TECHNICAL REPORT

ISO/IEC TR 23187

First edition
2020-06

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

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
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) can 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.

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

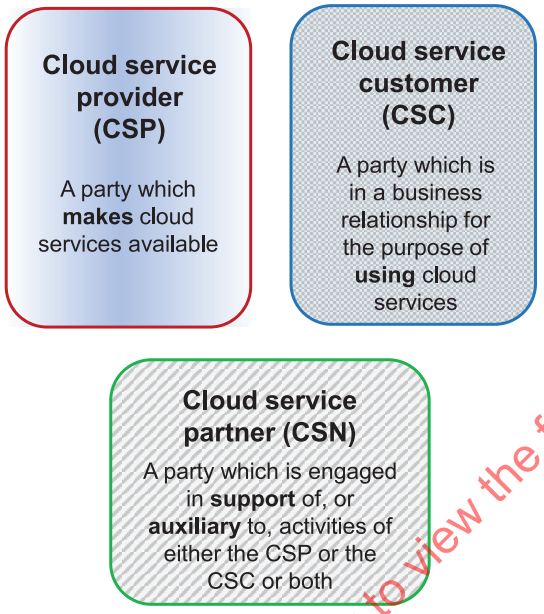
As the use of cloud computing increases, the cloud service products evolve and adapt to meet the demand. Technological development is evolving, and cloud computing is becoming part of the solutions for the Internet of Things (IoT), edge computing, and artificial intelligence (see ISO/IEC 23167 and ISO/IEC 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

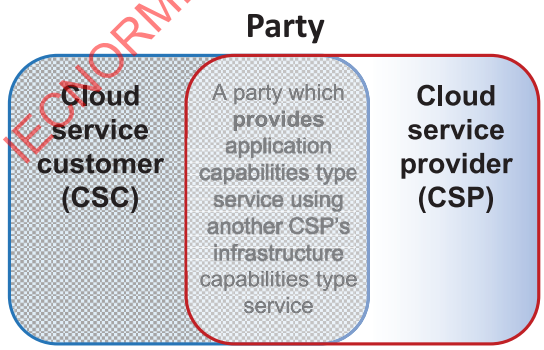
This document focuses on the same three cloud computing roles as in ISO/IEC 17789 but examines the evolving relationship and sub-roles of these roles as they interact in a cloud service environment. ISO/IEC 17789 specifies the basic cloud computing activities to establish the requirements of "what" cloud 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 described as a set of cloud computing activities performed by a party 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)

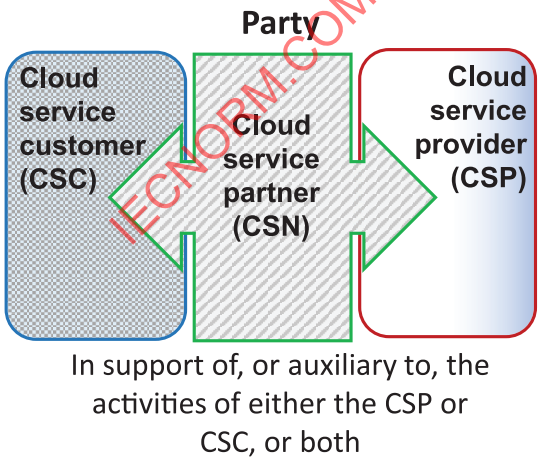
The CSC is a party which is in a business relationship for the purpose of using cloud services. For the activities of using cloud services, a CSC can be an individual person, a person using multiple different CSPs and even as one of the tenants sharing access to a set of cloud physical and virtual resources. 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)

The CSPs work with various partners to serve CSCs and to expand more offerings to meet the needs and demands of their CSCs. The CSNs, in partnering with CSPs, are not constrained to prescribed activities and can respond by assuming activities that are otherwise described for sub-roles of CSCs and CSPs in ISO/IEC 17789. Consequently, to strategically expand a customer base, the CSPs empower CSNs to expand their activities to include providing customized services such as localization, while not providing a comprehensive cloud service.

Some cloud services utilize third-party cloud services to augment functionality and the flow of data. The roles and responsibilities of CSNs might need to go beyond a supporting role to CSPs and CSCs. Defining roles and responsibilities that CSNs can perform will not only help to establish the appropriate components in the agreements, but most importantly, determine the security safeguards.

Depending on the type of partnership with CSP and CSC, the CSN can perform one or more sub-roles, including cloud auditor, cloud service broker and cloud service developer.

7.5.2 Cloud auditor

The cloud auditor is responsible for conducting an independent audit of the provision and use of cloud services as defined in ISO/IEC 17789:2014, 8.4.1.2. A cloud audit typically covers operations, performance, privacy impact and security and examines whether a specified set of audit criteria (see definition below – ISO 19011:2018, 3.7) are met.

The cloud auditor is a sub-role of the CSN and performs the following cloud computing activities:

— Perform audit (ISO/IEC 17789:2014, 8.4.2.4)

  The audit objectives, specifications, policies and agreement can be established in the cloud service agreement, which is addressed in Clause 9 of this document.

— Report audit results (ISO/IEC 17789:2014, 8.4.2.5)

  In this document, two types of cloud auditor are considered;

  1) External cloud auditor

     An organization commissioned by an independent accreditation body (e.g. a government) conducts audits from the perspective of a third party. The external cloud auditor can also be called “Third-party cloud auditor” (see Table 1).

     For example, in order to ensure cloud services procured by a government meet their control measures, there are three main entities for consideration: (1) the government as the CSC using cloud services; (2) the CSP which provides the cloud services; and (3) the external cloud auditor that audits the cloud services provided by the CSP and used by the CSC. The government needs to specify a set of control measures required by the government based on their level of acceptable risk, and the CSP is required to meet the specified set of control measures. The role of the external cloud auditor is to confirm that the CSP's individual control measures meet the control criteria properly.

     In another case the cloud audit is performed by a partner that makes an alliance with a CSP for their business. The partner audits the cloud services to obtain the partner viewpoint. This can also be treated as an internal audit.

     For another case, multiple external cloud auditors can be auditing one cloud service simultaneously. The auditors will need to coordinate audits collaboratively while meeting independent Cloud SLAs made between the CSP and CSC.

     Some information, such as actual audit data shared between the external cloud auditor, CSC and CSP, may be confidential information belonging to the CSP. It may therefore be subject to a non-disclosure agreements (NDA) between the relevant parties.

  2) Internal cloud auditor

An internal audit as shown in Table 1 is referred to as a first party audit and can be conducted on the CSC's use of cloud services or on the CSP's anticipated cloud services. An internal auditor can be an "in-house cloud auditor" within an organization or contracted third party. A CSP:cloud service operations manager performing the sub-role as a cloud auditor (ISO/IEC 17789:2014, 8.3.1.1) provides audit data from an audit performed internally.

One of the important rationales for internal audits is to monitor the ongoing status of the results evaluated by external audits as the appropriate measures as necessary for the CSP to demonstrate continued compliance.

From the perspective of conformity assessment, the definition for audit as per ISO 19011 is provided in 3.1.

The internal cloud auditor should perform the audit as the first party audit, and the external cloud auditor should perform the audit as the second party audit and third party audit (see ISO 19011). While ISO 19011 concentrates on internal audits (first party) and audits conducted by organizations on their external providers and other external interested parties (second party), the document can also be useful for external audits conducted for purposes other than third party management system certification. As an additional reference, ISO/IEC 17021-1 provides requirements for auditing management systems for third party certification.

