TECHNICAL REPORT

ISO/IEC TR 23187

First edition

Information technology — Cloud computing — Interacting with cloud service partners (CSNs)

PROOF/ÉPREUVE

Reference number
ISO/IEC TR 23187:2020(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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

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

The purpose of this document is to expand on the understanding of the interactions between cloud service partners (CSNs) and cloud service customers (CSCs), and between CSNs and cloud service providers (CSPs).

Cloud computing offers solutions to many emerging technologies and it offers many benefits to all cloud service users (CSUs) and CSCs. The broader requirement for cloud computing solutions is to ensure organizations have the best capabilities to fulfil their business missions. This has helped to drive the adoption of cloud services and the marketplace is adjusting to the increasing demands.

In finding and applying appropriate solutions and leveraging the many benefits of using cloud services, many CSCs use multiple CSPs and various deployment models. In using, sharing, and assessing data, an understanding and clarification of roles, activities and responsibilities will help to maintain the security, privacy, confidentiality and integrity of cloud services.

Interactions of CSCs and CSPs with the various CSNs have caused a degree of concern and confusion in the cloud service marketplace. In some cases, causing harm to CSCs through inappropriate security controls and the lack of proper cloud service agreements relating to the cloud services being used. This is in part caused by an inadequate understanding of the relationships involved and by the lack of standards which might apply to those relationships.

Interactions between CSCs and CSPs have been described in detail in standards documents – ISO/IEC 17789, ISO 19011, ISO/IEC 19941, ISO/IEC 27017, ISO/IEC 27018 and the ISO/IEC 19086 series. Interactions of CSNs, a key role in the cloud service environment, with CSCs and CSPs have not been described in similar detail. This document provides further clarity about those interactions.

This document provides clarification of the concepts provided in ISO/IEC 17788, ISO/IEC 17789, the ISO/IEC 19086 series, and ISO/IEC 19941 regarding CSNs, and CSN interactions with CSCs and CSPs with the help of a few exemplary market scenarios. Building on an expanded description of sub-roles and activities, this document provides guidance on using cloud service agreements (CSAs) and cloud service level agreements (cloud SLAs) to provide more clarity for CSN interactions.

Information technology — Cloud computing — Interacting with cloud service partners (CSNs)

1 Scope

This document provides an overview of and guidance on interactions between cloud service partners (CSNs), specifically cloud service brokers, cloud service developers and cloud auditors, and other cloud service roles. In addition, this document describes how cloud service agreements (CSAs) and cloud service level agreements (cloud SLAs) should be used to address those interactions, including the following:

— definition of terms and concepts, and provision of an overview for interactions between CSNs and CSCs and CSPs;

— description of types of CSN interactions;

— description of interactions between CSNs and CSCs;

— description of interactions between CSNs and CSPs;

— description of elements of CSAs and Cloud SLAs for CSN interactions, both with CSPs and with 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 17789, *Information technology — Cloud computing — Reference architecture*

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, ISO/IEC 17789, ISO/IEC 19086-1, and the following 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/

3.1
audit
systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the *audit criteria* (3.2) are fulfilled

Note 1 to entry: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself.

Note 2 to entry: External audits include those generally called second and third party audits. Second party audits are conducted by parties with an interest in the organization, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing organizations, such as those providing certification/registration of conformity or governmental agencies.

[SOURCE: ISO 19011:2018, 3.1]

3.2
audit criteria
set of requirements used as a reference against which objective evidence is compared

Note 1 to entry: If the audit criteria are legal (including statutory or regulatory) requirements, the words "compliance" or "non-compliance" are often used in an audit finding (3.3).

Note 2 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, etc.

[SOURCE: ISO 19011:2018, 3.7]

4 Symbols and abbreviated terms

CCRA	cloud computing reference architecture
Cloud SLA	cloud service level agreement
CSA	cloud service agreement
CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
IaaS	infrastructure as a service
PaaS	platform as a service
PII	personally identifiable information
SaaS	software as a service
SLA	service level agreement
SLO	service level objective
SQO	service qualitative objective

5 Structure of this document

In supporting the scope presented in Clause 1, this document is faithful to the existing descriptions of roles and sub-roles as presented in ISO/IEC 17789:2014, 7.2.2 and cloud computing activities in ISO/IEC 17789:2014, 7.2.1. This document explains the relationship between cloud service partners (CSNs), specifically cloud service brokers, cloud service developers and cloud auditors, and other cloud service roles:

Clause 6 – presents the challenges of managing risks relating to roles and activities in cloud services.

