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.

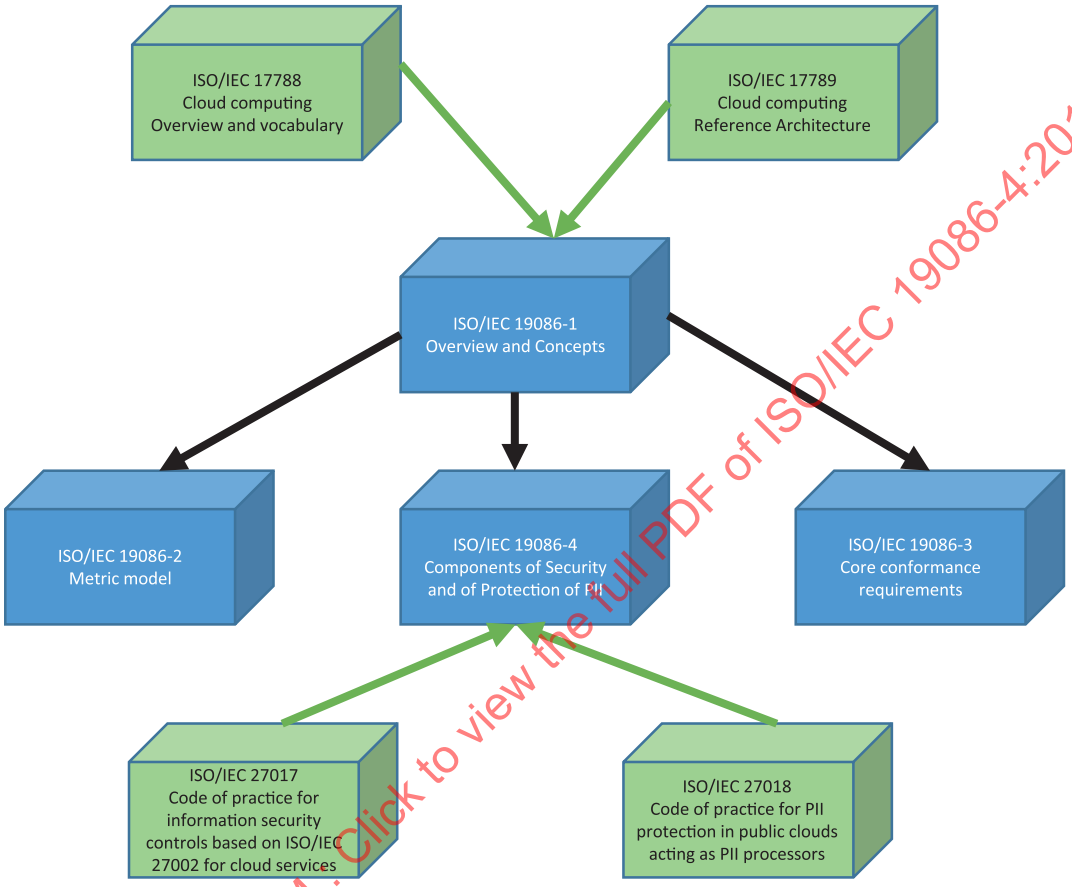

Figure 1 — Relationship of parts of ISO/IEC 19086 (all parts) and other cloud computing standards

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.

An asset management component shall specify the assets and responsibilities relating to those assets in relation to the covered services.

7.3.2 Cloud service level objectives

Asset data update frequency

The maximum interval between refreshes of the asset database.

An asset data update frequency SLO shall specify the maximum interval between refreshes of the asset database.

7.3.3 Cloud service qualitative objectives

Asset and responsibility inventory

A list of the assets or categories of assets and the responsibilities, in terms of the CSC or the CSP, regarding those assets or categories of assets relating to the covered services.

An asset and responsibility SQO shall provide a list of the assets and the responsibilities regarding those assets for the covered services.

7.3.4 Guidance

Additional information about categories of data types, expressed as a taxonomy, that can be used to describe those assets can be found in ISO/IEC 19944.

Additional information about asset management can be found in ISO/IEC 27017:2015, Clause 8.