Table 1 lists the three types of audit as referenced in ISO 19011.

Table 1 — Different types of audits (see ISO 19011)

First party audit	Second party audit	Third party audit
Internal audit	External provider audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

Regardless of whether it is an internal or external audit, it is essential that the cloud auditor and the CSC have a mutual and clear understanding of the scope of the cloud computing environment, the CSPs and potential outsourcing partnership, and any third-party providers. Many audit standards exist within ISO and external to ISO. The objectives and scope for the audits, identify the key roles and sub-roles to be considered and included as part of the audit. ISO/IEC 27007 provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. The audit is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

Depending on the objectives and scope of the cloud computing audit, the cloud auditor interacts with CSP, CSC, and CSN, i.e. the cloud service broker and cloud service developer, to produce the appropriate audit results. For example, a cloud auditor may need to audit the service after the cloud service developer has completed the test(s).

7.5.3 Cloud service broker

The cloud service broker negotiates business relationships between CSCs and CSPs as defined in ISO/IEC 17789:2014, 8.4.1.3. Unlike the inter-cloud provider (CSP's sub-role [ISO/IEC 17789:2014, 8.3.1.6]), the cloud service broker is not involved in providing the cloud service and is not itself a CSP. The party assuming the sub-role of cloud service broker could operate independently or also assume the sub-role by combining its activities with the CSP:inter-cloud provider and performing activities of peering, intermediation, aggregation and managing peer cloud service (see 7.6).

The cloud computing activities of a cloud service broker include:

— acquire and assess customers (ISO/IEC 17789:2014, 8.4.2.6);

— assess marketplace (ISO/IEC 17789:2014, 8.4.2.7);

— set up legal agreement (ISO/IEC 17789:2014, 8.4.2.8).

A cloud service broker could set up a business solution to connect CSU or CSC to one or more CSPs as shown in the scenarios in Clause 10. The CSCs could be in contact with a CSN offering cloud service solutions that include offerings of cloud service products on behalf of CSPs. The marketplace assessment can occur prior to CSU or CSC acquisition, allowing the creation of pre-agreements with CSPs. This enables CSCs to select CSPs from a service catalogue, possibly negotiating service details (e.g., service level objectives) at selection time.

The cloud service broker, acting as the intermediary between the CSC and the CSP, may expand its activities and offerings to help CSCs with understanding the complexity of cloud service offerings and to create added value for the cloud services. A cloud service broker may also be in the position to negotiate contracts with the CSP on behalf of the CSC. Whether in support of the CSC or the CSP, the cloud service broker only acts during the contracting phase of the service. The cloud service broker is not involved during the consumption of the service. In such cases, the activities involved are the CSP's activities.

7.5.4 Cloud service developer

A cloud service developer is responsible for designing, developing, testing and maintaining the implementation of a cloud service as defined in ISO/IEC 17789:2014, 8.4.1.1. The cloud service developer hands over the created package to the CSP's cloud service manager to perform the deploy services activity, resulting in the service being made available for use by CSCs.

The cloud service developer's cloud computing activities include:

— design, create and maintain cloud service components (ISO/IEC 17789:2014, 8.4.2.1);

— compose services (ISO/IEC 17789:2014, 8.4.2.2);

— test services (ISO/IEC 17789:2014, 8.4.2.3).

A cloud service developer collaborates with a CSP or a CSC, and sometimes also with a cloud service integrator or cloud service component developer. The role, activities and responsibilities of the cloud service developer are versatile and fluid when interacting with a CSC, a CSP and other CSNs.

There are various models for a CSN developing and deploying code artefacts for use as (or within) a cloud service. For example, consider a scenario wherein the CSP contacted a CSN:cloud service developer to create and package service implementations and hand them to the CSP for deployment and operation. The cloud service developer interacts with the CSP to:

— inspect the CSP's environment for service execution;

— test service implementations;

— hand over the service implementation packages.

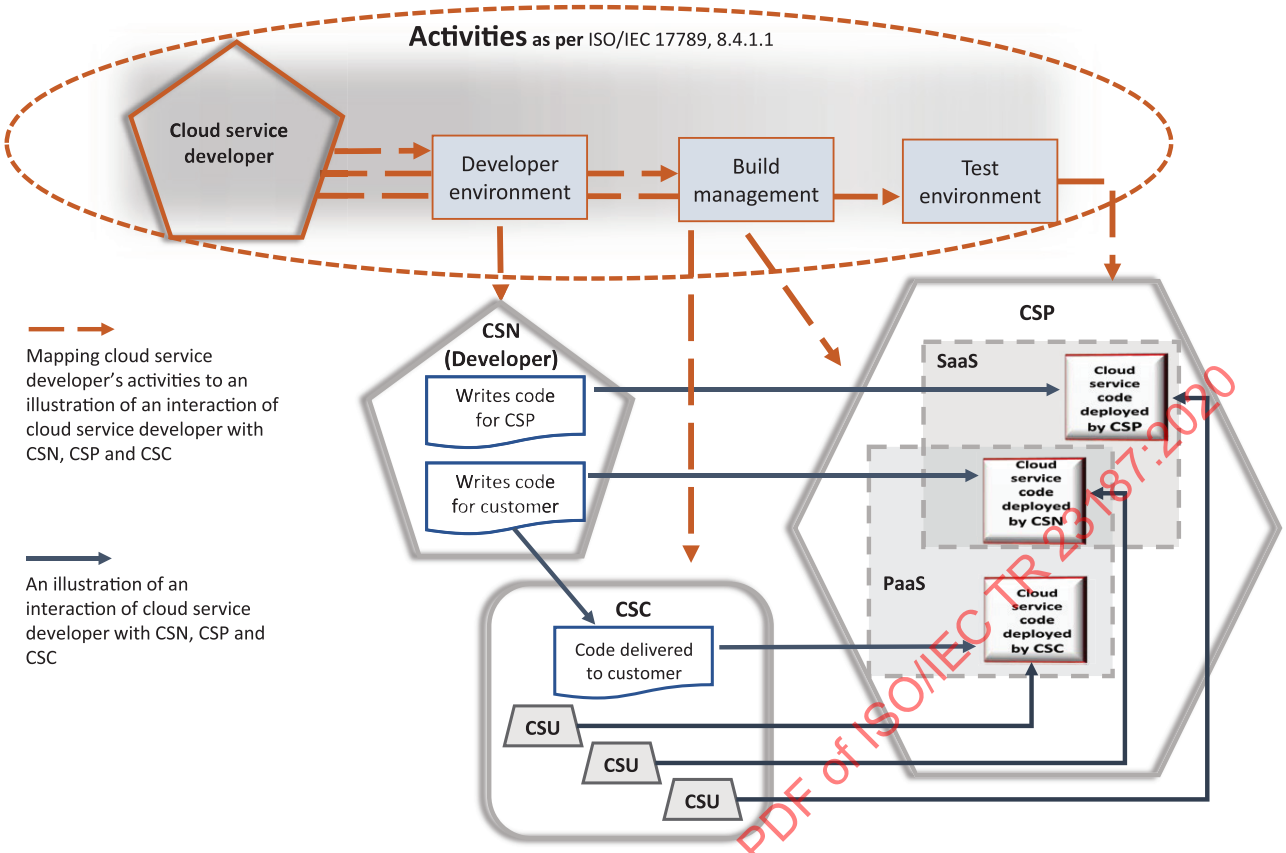


Figure 4 — Example - Interaction of cloud service developer with CSCs and CSPs

Figure 4 provides an example of an illustration of the CSN:cloud service developer interaction with the CSP, CSC and CSN with a mapping of the activities as per ISO/IEC 17789:2014, 8.4.1.1.