Clause 7 – provides an overview of the roles, sub-roles, and responsibilities of cloud service partners and provide the essential connection to the reference material in ISO/IEC 17789.

Clause 8 – building on Clause 7 and the exemplary scenarios in Clause 10, this clause discusses an overview and description of the types of interactions between cloud service partners (CSNs) and CSPs, CSCs and other CSNs.

Clause 9 – provides guidance on the use and tailoring of cloud service level agreements (cloud SLAs) and other agreements with the understanding of the roles, sub-roles and activities of CSNs in relation to the use of cloud services.

Clause 10 – presents examples that involve CSCs, CSPs, CSNs and demonstrates how different sub-roles can share the cloud computing activities associated with a given role as described in ISO/IEC 17789:2014, 7.2.2.

Clause 11 – presents issues relating the roles, activities and responsibilities.

Clause 12 – identifies existing relevant standards.

6 Relationship of roles and activities, and managing risks in cloud services

6.1 Overview

Cloud computing embraces different cloud service categories, cloud deployment models, cloud capabilities types, and cloud computing cross cutting aspects. To this end, roles and activities are critical contributors, and it is often necessary to differentiate requirements and issues for certain parties (see ISO/IEC 17021-1).

The cloud computing roles and their associated activities and components are defined in ISO/IEC 17788 and ISO/IEC 17789 (CCRA). One of the goals of ISO/IEC 17789, as specified in Clause 6, is "*to specify basic cloud computing activities and functional components, and describe their relationships to each other and to the environment*." For example, a cloud service broker is a sub-role of a cloud service partner (CSN) as defined in ISO/IEC 17788 and ISO/IEC 17789. These standards make it clear that a CSN does not provide cloud services. On the other hand, an inter-cloud provider is a sub-role of a CSP that can and does provide cloud services.

Note that ISO/IEC 17788 and ISO/IEC 17789 do not claim to describe all possible sub-roles of CSN, and initially identified the three sub-roles a cloud service broker, cloud service developer and cloud auditor. This document extends the ISO/IEC 17789 description of CSNs based on a survey of recent developments in cloud computing.

The CSP's role and all its sub-roles when providing cloud services to a CSC are not only just delivering cloud services but are also carrying out all activities necessary to safeguard its delivery and maintenance of those cloud services. ISO/IEC 27017 provides guidelines for the provision and use of cloud services specifically for CSPs and CSCs. ISO/IEC 27036-4 addresses relationships of CSPs and CSCs with suppliers of cloud service products[1].

In a cloud computing environment, CSC data is stored, transmitted and processed by one or more cloud services. A CSC's business processes depend upon the information security of those cloud services. Without sufficient control over the cloud services, the CSC might need to take extra precautions with its information security practices.

It is necessary for a CSC or any potential user to be concerned about protecting their data and to have an appreciation of both the benefits and risks of cloud computing. It would be prudent to have requirements for higher assurance for data security and privacy regardless of whether they are accessing cloud services from a CSP or are working with a CSN. The roles and related activities in handling CSC's data when delivering cloud services should be understood by all parties to ensure appropriate precautions and safeguards are in place. When using the service of a CSN, it is pertinent to have some form of

1) ISO/IEC 17789:2014, 3.2.2 cloud service product: A cloud service, allied to the set of business terms under which the cloud service is offered. NOTE – Business terms can include pricing, rating and service levels.

agreement or understanding, to clarify data ownership, who has access to the data, and how data is being accessed and handled.

The role and responsibilities of PII processors for protection of personally identifiable information (PII) in public clouds are specified in ISO/IEC 27018. ISO/IEC 27018 also emphasizes the responsibilities of the CSP, especially for a public CSP who is processing PII for a CSC, and the contractual relationship between CSC and CSP. To articulate consistently how data is to be collected and used, the taxonomy and structured data use statements defined in ISO/IEC 19944 are recommended.

When a potential user or CSC uses direct or indirect contact to search for cloud service products to meet its mission, the CSC will find offerings from businesses of various sizes with different cloud deployment models, cloud services, and different cloud capabilities types, such as IaaS, PaaS and SaaS. The quandary is in determining the providers of the services and their roles in delivering the services, and the roles and activities of those involved in delivering and using the cloud services.

Following this thought, interactions between CSNs specifically cloud service brokers, cloud service developers and cloud auditors are the focus of the discussion in this document. Interactions in the delivery and use of cloud services are related activities initiated by one party that influence responsive activities from another party or parties. The fluidity of the cloud marketplace embraces the flexibility of all parties and different sub-roles to play multiple and interchanging roles in delivering and using cloud services.