7.4 Access control component

7.4.1 Description

The access control component deals with the access controls in place for the covered services, including the service access, administration access and business access as described in ISO/IEC 17789.

An access control component shall specify the access controls relating to the covered services.

7.4.2 Cloud service level objectives

7.4.2.1 Maximum time required to revoke user access

The maximum time required to revoke user access to the covered services.

A maximum time required to revoke user access SLO shall provide the maximum time to revoke access to the covered services.

7.4.2.2 Time required to revoke user access at a specified commitment level

The time required to revoke user access to the covered services for at least the specified fraction of all such requests. For example, 95 % of user revocation requested is completed within two hours.

A time required to revoke user access at a specified commitment level SLO shall provide a specified lower bound on the percentile of user revocation requests that shall be completed within the specified upper bound on elapsed time.

7.4.3 Cloud service qualitative objectives

7.4.3.1 User registration and de-registration

A statement describing the process used for registering and de-registering cloud service users for the covered services.

A user registration and de-registration SQO shall specify the process used for registering and de-registering cloud service users for the covered services.

7.4.3.2 Review access patterns

A statement describing the capabilities to support review of access patterns and to proactively identify and mitigate potential threats.

A review access patterns SQO shall provide a statement describing the capabilities for review of access patterns and to identify and mitigate potential threats for the covered services.

7.4.3.3 Authentication mechanism

A description of the available authentication mechanisms supported by the CSP on the covered services.

A description of the available authentication mechanisms for both users and administrators supported by the CSP on its covered services.

An authentication mechanism SQO shall provide a description of the available authentication mechanisms for the covered services.

7.4.3.4 Third-party authentication support

A description of what third-party authentication mechanisms are supported by the CSP.

A third-party authentication support SQO shall provide a description of the available third-party authentication mechanisms for the covered services.

7.4.3.5 Strong authentication support

A description of any strong authentication mechanisms which can be used to control CSC's access to covered services. This includes for example multi-factor authentication.

A strong authentication support SQO shall provide a description of the available strong authentication mechanisms for the covered services.

7.4.3.6 Anonymous and pseudonymous authentication support

A description of available mechanisms for anonymous and pseudonymous authentication support provided for the covered services.

An anonymous and pseudonymous authentication support SQO shall provide a description of the available mechanisms for anonymous and pseudonymous authentication support for the covered services.

7.4.4 Guidance

Access control guidance for cloud computing is given in ISO/IEC 27017 and ISO/IEC 27002.

Additional information about access control can be found in ISO/IEC 27002.

7.5 Cryptography component

7.5.1 Description

A description of cryptographic controls that the CSP offers to the CSC for the covered services. The controls are given for the three states of data in motion, data at rest and data during execution.

Cryptography is described in ISO/IEC 27002.

A cryptography component shall specify the cryptographic controls relating to the covered services. The specification shall include an identifier for the protocols and algorithms used, as well as a definition of their cryptographic strength such that controls become comparable for the CSC.

7.5.2 Cloud service qualitative objectives

7.5.2.1 Cryptographic controls for data in motion

A description of the cryptographic controls available for data in motion associated with the covered services.

NOTE These controls provide for securing data with respect to confidentiality and integrity, while being transferred within a covered service, between covered services, and between the CSC and the covered services.

A cryptographic controls for data in motion SQO shall describe the cryptographic controls for the protection of data in motion.

7.5.2.2 Cryptographic controls for data at rest

A description of the cryptographic controls available for data at rest associated with the covered services.

NOTE These controls provide for securing data with respect to confidentiality and integrity, while being stored in the covered services.

A cryptographic controls for data at rest SQO shall describe the cryptographic controls available for the protection of data at rest.

7.5.2.3 Cryptographic controls for data during execution

A description of the cryptographic controls available for data during execution associated with the covered services.

NOTE These controls provide for securing data with respect to confidentiality and integrity, while being processed in the covered services.

A cryptographic controls for data during execution SQO shall describe the cryptographic controls available for the protection of data during execution.

7.5.2.4 Key management policy

A statement describing the key management policy for the covered services which can include any mechanisms in place to isolate customer controlled keys from the CSP.