For example:

— The CSP can obtain code directly from the CSN:cloud service developer for implementation within their cloud service. The interaction is between the CSN and CSP without any involvement from the CSC, and this would generally be regarded as an "application capabilities type" cloud service such as SaaS.

— The CSN can provide code to the CSP on behalf of a CSC, such as where the CSC has purchased a package independently, and the CSN is responsible for the deployment. The resulting cloud services to the CSC are either a "SaaS" or "PaaS" service, depending on other characteristics.

— The CSN can provide code to the CSC, and the CSN takes responsibility for integrating with other code developed in-house or by another developer before deploying it to the CSP. A cloud service that supports this is usually referred to as a "PaaS". A cloud service integrator (ISO/IEC 17789:2014, 8.2.1.4) can be used for the integration of cloud services such as with the CSC's existing ICT systems, including application functions and data.

In each case, the code artefacts will go through phases of design, development, testing, deployment, operation, maintenance, and eventual retirement that will not be further discussed here. However, it is important to realize that the relationship with the CSN rarely ends with deployment. For some general information about the cloud service code lifecycle, see Recommendation ITU-T Y.3522.

7.6 Relationships between CSNs, and other roles and sub-roles

7.6.1 Differences between CSNs, CSCs and CSPs

In support of the CSPs and CSCs, the CSN's cloud computing activities position the CSNs to be involved in wide variety of activities without providing the cloud services. The CSN can either assume or share certain activities with either CSC or CSP. For example, the CSN can serve as the CSC:cloud service administrator and the CSP:cloud service business manager to support the CSC and CSP.

Therefore, cloud computing activities of sub-roles are not necessarily exclusively associated with a given role. The CSNs, in assisting their potential customers of cloud service in securing appropriate adoption of cloud computing, are responsible for initiating and dealing with the business relationship and not as a traditional channel between CSPs (specifically CSP:cloud service business manager) and CSCs. In their service offering to assist CSCs in finding CSPs, CSNs use the criteria provided by the CSCs to make appropriate determination and metrics for identifying the desired cloud services. The information gathering is associated with the activities of CSP:cloud service deployment manager (ISO/IEC 17789:2014, 8.3.1.2).

A party can play one or more roles, i.e. a party can perform the role of CSN and CSP. A party can be a CSN in support of either the CSC or CSP, and the party can carry out activities of either a CSP to a CSC or CSC using a service supplied by a CSP. The responsibilities are specifically related the cloud computing activities of the roles and sub-roles.

7.6.2 CSNs and inter-cloud providers

The inter-cloud provider described in ISO/IEC 17789:2014, 8.3.1.6 is a sub-role of the CSP. The CSP and its sub-roles define the cloud computing activities necessary for providing a cloud service and the cloud computing activities necessary for ensuring its delivery to the CSC. The activities of an inter-cloud provider concentrate on using and managing the cloud services of a peer cloud service provider.

The cloud service broker, a sub-role of the CSN, is engaged in activities to support the CSC, CSP or both, and not in providing services, which are the activities of the inter-cloud provider. This distinction is particularly important for CSCs to have appropriate contractual agreements for handling the relationship between a CSN and an inter-cloud provider.

Any sub-roles of CSN can have an agreement with a CSP or CSPs to offer not only solutions but cloud service products. The agreement may involve a cloud service broker to collaborate with CSPs and will have help from the CSP:inter-cloud provider. If a CSN, e.g. cloud service broker, has an agreement with a CSP to represent and offer cloud service products, this CSN might then assume some of the activities in collaboration with a CSP in providing cloud services to the CSC. The roles and responsibilities should be transparent to all parties and clearly defined in the appropriate agreement with the CSNs and CSCs.

8 Overview and description of types and interactions between cloud service partners (CSNs) with CSPs, CSCs, and CSNs

8.1 General

With the increasing adoption of cloud services, the market reaction is to provide a larger quantity and range of service offerings. The CSPs are working with various market players to serve CSCs and to expand more offerings to meet CSCs' needs. As the apprehension surrounding cloud computing gradually dissolves into confidence, CSCs seeking to design and adopt solutions that fit their needs can choose to use multiple CSPs and multi-cloud scenarios.

The core of cloud computing is distributed services and their delivery. All cloud computing related activities can be categorized into:

— activities that use services,

— activities that provide services, and

— activities that support services.

This document focuses on "what" cloud services provide and not on how to design cloud-based solutions and implementations. On that path, cloud computing activities are required to support a purpose to deliver one or more outcomes. A set of cloud computing activities that serve a common purpose is only a generic representation of a role, not a definitive one.

8.2 Interaction between CSNs and CSCs

8.2.1 Overview

A CSC interaction with a CSP is a business relationship for using cloud services. Furthermore, ISO/IEC 17789 also specifies that a CSC has a business relationship with a CSN or CSNs for a variety of purposes. As the cloud computing landscape evolves, CSPs in collaboration with CSNs in the marketplace have either shared or allowed CSNs to assume some activities to initiate cloud services, e.g. a CSN designing the design template with the CSP's service catalogue. This collaboration allows CSPs to expand their customer base and to provide an avenue for more users to CSPs' excess or unused resources from their existing capacity of cloud services. This can offer competitive cost incentives to CSCs or users of small and medium size businesses and offers the flexibility to combine different cloud services from different providers to meet their needs.

There are myriad different solutions when implementing cloud computing to meet business needs and addressing required security and privacy controls that are offered for a diverse combination of costs. A simple online platform set up by a CSN connects a CSC with a selected cloud service serviced by various CSPs. Apart from hosting the online service, the entity/organization has limited involvement in providing cloud services. The services offered could be a simple, basic use of data storage, email, and office applications. The CSC can expand its appetite for cloud service for more applications, storage or interconnecting to other services and another cloud. The expanded needs might involve the help of other CSNs, for example, a cloud service developer or cloud service broker. CSCs may also interact with other CSNs in using cloud services that are not directly involved with implementing, building and providing cloud services, such as a CSN providing consulting services to CSCs in advising strategic planning for cloud computing. Apart from the activity of using cloud services, cloud computing activities that ISO/IEC 17789 defines as being related to the sub-roles of a CSC can be activities performed by the sub-roles of CSNs as supported by the scenarios described in Clause 10.