6.2 Scope in relation to the cloud computing reference architecture (ISO/IEC 17789)

The focus of this document is on roles and related activities, and specifically interactions between cloud service partners (CSNs) such as cloud service brokers, cloud service developers and cloud auditors, with other cloud service roles and their related activities. ISO/IEC 17789 (cloud computing reference architectural /CCRA) covers roles and activities through the lens of the reference architecture user and functional views. The functional view includes a layering framework that makes up the user layer, access layer, service layer and resource layer as described in ISO/IEC 17789:2014, 9.1.1. The CCRA also includes cross cutting aspects, layering framework and operational support systems components and components relating to the user and functional views. The approach of this document is not to redefine roles, sub-roles and activities as laid out in ISO/IEC 17789, but it is important to emphasize that roles can change through interaction of stakeholders during the use of cloud services, and that it may be possible to expand on these roles and sub-roles in the future. While this document will align closely to the roles and activities described ISO/IEC 17789, it is not necessary to include all components from ISO/IEC 17789 to support the scope of this document.

7 Overview of roles, sub-roles, and responsibilities of cloud service partners (CSNs)

7.1 Relationship between roles, activities and responsibilities

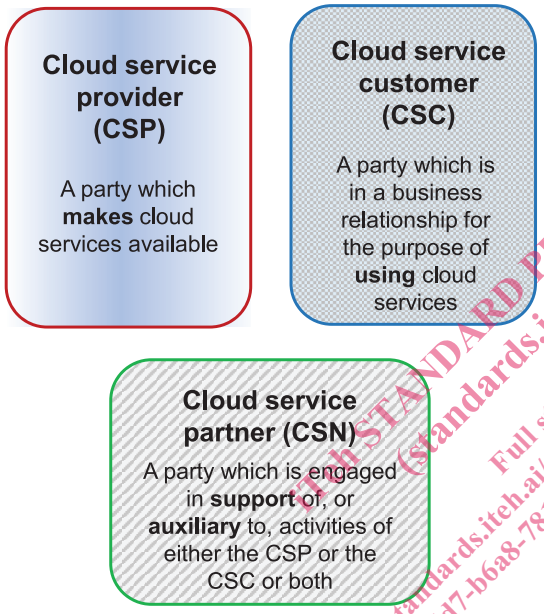
As the use of cloud computing increases, the cloud service products evolve and adapt to meet the demand. Technological development is evolving, and cloud computing is becoming part of the solutions for the Internet of Things (IoT), edge computing, and artificial intelligence (see ISO/IEC 23167 and ISO/IEC 23188). To meet the changing environment and increasing demands, the roles, responsibilities and activities in providing cloud services need to be re-examined in relation to the technological development and growing adoption of cloud computing.

The diversity of different cloud service offerings is accelerating the need for additional standards. Some roles and the associated responsibilities described in existing standards need to be further expanded for the spectrum of offerings as discussed in Clause 12. A party is not defined by a set of activities, and at any time, can assume more than one role and can take on a specific subset of activities of that role. Understanding the roles and associated activities for the use of cloud computing is necessary for clarifying gaps in responsibility, specifically for security, privacy and the key characteristics described in ISO/IEC 17788, when building applicable agreements including cloud service level agreements (see 9.2).

7.2 Roles and sub-roles

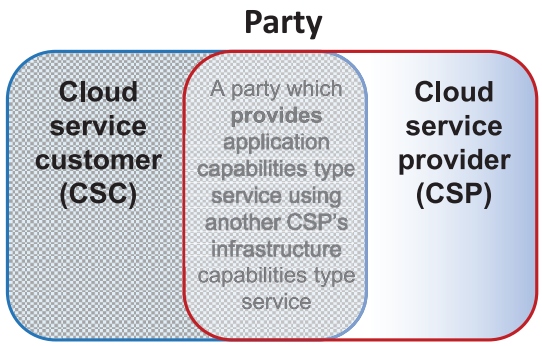
This document focuses on the same three cloud computing roles as in ISO/IEC 17789 but examines the evolving relationship and sub-roles of these roles as they interact in a cloud service environment. ISO/IEC 17789 specifies the basic cloud computing activities to establish the requirements of "what" cloud services provide. A role is defined by a set of cloud computing activities but some of the activities with one role can be shared or performed by other roles to facilitate and enable the delivery and use of cloud services (see ISO/IEC 17789:2014, 7.2.2).

From selection through eventual uses of a cloud service there are many components, such as the cross-cutting aspects, that require coordination across roles and need to be implemented consistently in a cloud computing system. A clear understanding of roles and the representative sets of cloud computing activities is necessary to avoid any misunderstanding of responsibilities and to facilitate a mutual agreement for the use of cloud services.



