covered services.

7.1.2 Cloud service qualitative objectives

Information security policy

A statement that describes the CSP's policies and processes for securing the covered services.

An information security policy SQO shall describe the information security policy that relates to the covered services.

7.1.3 Guidance

Information about information security policies can be found in ISO/IEC 27002 and ISO/IEC 27017.

NOTE ISO/IEC 27017:2015, 5.1.1 describes what the information security policy should encompass.

7.2 Organization of information security component

7.2.1 Description

The organization of information security component describes the separation of roles and responsibilities between the CSP and the CSC.

An organization of information security component shall specify roles and responsibilities in relation to the covered services.

7.2.2 Cloud service qualitative objectives

Allocation of roles and responsibilities

A statement of the separation of the roles and responsibilities between the CSP and the CSC.

An allocation of roles and responsibilities SQO shall provide a statement of the allocation of roles and responsibilities between the CSC and the CSP for the covered services.

7.2.3 Guidance

Information about the organization of information security component can be found in ISO/IEC 27002 and ISO/IEC 27017.

7.3 Asset management component

7.3.1 Description

The asset management component deals with identifying the assets covered and defining the responsibilities regarding those assets, in terms of the CSC or the CSP. Assets can include hardware, software and/or data, in terms of the CSC or the CSP.