8.2.2 CSN managing CSC's cloud adoption

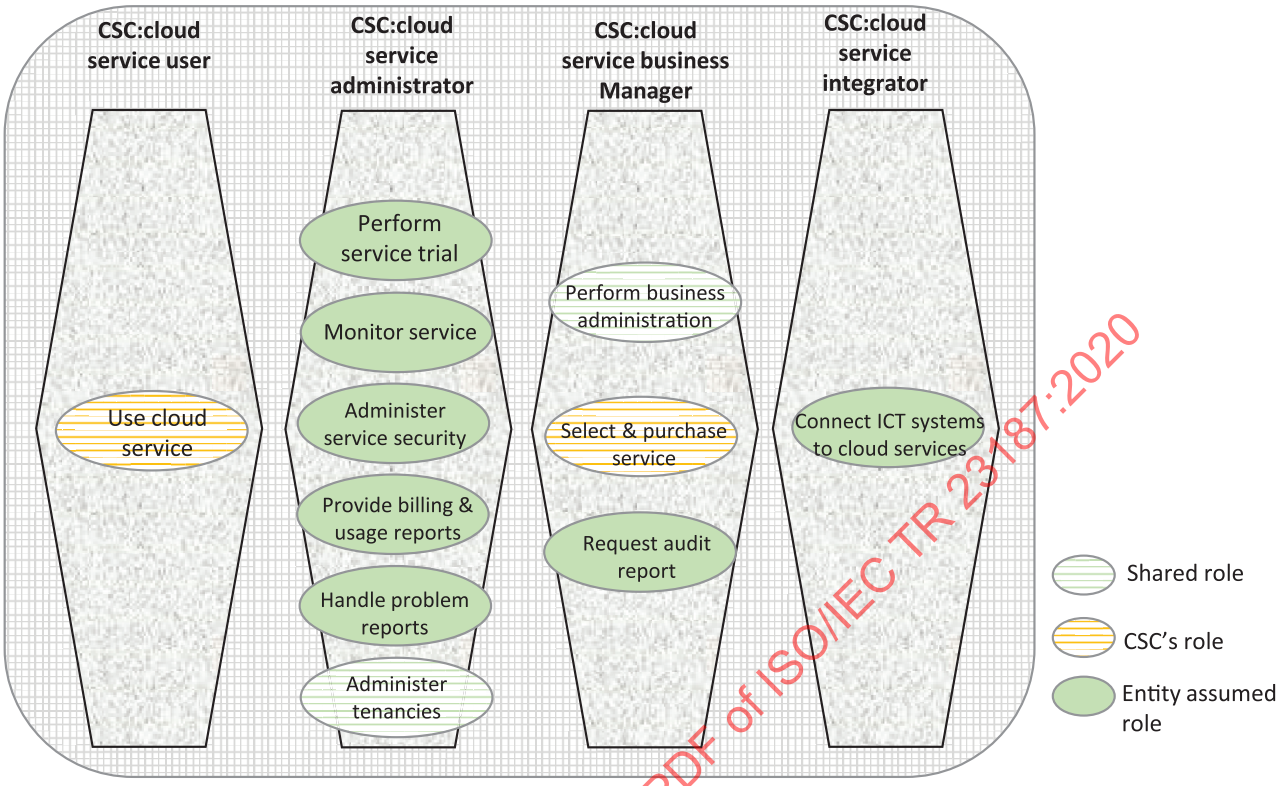


Figure 5 — CSN as manager of CSC's cloud

Upon selecting and contracting a cloud service, the CSC might consider engaging a CSN, such as a cloud service developer, to bridge possible gaps between the CSC's information security requirements and the information security capabilities offered by the service. A CSC can engage a CSN to manage part or entire use of the cloud service. Alternatively, the CSC might outsource the process beginning from selection through to adoption, implementation and management of the cloud computing. In establishing this relationship, the CSN assumes or shares the CSC's responsibilities and activities for the CSC use of cloud services. In the second example, the CSN might assume the role of CSP or joint CSP in providing the cloud service. In another example, the CSC might extend the CSN's management of the CSC's cloud to include managing multiple or federated clouds. Depending on the service engagement on the extent of services agreed between CSC, CSP, and CSN, the CSN could either share the activities with the CSC (see keys in Figure 5) or be completely responsible for the activities for the CSC's consumption of cloud services.

8.3 Interaction between CSNs and CSPs

The CSNs' interaction with CSPs, based on ISO/IEC 17789, is likely be described in these examples:

a) Between cloud service broker and cloud service business manager:

- Manage business plan (ISO/IEC 17789:2014, 8.3.2.11);
- Manage customer relationships (ISO/IEC 17789:2014, 8.3.2.12);
- Manage financial processing (ISO/IEC 17789:2014, 8.3.2.13).

b) Between cloud service developer and cloud service manager:

- Provide services (ISO/IEC 17789:2014, 8.3.2.8);
- Deploy and provision services (ISO/IEC 17789:2014, 8.3.2.9);

— Perform service level management, with cloud service security and risk manager (ISO/IEC 17789:2014, 8.3.2.10);

— Manage security and risks (ISO/IEC 17789:2014, 8.3.2.17).

c) Between CSN and inter-cloud provider:

— Manage peer cloud services (ISO/IEC 17789:2014, 8.3.2.15);

— Perform peering, federation, intermediation, aggregation and arbitrage (ISO/IEC 17789:2014, 8.3.2.16).

d) Between cloud auditor and operation manager

— Provide audit data (ISO/IEC 17789:2014, 8.3.2.4)

The cloud auditor requests audit evidence from the CSP through the administration access functional component of the CSP, invoking the necessary administration capabilities (ISO/IEC 17789:2014, Figure 10-2).

A CSN/organization with an agreement with a CSP to build solutions on top of CSP's cloud service products can assume the role and sub-roles of CSP as the CSP to its CSCs.

8.4 Interaction between CSNs and other CSNs

8.4.1 Description of types of CSNs interactions

All CSNs can be in business independent of the other. Each role may also interact with the other in the cloud marketplace in meeting the needs of their customers. For example, a cloud service developer and cloud service broker collaborate to design cloud services or draft a roadmap for CSCs (ISO/IEC 17789:2014, 8.3.2.2 [compose services] and 8.3.2.3 [test services]), or a cloud service broker negotiates a relationship with other CSNs and CSPs to offer cloud services to CSCs and CSPs. Multiple cloud auditors may interact in performing audits on multiple different geolocations or where important functions are outsourced and managed under leadership of different organizations (ISO 19011).

8.4.2 CSN – interaction and responsibilities

The document established in subclause 7.2 the importance of differentiating among the requirements and issues for certain parties. This is to enable the definition of the perimeter of responsibility and accountability within the context of cloud computing. The CSN is defined not as a provider of cloud services, but as a party which is engaged in support of, or auxiliary to, the activities of either the CSP or CSC, or both ISO/IEC 17788. In presenting the examples in Clause 10, this document also presents the CSNs in their interaction with CSCs and CSPs assuming activities as previously designed for CSCs and CSPs, i.e., the CSNs are performing additional roles and activities to their supportive activities to CSCs and CSPs. In performing more than one role at a time, the CSN, in supporting either the CSC or the CSP, can assume different roles and activities and thereby offer products and provide cloud services to another party. Figure 5 demonstrates the need to align accountabilities and have appropriate agreements for activities performed by various actors. This is particularly essential for recognizing and accounting for responsibilities associated with security and privacy in the cloud computing environment.

