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/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **1**
5 Relationship with other parts of the cloud computing SLA framework **2**
5.1 General 2
5.2 Conformance 2
6 Overview **3**
6.1 General 3
6.2 Structure of this document 3
7 Information security components **4**
7.1 Information security policy component 4
7.1.1 Description 4
7.1.2 Cloud service qualitative objectives 4
7.1.3 Guidance 4
7.2 Organization of information security component 4
7.2.1 Description 4
7.2.2 Cloud service qualitative objectives 4
7.2.3 Guidance 4
7.3 Asset management component 4
7.3.1 Description 4
7.3.2 Cloud service level objectives 5
7.3.3 Cloud service qualitative objectives 5
7.3.4 Guidance 5
7.4 Access control component 5
7.4.1 Description 5
7.4.2 Cloud service level objectives 5
7.4.3 Cloud service qualitative objectives 6
7.4.4 Guidance 6
7.5 Cryptography component 7
7.5.1 Description 7
7.5.2 Cloud service qualitative objectives 7
7.5.3 Guidance 7
7.6 Physical and environmental security component 8
7.6.1 Description 8
7.6.2 Cloud service qualitative objectives 8
7.6.3 Guidance 8
7.7 Operations security component 9
7.7.1 Description 9
7.7.2 Cloud service level objectives 9
7.7.3 Cloud service qualitative objectives 9
7.7.4 Guidance 10
7.8 Communications security component 10
7.8.1 Description 10
7.8.2 Cloud service qualitative objectives 10
7.8.3 Guidance 10
7.9 Systems acquisition, development and maintenance component 10
7.9.1 Description 10
7.9.2 Cloud service qualitative objectives 11
7.9.3 Guidance 11

© ISO/IEC 2019 – All rights reserved

7.10 Supplier relationships component 11
7.10.1 Description 11
7.10.2 Cloud service qualitative objectives 11
7.10.3 Guidance 12
7.11 Information security incident management component 12
7.11.1 Description 12
7.11.2 Cloud service level objectives 12
7.11.3 Cloud service qualitative objectives 12
7.11.4 Guidance 12
7.12 Business continuity management component 12
7.12.1 Description 12
7.12.2 Cloud service qualitative objectives 12
7.12.3 Guidance 13
7.13 Compliance component 13
7.13.1 Description 13
7.13.2 Cloud service qualitative objectives 13
7.13.3 Guidance 13

8 Protection of personally identifiable information component 13
8.1 Consent and choice component 13
8.1.1 Description 13
8.1.2 Cloud service qualitative objectives 13
8.1.3 Guidance 14
8.2 Purpose legitimacy and specification component 14
8.2.1 Description 14
8.2.2 Cloud service qualitative objectives 14
8.2.3 Guidance 14
8.3 Data minimization component 14
8.3.1 Description 14
8.3.2 Cloud service level objectives 15
8.3.3 Cloud service qualitative objectives 15
8.3.4 Guidance 15
8.4 Use, retention and disclosure limitation component 15
8.4.1 Description 15
8.4.2 Cloud service qualitative objectives 15
8.4.3 Guidance 15
8.5 Accuracy and quality component 16
8.5.1 Description 16
8.5.2 Cloud service qualitative objectives 16
8.5.3 Guidance 16
8.6 Openness, transparency and notice component 16
8.6.1 Description 16
8.6.2 Cloud service qualitative objectives 16
8.6.3 Guidance 17
8.7 Individual participation and access component 17
8.7.1 Description 17
8.7.2 Cloud service qualitative objectives 17
8.7.3 Guidance 17
8.8 Accountability component 17
8.8.1 Description 17
8.8.2 Cloud service level objectives 18
8.8.3 Cloud service qualitative objectives 18
8.8.4 Guidance 18
8.9 Protection of PII compliance component 18
8.9.1 Description 18
8.9.2 Cloud service qualitative objectives 18
8.9.3 Guidance 19

Bibliography 20

 © ISO/IEC 2019 – All rights reserved

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.

© ISO/IEC 2019 – All rights reserved

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.

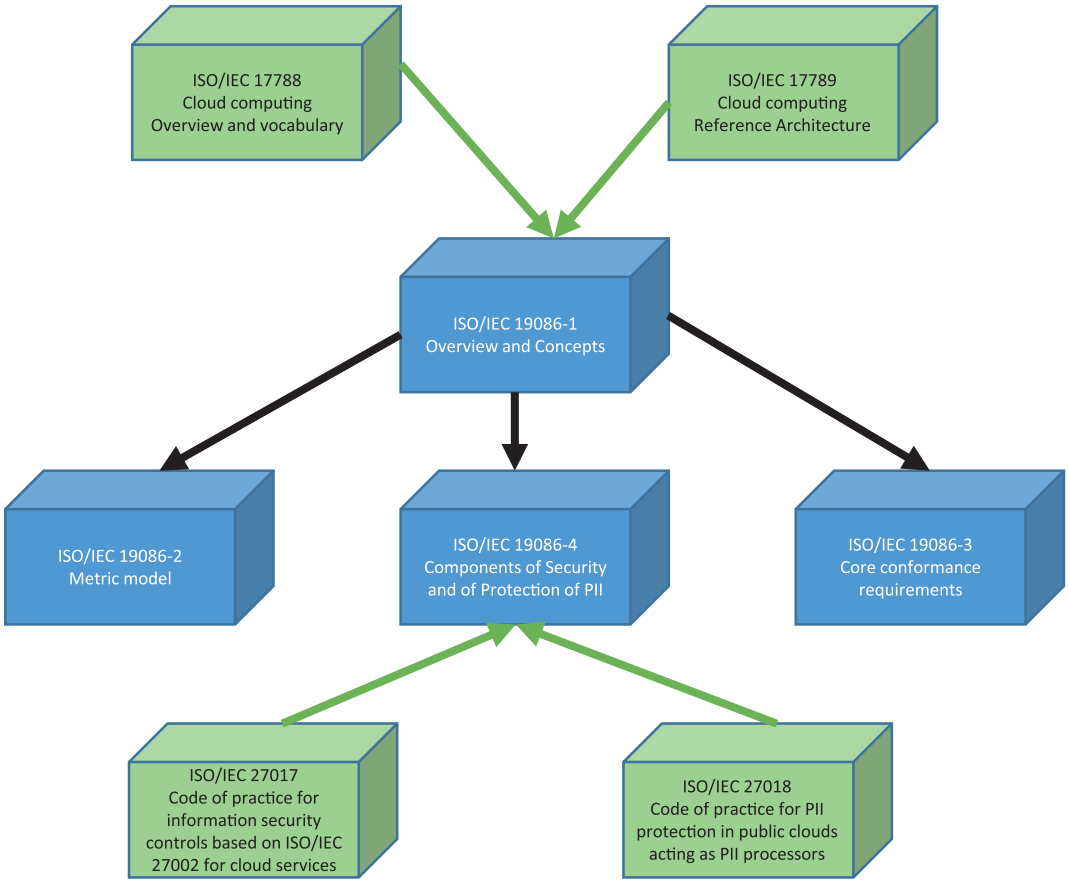


Figure 1 — Relationship of parts of ISO/IEC 19086 (all parts) and other cloud computing standards

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.

© ISO/IEC 2019 – All rights reserved

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

© ISO/IEC 2019 – All rights reserved