A key management policy SQO shall provide a description of the key management policy for the covered services.

7.5.3 Guidance

Cryptographic controls are described in ISO/IEC 27002.

ISO/IEC 27040 provides definitions for data in motion and data at rest.

7.6 Physical and environmental security component

7.6.1 Description

The physical and environmental security component describes the security processes and controls provided by the CSP to protect the physical facilities used to provide the covered services from loss of data, connectivity and availability of necessary infrastructure and IT equipment. These processes and controls should protect the physical facilities from theft, fire, flood, earthquake, intentional destruction, unintentional damage, mechanical equipment failure and power failures.

Physical facilities include the building shell, infrastructure equipment such as cooling, power distribution, security and fire protection systems along with IT equipment such as servers, storage and network equipment. Physical facilities also include any locations, such as operations centres for monitoring the covered services that can process CSC data, derived data and CSP data.

A physical and environmental security component shall specify the physical security controls relating to the covered services.

7.6.2 Cloud service qualitative objectives

7.6.2.1 Data centre monitoring

A statement describing the monitoring done on data centres used for the covered services. This is covered in ISO/IEC 19086-1:2016, 9.4.

A data centre monitoring SQO shall describe the monitoring of the data centres used for the covered services.

7.6.2.2 Secure disposal and re-use of equipment

A description of processes for the secure disposal and re-use of equipment.

A secure disposal and re-use of equipment SQO shall describe the processes for secure disposal and re-use of equipment related to the covered services.

The secure disposal and re-use of equipment process shall ensure that data is deleted from storage devices, and state how devices no longer in use are disposed of. ISO/IEC 19086-1:2016, 10.12.8 covers the cloud SLA data deletion component.

7.6.2.3 Facilities authorization

A statement describing the policy and process for granting access to the facilities used to provide the covered services.

A facilities authorization SQO shall describe the policy and process for granting access to the facilities used for the covered services.

7.6.3 Guidance

Information on physical and environmental security can be found in ISO/IEC 27002.

Information on techniques for data deletion from storage devices can be found in ISO/IEC 27040.

7.7 Operations security component

7.7.1 Description

An operations security component specifies processes that secure the covered services during the operation of the covered services.

An operations security component shall specify the processes in place to secure the covered services during operation.

7.7.2 Cloud service level objectives

7.7.2.1 Vulnerability reporting interval

The maximum time for the CSP to send a vulnerability report to the CSC following the discovery of a vulnerability.

NOTE Vulnerabilities that are reported are described in the vulnerability management SQO (7.7.3.3).

A vulnerability reporting interval SLO shall state the maximum time for the CSP to send a vulnerability report to the CSC following the discovery of a vulnerability related to the covered services.

7.7.2.2 Period of time of logs availability

A defined period of time during which the logs are available for analysis by the CSC.

A period of time of logs availability SLO shall state the period of time for which the logs are available for analysis by the CSC for the covered services.

7.7.3 Cloud service qualitative objectives

7.7.3.1 Malware protection

A statement describing mechanisms to ensure the availability and any routine application of any anti-malware protection offered by the CSP for the covered services.

A malware protection SQO shall describe the availability and application of anti-malware protection for the covered services.

7.7.3.2 Logging and monitoring

A statement describing the logging and monitoring relating to the security of the covered services and the methods the CSC can use to access reports of that logging and monitoring.

A logging and monitoring SQO shall describe the logging and monitoring relating to the security of the covered services and the methods the CSC can use to access reports of the logging and monitoring.

7.7.3.3 Vulnerability management

A description of the process for the monitoring, identification, notification and patching of technical vulnerabilities of the covered services.

A vulnerability management SQO shall describe the process for monitoring, identification, notification and patching of technical vulnerabilities for the covered services.

7.7.3.4 Vulnerability notification method

A description of the method the CSP uses to notify the CSC of technical vulnerabilities and their associated fixes relating to the covered services.

A vulnerability notification method SQO shall describe the method the CSP uses to notify the CSC of technical vulnerabilities and their associated fixes relating to the covered services.

7.7.3.5 Vulnerability impact statement

A statement describing the process used by the CSP to describe the impact of vulnerabilities.