9 Elements of cloud service agreements (CSAs) relating to CSN interactions

9.1 General principles

A CSC will have some form of an agreement with the CSP for the purchase and use of cloud service. ISO/IEC 19086-1:2016, Clause 6, refers to this agreement as a Cloud service agreement (CSA). A CSA has one or more parts that are formulated in one or more documents. The agreement includes information security arrangements. A service level agreement (SLA) might include availability,

reliability, performance, security, data protection, compliance and data handling. The cloud service level agreement (cloud SLA) is among those common parts of CSAs. It should account for the key characteristics of cloud computing with metrics expressed as cloud service level objectives (SLOs) and service qualitative objectives (SQOs). The scope of this clause is limited to cloud SLAs.

Generally, the traditional use of a cloud service begins between the CSC and CSP. The journey begins when a cloud service is selected, and as the prescribed sub-roles of the CSC (see ISO/IEC 17788) intend to explain how the CSP manages the use of the cloud service to meet its requirements. The CSP should provide the information and technical support necessary for meeting the CSC's requirements, which could be used to craft a cloud SLA. For certain arrangements, for example, the CSC purchases from a cloud service reselling CSN (see 10.2), a standardized service level agreement (SLA) covering the pre-determined information security controls is provided by the CSP. The CSC may need to work with the CSP for customizing the SLA and/or to implement additional controls of its own to mitigate risks.

NOTE The ISO/IEC 19086 series describes various standardized elements of an SLA which can be used as appropriate.

As adoption of cloud computing continues to increase, in meeting the customers' demand of various sizes in transitioning from disparate systems to the cloud, many businesses often collaborate with third parties. Many CSPs increasingly out-source components including critical functions to third parties to offer a comprehensive and competitive package to their customers. These business collaborations are not always transparent or known to the CSPs' customers. Without visibility into who is performing those critical functions or the establishment of cloud SLA for all parties, a risk assessment remains incomplete and CSCs, particularly for small and medium size businesses, are subjected to potential and possibly serious security risks.

Cascading relationships for CSNs and other roles and sub-roles add to the complexity for negotiation and monitoring of SLAs. As an example, one cloud service developer may use many other cloud service developer services (including open source), all of which impacts the SLA offered to the CSC. The cloud service broker and cloud auditor need to be aware of such cascading SLAs complexities and the other contractual elements.

9.2 Role, relationship and agreement

9.2.1 Overview

Traditionally, when a CSC or potential user contacts a CSP with the intent of using a cloud service, the parties will likely be communicating throughout the development, testing and eventual usage of cloud services. The service level agreement (SLA) will be between the CSC and CSP (see ISO/IEC 19086-1:2016, 9.5). The CSP and all of its sub-roles focus on the cloud computing activities necessary for providing a cloud service and the cloud computing activities necessary for ensuring its delivery to the CSC. The CSC could negotiate to use a cloud service through a CSN such as a reselling package (10.2) as illustrated in Figure 6. The contract agreement for the use of the cloud service with all the components therein is made between the CSN and CSC or CSU.

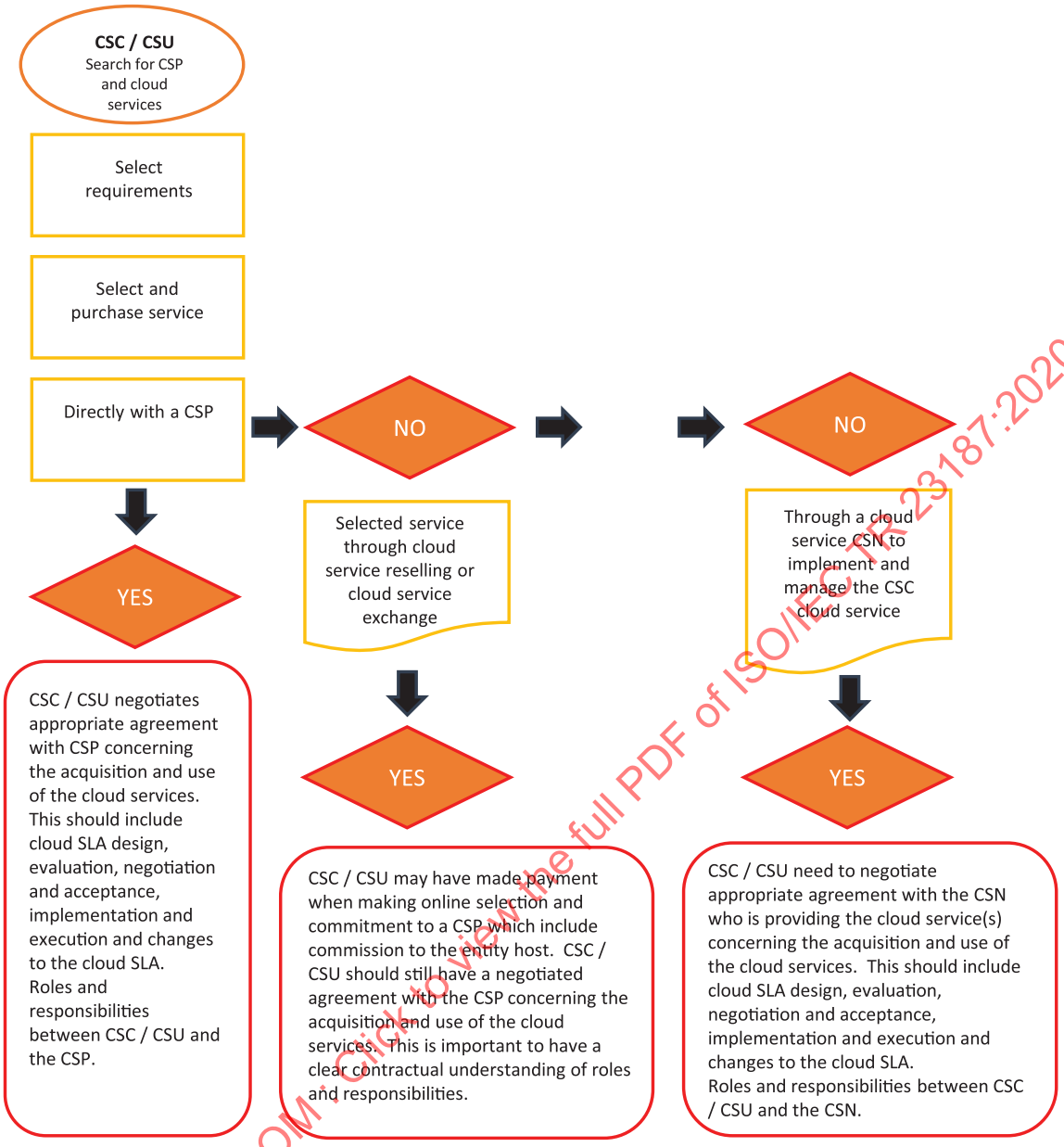


Figure 6 — Scenarios and SLAs

In the event where two or more CSPs are involved in the delivery of one or more cloud services to a CSC, the CSC would have set up an agreement with each CSP on the services and products. In the layout of a hierarchical inter-cloud, a single CSP provides a service that is composed of resources from a hierarchy of secondary CSPs, and the CSC can have an SLA directly with the primary CSP defining a standard set of cloud service level objectives (SLOs) and cloud service qualitative objectives (SQOs) that will apply to all cloud services. CSCs and CSPs could be interacting with one or more CSNs, such as in the setting of shared services management (10.6) and cloud data management service (10.5). This requires multiple SLAs with various roles.