Within the context of cloud computing, it is necessary to differentiate among the requirements and issues for certain parties ISO/IEC 17788. These parties are entities that play roles (and sub-roles). A role is a set of cloud computing activities that serve a common purpose. The three roles identified in ISO/IEC 17789 are cloud service provider (CSP), cloud service customer (CSC) and cloud service partner (CSN), as described in Figure 1. A sub-role is a subset of the cloud computing activities for a given role. Different sub-roles can share the cloud computing activities associated with a given role. A party can play more than one role at any given point in time and can only engage in a specific subset of activities of that role.

Figure 1 — Common roles of cloud computing



A party can play more than one role. For example, a CSP can provide an application capabilities type service to CSCs using the infrastructure capabilities type service from another CSP. In this scenario, as shown in Figure 2, this party is performing the roles of CSP and CSC, and its responsibilities change depending on its engagement.

NOTE ISO/IEC 27017 provides guidelines for the implementation of information security controls based on the roles and responsibilities of CSPs and CSCs. A clear definition of roles and responsibilities supports the segregation of duties in the cloud environment and establishes the applicable security controls to address cloud-specific information security threats and risks considerations.

Figure 2 — A party can play more than one role

7.3 Cloud service provider (CSP)

A CSP is specifically responsible for making cloud services available. The role of providing cloud services focuses on the activities necessary to ensure services are delivered to the intended CSC or CSU. Some of the necessary activities are identified in ISO/IEC 17789 for the various CSP sub-roles.

The CSP can supply its cloud service products in co-operation with one or more CSNs who are responsible for different aspects such as control, security and configuration of the cloud services.

7.4 Cloud service customer (CSC) and Cloud service user (CSU)

7.4.1 Cloud service customer (CSC)

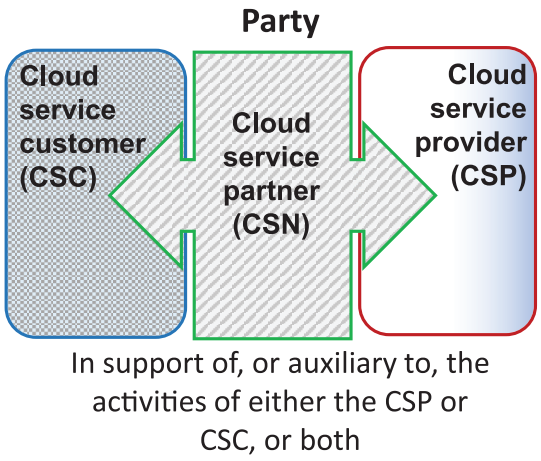
The CSC is a party which is in a business relationship for the purpose of using cloud services. For the activities of using cloud services, a CSC can be an individual person, a person using multiple different CSCs and even as one of the tenants sharing access to a set of cloud physical and virtual resources. The CSC may acquire cloud services directly from one or more CSPs or through a CSN. In addition, the CSC may choose to engage another party to be responsible for the cloud services and for a variety of activities relating to cloud service usage. In doing so, the CSC allows this party to assume many of the CSC's sub-roles and associated activities.

7.4.2 Cloud service user (CSU)

The cloud service user (CSU) is defined in ISO/IEC 17788:2014, 3.2.17, as a natural person, or entity acting on their behalf, associated with a cloud service customer (CSC) that uses cloud services. A CSU is also recognized as a tenant sharing access to a set of physical and virtual resources of a CSC's cloud service. A CSC may have many different CSUs using the cloud services to which it has access. The CSU is not described as one of the three main cloud computing roles in either ISO/IEC 17788 or ISO/IEC 17789. A CSU is associated to the CSC for the use of cloud services and is likely to have some form of permission or authorization with the CSC governing the CSU's use of the cloud services the CSC is accessing.

7.5 Cloud service partner (CSN)

7.5.1 Overview



A CSN is recognized as a party which is engaged in support of, or auxiliary to, the activities of either the CSP or CSC, or both. It may be true that CSNs are not providing cloud services. However, in recognizing that any party can play more than one role at any given point and different sub-roles can share the cloud computing activities associated with a given role, CSNs can perform various activities needed in support of CSCs and CSUs in their usage of cloud services. In their interaction with CSCs and CSPs, the sub-roles of CSNs are changing, and many activities and functions morph smoothly with those of the CSCs and CSPs in responding to the support needed. A CSN might perform various cloud computing activities depending on the types of partnership and their relationship with the CSP and the CSC, as shown in Figure 3.

Figure 3 — Cloud Service Partner (CSN)