A vulnerability impact statement SQO shall describe the process used by the CSP to describe the impact of vulnerabilities for the covered services.

7.7.4 Guidance

A vulnerability management process is defined in ISO/IEC 30111.

ISO/IEC 29147 provides additional information on describing the vulnerability impact.

Change management is covered in ISO/IEC 19086-1:2016, 10.10.1.

7.8 Communications security component

7.8.1 Description

The communications security component specifies the needs for securing the network and any other communications channels used in the covered services.

A communications security component shall describe the security controls in place for the networks and communications channels used by the covered services.

7.8.2 Cloud service qualitative objectives

Network segregation

A description of the technical means used to ensure segregation of network access both between tenants in a multi-tenant environment and also between the CSP administration capabilities and the CSC's environment and prevent unauthorized tenant to tenant communications.

A network segregation SQO shall describe the technical means used to ensure segregation of network access for the covered services.

7.8.3 Guidance

ISO/IEC 27033 (all parts) provides implementation guidance for communications security covering Network Security, Security gateways, VPNs and Wireless security.

ISO/IEC 27002:2013, 13.2.1 provides further information on communications security.

7.9 Systems acquisition, development and maintenance component

7.9.1 Description

The system acquisition, development and maintenance component describes the processes implemented to secure system acquisition, development and ongoing maintenance of the covered services.

A systems acquisition, development and maintenance component shall describe the information security controls in place for the acquisition, development and maintenance of elements related to the covered services.

7.9.2 Cloud service qualitative objectives

7.9.2.1 System acquisition procedures

A statement that describes the information security related procedures of the CSP when acquiring systems or components from third parties to be used for the provision of the covered services.

A system acquisition procedures SQO shall describe the information security related procedures of the CSP when acquiring a system or component from third parties to be used for the provision of the covered services.

7.9.2.2 Secure development procedures

A description of the secure development procedures used by the CSP when developing the covered services and associated systems.

A secure development procedures SQO shall describe the secure development procedures used by the CSP when developing the covered services and associated systems.

7.9.2.3 Maintenance procedures

A statement describing the information security and privacy related measures a CSP undertakes to maintain the secure operation of the covered services. Examples are procedures on updating software and hardware, including the documentation of those steps.

NOTE Vulnerability management is treated in 7.7.3.3.

A system maintenance procedures SQO shall describe the information security related measures a CSP undertakes to maintain the secure operation of the covered services.

7.9.3 Guidance

Acquisition, development and maintenance procedures for systems are described in ISO/IEC 27017.

Secure disposal of decommissioned hardware is described in ISO/IEC 27040.

Risk Management is described in ISO 31000.

ISO/IEC 27034 (all parts) provides information on securing the application development lifecycle.

7.10 Supplier relationships component

7.10.1 Description

Managing supplier relationships is an integral part of cloud services and, as such, the supplier relationships component specifies how these relationships are managed.

A supplier relationships component shall describe how supplier relationships are managed for the covered services.

7.10.2 Cloud service qualitative objectives

Supplier relationship management

A description of how the CSP procures, utilizes, secures, monitors, maintains and reviews the use of third-party services.

A supplier relationship management SQO shall provide a description of how the CSP procures, secures, monitors, maintains and reviews the use of third party services in the provision of the covered services.

7.10.3 Guidance

Information on securing supplier relationships for cloud services can be found in ISO/IEC 27036-4, ISO/IEC 27002 and ISO/IEC 27017.

7.11 Information security incident management component

7.11.1 Description

The information security incident management component specifies the process and actions to be taken regarding incidents that arise in the covered services.

An information security incident management component shall document the process and actions to be taken regarding incidents that arise related to the covered services.

7.11.2 Cloud service level objectives

Information security incident notification period

Description of the maximum length of time taken for the CSP to notify the CSC of the occurrence of an information security incident.

An information security incident notification period SLO shall describe the maximum length of time taken for the CSP to notify the CSC of the occurrence of an information security incident in relation to the covered services.

7.11.3 Cloud service qualitative objectives

Information security incident management

A statement documenting information security incident management procedures used by the CSP.