When a CSC or potential user engages a CSN through a public website in planning for the adoption of cloud computing, whereby the services offered can be simply described and accompanied by friendly check boxes for the selection of options, there is limitation for the CSC or potential user to request detailed specifications and requirements. The CSPs could have included a blanket or basic agreement among the selection check boxes that the potential CSC or user would have easily overlooked.

9.2.2 Cloud migrations and cloud deployment models

Whether an individual or an organization is planning to use cloud services for the first time or planning on expanding their use of cloud services, it is worthwhile including a plan on managing and moving data as part of the broader mission strategy. Depending on needs and requirements, cloud migrations may extend from moving an entire IT infrastructure to a CSP to adopting a hybrid cloud model combining with on-premises data centres. A CSU or CSC may be collaborating with more than one CSP and CSN. A CSP delivers cloud services according to firm SLAs or CSAs supporting a clear description of roles, activities and responsibilities that is crucial not just for mission success, but also for maximizing value out of the data and cloud capabilities. The ISO/IEC 38505 series can help with this process.

A potential user or CSC is confronted with an array of service offerings – cloud and cloud related services. In determining what is best suited to meet the business mission, the user or CSC should consider if the service constitutes a cloud service and if it meets the needs of the CSC and aligns with the capabilities of the covered services. For guidance on definition and concepts of cloud computing, see ISO/IEC 17788. ISO/IEC 17789, and ISO/IEC 22123. CSCs should ensure that cloud SLAs and other governing documents align with their business cases and overall strategy ISO/IEC 17789.

ISO/IEC 27036-4:2016, Figure 1, and reproduced in Figure 7, uses the comparison of the acquisition process between the public cloud deployment model and ICT outsourcing as an initial example to illustrate the differences in the acquisition process for various deployment models and cloud service solutions designed by providers. This is applicable to scenarios such as cloud service exchange. The implementation and agreement for the use of the cloud services differs among cloud service models and cloud capabilities types.

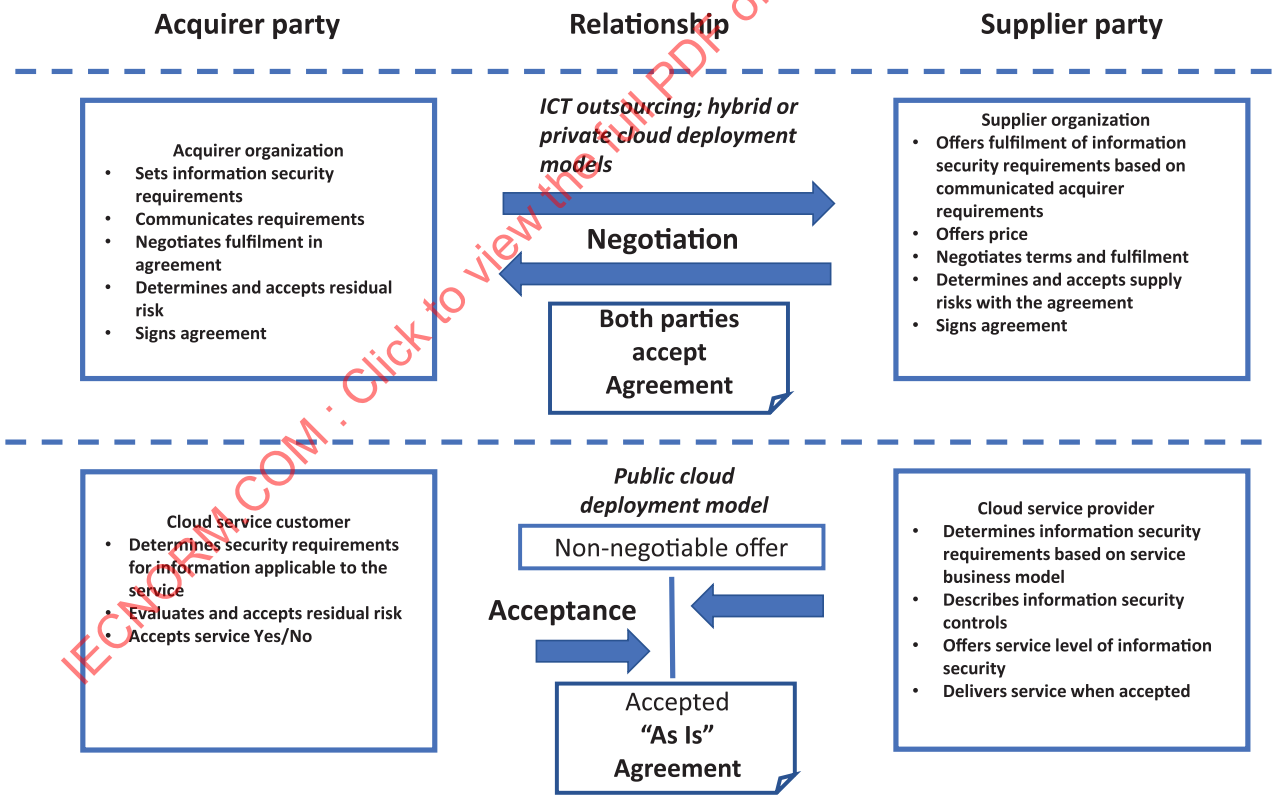


Figure 7 — Differences and similarities between ICT outsourcing and public cloud deployment models

9.3 Cloud service level agreement (Cloud SLA)

9.3.1 Overview

A cloud service agreement (CSA) is a documented agreement between the CSP and CSC that governs the covered services. A CSA can consist of one or more parts recorded in one or more documents and a cloud SLA will be one of those parts. The ISO/IEC 19086 series provides pertinent details on service level agreements for cloud computing. The definition provided in ISO/IEC 17788:2014, 3.1.7 includes a note stating that "an SLA can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier." The parts of the ISO/IEC 19086 series can be found in the Bibliography, [3] - [5].

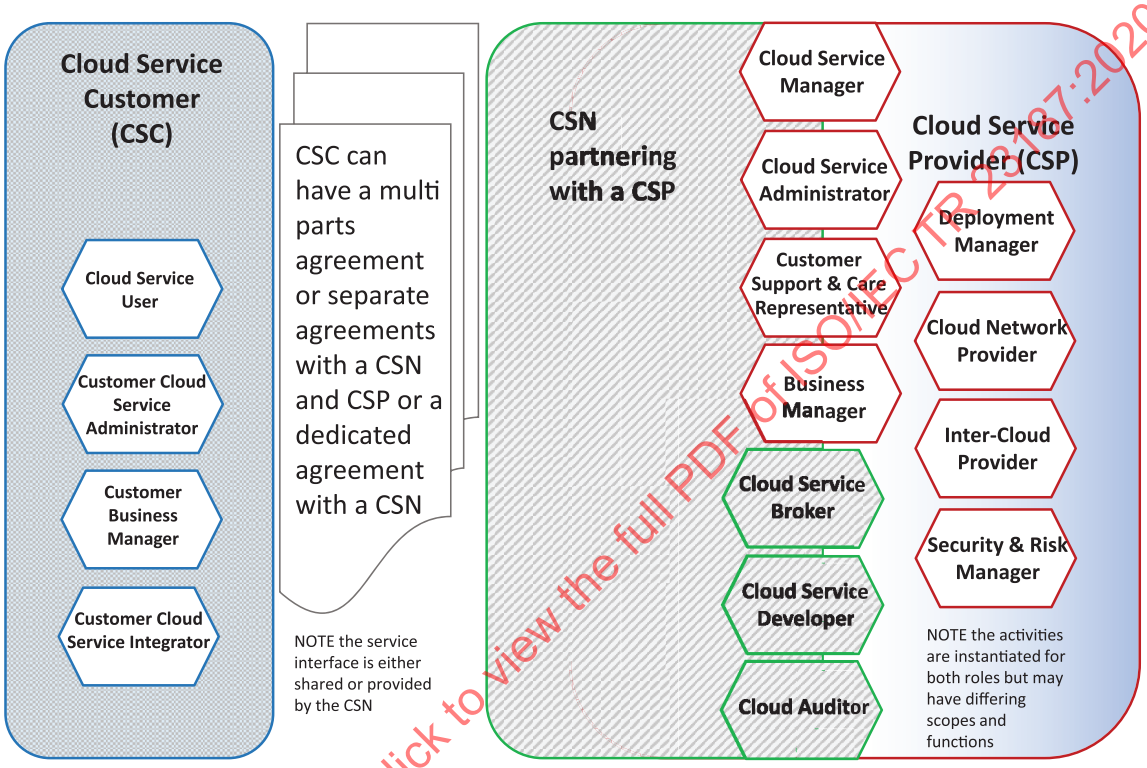


Figure 8 — CSC using a managed service

A CSC should have an SLA with the provider of covered cloud services and should have a separate agreement with the CSN that administers and supports the delivery of the cloud services. For example, Figure 8 describes the separate agreements necessary when using a managed cloud service partnered with a CSP (see 10.4 and Figure 12). A potential user signing up for a basic cloud service, for example, through a cloud exchange (see 10.3), should have a predetermined agreement/SLA simply by clicking a check box on a webpage or by registering for the cloud service. A predetermined standardized SLA will have limited flexibility for any potential user to negotiate for specificities. It is still a primary objective to read the fine print and discuss clarifications on the cloud offerings with the provider to meet the CSC's expectations, which in the long run may help to contain any increase in costs and align compliance with regulations and requirements.

9.3.2 SLA terminology

The cloud SLA should account for the key characteristics of cloud computing as described in ISO/IEC 17788:2014, 6.2. Deploying a cloud service begins with the CSC specifying their requirements for a cloud service. This understanding will then be used to build the cloud SLA components and defined concepts with the CSP(s).

9.3.3 Roles and responsibilities

9.3.3.1 General

The roles and responsibilities component in a cloud SLA includes a description of the roles and responsibilities for all roles. Defining the roles and responsibilities for the parties involved in cloud computing is an important foundation for describing the activities that are required. The activities define the role and thereby also the responsibilities. For example, a CSC engaging a CSN through a cloud service reselling platform (see 10.2) can negotiate a cloud SLA once it is established that this party agrees to perform some of the CSP sub-roles. A basic cloud SLA can generally be found on the webpage of an online cloud service offering such as cloud service reselling package or cloud service exchange.

9.3.3.2 CSCs interacting with CSNs

The CSCs logically use cloud service products from CSPs, and CSNs work and interact with CSPs as illustrated in ISO/IEC 17789:2014, 10.2.2. The cloud service brokers do not provide cloud services but can have a business relationship with CSPs to support the provision of cloud services. In this endeavour, the CSN:cloud service broker may work with cloud service developers and interact with CSCs as demonstrated in Clause 8.

In many cases when the initial contact for use of a cloud service begins with an engagement with a CSN and not directly with a CSP, the CSC should determine the provider or 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. The CSCs need to have a clear understanding of the party or parties supplying the services during the acquisition process. A clear delineation of roles and responsibilities should be discussed and included in any agreement that covers pertinent security policy to cloud services.

9.3.3.3 CSPs interacting with CSNs

A CSP may incorporate third party cloud services to enhance their offering or to customize the cloud service to meet a CSC's specific requirements. From an auditing perspective, transparency is desirable, but such information may not be readily available. The cloud service governance component described in ISO/IEC 19086-1:2016, 10.9, discusses the importance of adhering to certain industry regulations and involves the description of CSPs, CSCs and other roles, e.g. security, data protection, financial and healthcare regulations for data.

A typical illustration of cloud computing activities involving CSP and sub-roles interacting with CSC and CSN is provided ISO/IEC 17789:2014, 10.2.2, Figure 10-1 and Figure 10-2. This document illustrates that parties in a cloud computing system can assume any one role and carry out a specific set of activities that are not necessarily of that role (see Figure 2).

The following examples of interaction between CSN:sub-roles with CSPs are extracted from ISO/IEC 17789:

— CSN:Cloud auditor interacting with CSP (ISO/IEC 17789:2014, A.4);

— CSN:Cloud service developer interacting with CSP (ISO/IEC 17789:2014, A.3 and Figure A.7).

10 Examples of scenarios illustrating CSN activities

10.1 Introduction

This clause presents examplary scenarios to illustrate evolving roles and activities in the marketplace and highlight potential issues. These examples are included as a means for illustration and discussion, and they are by no means conclusive as factors such as the deployment models, business practices, sectors and locations result in many different scenarios. Many publications including those listed in the Bibliography on cloud computing are directed at interaction between CSPs and CSCs, as explained in Clause 11. The examples help to expand the focus on the interaction between CSPs, CSCs, and CSNs.

The definition of cloud computing includes many key characteristics and is eloquently expressed in ISO/IEC 22678:2019, 6.2.1, as "*ICT resources can be accessed almost as simply as pressing a switch to turn on a light – and can be released almost as simply as pressing the switch again to turn the light off.*" The journey to use cloud computing has different paths to implementing cloud computing and it is much more complex than pressing the switch. As the cloud computing definition also describes cloud service categories, cloud deployment models, cloud capabilities types, cloud computing cross cutting aspects, and finally, cloud computing roles and activities, a CSC is to determine which of those cloud computing components to tailor the solutions to meet the CSC's mission, values, and the time to delivery. This CSC is further challenged by the creative offerings in the marketplace. In seeking to expand their offerings to provide more solutions to customers, the CSPs partner with other parties to find more customers directly and indirectly. Potential CSCs can find adoption, implementation and maintenance of cloud challenging and decide to outsource those activities to another CSN.