An information security incident management SQO shall document information security incident management procedures used in relation to the covered services.

7.11.4 Guidance

ISO/IEC 27035-1 and ISO/IEC 27035-2 cover information security incident management.

ISO/IEC 19086-1:2016, 10.8.1 provides additional SLOs and SQOs for incident management.

7.12 Business continuity management component

7.12.1 Description

The business continuity management component specifies the processes used by the CSP to ensure business continuity for the covered services.

A business continuity management component shall document the business continuity processes used by the CSP in relation to the covered services.

7.12.2 Cloud service qualitative objectives

Business continuity process

A statement describing the process used by the CSP to ensure business continuity of the cloud service.

A business continuity process SQO shall describe the business continuity process used in relation to the covered services.

7.12.3 Guidance

ISO/IEC 19086-1:2016, 10.11.2 covers SLOs and SQOs relating to service resilience and fault tolerance. ISO/IEC 19086-1:2016, 10.11.4 covers disaster recovery SLOs and SQOs.

ISO/IEC 27031:2011, 6.7 covers ICT performance measurement for ICT readiness.

ISO/IEC 27031:2011, 8.4.2 covers quantitative and qualitative performance measurement for ICT readiness.

7.13 Compliance component

7.13.1 Description

A CSC can have responsibilities with respect to attaining compliance to security standards, policies and regulations for the use of the covered services. The compliance component covers the methods CSPs may use to demonstrate such compliance.

The compliance component shall describe the aspects of compliance that the CSP attests to in relation to the covered services.

7.13.2 Cloud service qualitative objectives

NOTE ISO/IEC 19086-1:2016, 10.13 presents SQOs for attestations, certifications and audits as methods of the CSP to demonstrate compliance with standards, policies and regulations in general. The same SQOs can be applied for the demonstration of compliance with security standards, policies and regulations, in particular.

7.13.3 Guidance

ISO 19600 describes compliance management systems.

8 Protection of personally identifiable information component

8.1 Consent and choice component

8.1.1 Description

The CSP should provide the CSC with the means to enable the PII principals to exercise choice and express their consent in relation to the processing of their PII.

A consent and choice component shall describe the consent and choice capabilities for PII principals in the covered services.

NOTE The underlying privacy principles of the security and protection of PII components are described in ISO/IEC 29100.

8.1.2 Cloud service qualitative objectives

PII principal consent capabilities

A description of the mechanisms provided by the covered services to PII principals to exercise choice and to give consent in relation to the processing of their PII.

A PII principal consent capabilities SQO shall describe the mechanisms provided to PII principals to exercise choice and to give consent in relation to the processing of their PII in the covered services.

8.1.3 Guidance

Guidance is described in ISO/IEC 27018:2014, A.1.

8.2 Purpose legitimacy and specification component

8.2.1 Description

The purpose legitimacy and specification component describes SQOs for the legitimacy for the processing of CSC PII including any commitments to only process PII according to the CSA.

A purpose legitimacy and specification component shall describe the basis for the legitimate processing of PII in the covered services.

8.2.2 Cloud service qualitative objectives

8.2.2.1 Purpose legitimacy

A statement that the CSP only processes PII for purposes explicitly stated in the CSA.

A statement that the CSP processing of PII adheres to appropriate legal, regulatory and contractual requirements.

A purpose legitimacy SQO shall state that PII is only processed for purposes stated in the CSA for the covered services and that such processing adheres to appropriate legal, regulatory and contractual requirements.

8.2.2.2 Third-party access list

A list of third parties to the agreement between the CSC and the CSP, excluding those listed in response to 8.6.2.1 (PII subcontractor list), that have access to PII relating to the CSC, including the CSC's users and tenants.

A third-party access list SQO shall list third parties (other than subcontractors) who have access to PII relating to the CSC in the covered services.

8.2.3 Guidance

ISO/IEC 19944 provides categories of data in cloud services and supports the creation of data use statements with defined terms. Data use statements created according to ISO/IEC 19944 can be used by CSPs to define the specific use of data in the covered services, providing support for claims of legitimate use and collection limitation.

Guidance is also provided in ISO/IEC 27018:2014, A.2.

8.3 Data minimization component

8.3.1 Description

The data minimization component specifies the minimization of PII processing and access.

This can be achieved by limiting the maximum retention time for temporary files, by reducing the number of stakeholders with access to the PII, or by reducing the generation and exposure of PII by technical (cryptographic) means in the cloud service itself.

A data minimization component shall describe the minimization of PII processing and access in the covered services.

8.3.2 Cloud service level objectives

Maximum retention time for temporary files

The maximum period for which temporary files generated during processing are retained before being deleted or made permanently inaccessible.

A maximum retention time for temporary files SLO shall state the maximum period for which temporary files, which include PII, generated during processing are retained by the covered services.

8.3.3 Cloud service qualitative objectives

8.3.3.1 Minimize stakeholder access

A statement describing the policy for minimizing which people to whom PII is disclosed or have access along with the scope of that access.

A minimize stakeholder access SQO shall describe the policy for minimizing the number of people who have access to PII or to whom PII is disclosed in relation to the covered services.

8.3.3.2 Data minimization cryptographic controls

The description of the cryptographic controls available for minimization of PII processed by the covered services.

A data minimization cryptographic controls SQO shall describe the cryptographic controls available for the minimization of PII processed by the covered services.

8.3.4 Guidance

Guidance is described in ISO/IEC 27018:2014, A.4.

For additional detail, see ISO/IEC 19086-1:2016, 10.12.8.

ISO/IEC 29100:2011, 2.23 provides the definition of processing. ISO/IEC 29100:2011, 5.5 defines data minimization.

8.4 Use, retention and disclosure limitation component

8.4.1 Description

The use, retention and disclosure limitation component shall describe the use, retention and disclosure limitation of PII in relation to the covered services.

8.4.2 Cloud service qualitative objectives

Data use statements

Statements of the use made by the CSP of any data that can potentially contain PII.

A data use statements SQO shall describe the use made by the CSP of any data that can potentially contain PII in relation to the covered services.

8.4.3 Guidance

Data retention is dealt with in ISO/IEC 19086-1:2016, 10.7.1.1.

Disclosure of PII under law enforcement/regulatory requests is dealt with in ISO/IEC 19086-1:2016, 10.12.11.3.

Controls and associated implementation guidance is given in ISO/IEC 27018:2014, A.5.

Use, retention and disclosure limitation of PII is described in ISO/IEC 27018:2014, A.5.

Data use statements and the data classifications used for them are described in ISO/IEC 19944.

8.5 Accuracy and quality component

8.5.1 Description

The accuracy and quality component describes SQOs related to the accuracy, integrity and quality of PII.

An accuracy and quality component shall describe the means by which the covered services ensure that PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use.

8.5.2 Cloud service qualitative objectives

PII integrity, accuracy and quality

A statement describing the policy and process used to check the collected, stored, and updated PII for accuracy, integrity, and quality.

A PII integrity, accuracy and quality SQO shall describe the policy and process used to check the collected, stored, and updated PII for accuracy, integrity, and quality in relation to the covered services.

8.5.3 Guidance

Guidance is described in ISO/IEC 27018:2014, A.6.

For guidance on accuracy and quality of PII, see ISO/IEC 29100.

8.6 Openness, transparency and notice component

8.6.1 Description

The openness, transparency and notice component describes SQOs pertaining to the subcontractors used by the CSP, who have access to PII and the mechanisms the CSP uses to gain and store consent for the collection, processing and retention of PII.

An openness, transparency and notice component shall describe the notification of PII collection and processing of PII and notification of any subcontractors used to process the PII in relation to the covered services.

8.6.2 Cloud service qualitative objectives

8.6.2.1 PII subcontractor list

A list of the subcontractors of the CSP who have access to the CSC data containing PII.

A PII subcontractor list SQO shall provide a list of the subcontractors used to process PII in relation to the covered services.

8.6.2.2 Requirement for specific consent

Where the CSP collects PII, a description of the means by which the CSP provides notification to PII principals of the collection, processing and retention of PII, and the means by which the CSP obtains and stores their consent.