10.2 Reselling of cloud service

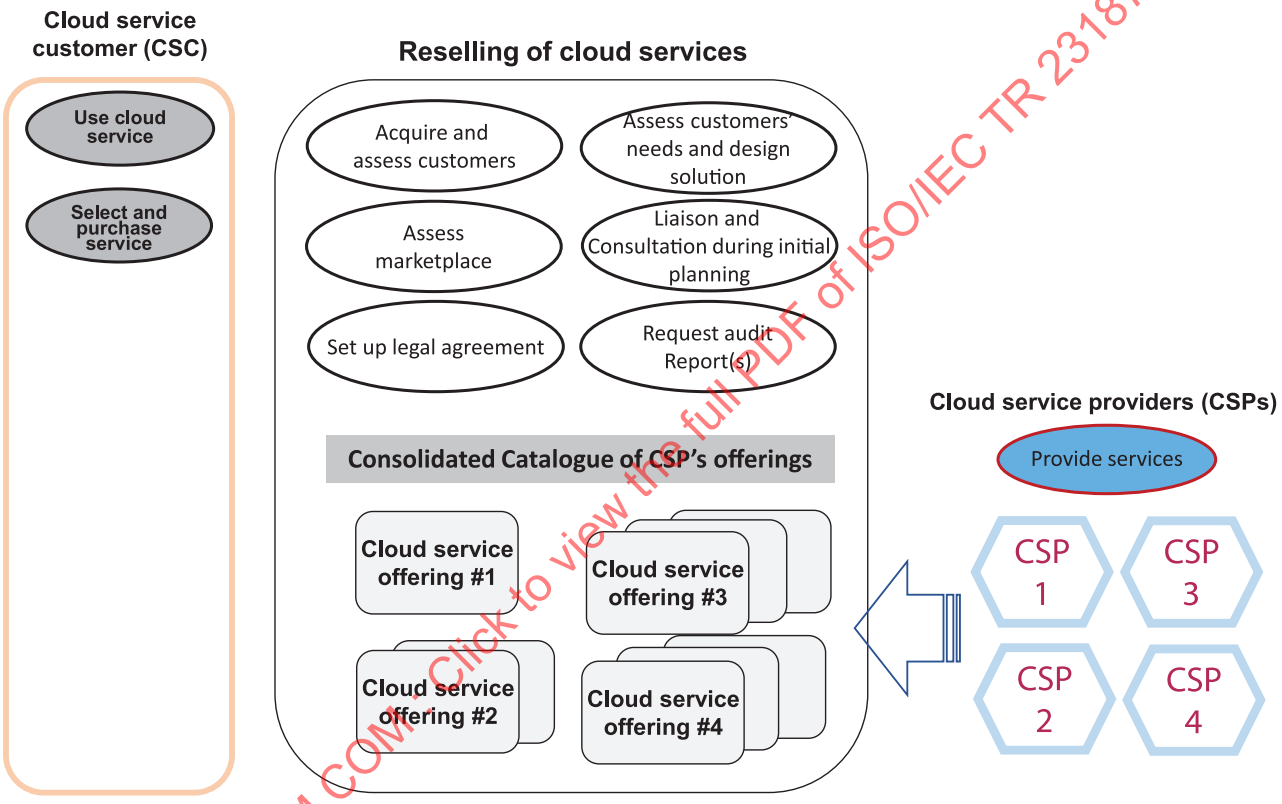


Figure 9 — Reselling of cloud service

Figure 9 describes an example where a party that is reselling cloud services may simply be a conduit to the CSP to satisfy contractual or policy requirements. Businesses that are reselling cloud services often also offer other value-added capabilities, which could include almost anything from technical brokering, development and even auditing. It is the CSCs responsibility to understand specifically what is required and what added value the reseller business is offering. This scenario illustration highlights a subset of the activities that could be performed under the title of "reseller". The CSN integrates solutions while managing the deployment of multiple cloud service products purchased through multiple CSPs or other similar entities. The CSN partners with various CSPs and re-packages CSPs' offerings of cloud service products to resell them with customized solutions as its offerings to potential users. The services offered may range from an introduction of the CSP(s) to the CSC after matching the CSP's services based on the CSC's requirements, to a full range of activities in assisting CSCs to adopt cloud services. In some cases, the CSPs use the reseller to offer excess or unused resources from their existing capacity of cloud services.

The CSN will have an agreement with CSPs to represent and market the CSPs' products and services. Some of the CSPs may also train and certify the representatives from the CSN. The CSN:reseller offers a catalogue of many CSPs' offerings. In meeting CSC's needs, the CSN can also formulate solutions by combining products and services from one or more CSPs.

The CSN can engage other CSNs, such as a cloud auditor, cloud service broker, and cloud service developer to assist in implementing the cloud services. Table 2 includes some potential cloud computing activities of this CSN depending on the arrangement negotiated between the parties, i.e. CSC, CSP and CSN. By including the cross reference to the activities from ISO/IEC 17789, Table 2 provides examples of activities of the scenario, "reselling cloud services".

Table 2 — Example of activities of the scenario: reselling cloud services

Examples of the activities of a CSN engaged in reselling cloud services	Activities as described in ISO/IEC 17789:2014[a]	
Formulate solutions by offering products and services from one or more CSPs	8.4.2.6 8.4.2.7 8.4.2.8	Acquire and assess customers Assess marketplace Set up legal agreement
Assess customers' needs and requirements for cloud services	8.3.2.1	Assessing the impact of new service deployments or the increase in use of existing services
Request audit data from CSPs Provide audit data	8.2.2.10	Audit report(s)
Analyse CSCs' requirements Consult and liaise with CSPs to provide the appropriate cloud service products	8.3.2.5	Liaison and consultation between CSC and CSP(s) during initial planning
[a] The activities in this table are extracted from ISO/IEC 17789 as a mapping to illustrate the potential activities that a CSN engages in each example.		

10.3 Cloud service exchange

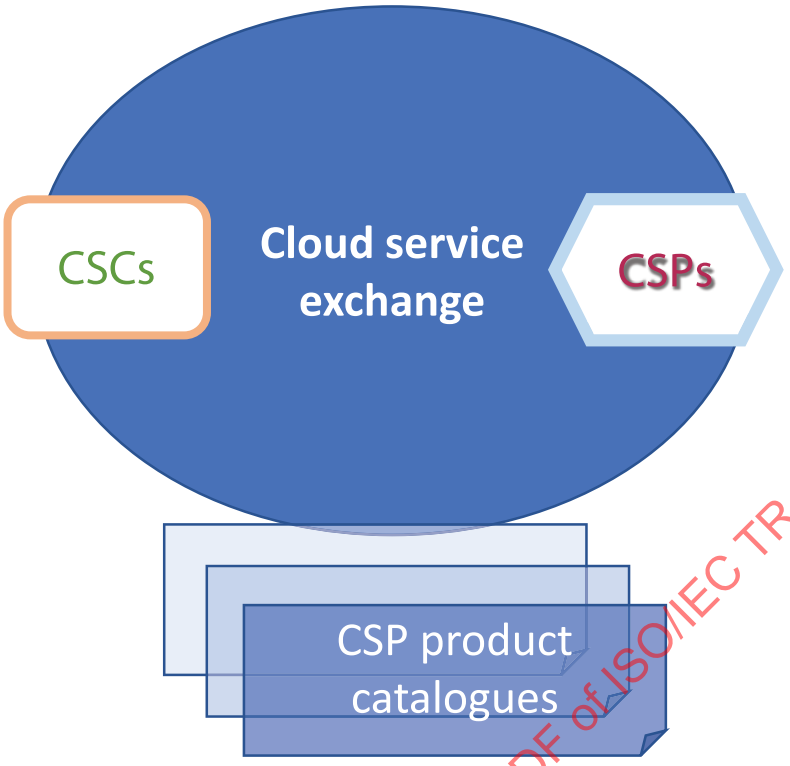


Figure 10 — Cloud service exchange

Figure 10 above describes a CSN operating a business as a cloud service exchange where any potential customers can search for cloud service products, provisions and request bids from a portfolio of CSPs that the exchange has established with the CSPs. The CSN business sets up a common website and profits from the monthly commission from successful cloud service contracts made through connections on the website.

An individual or organization interested in using the cloud service exchange can establish a business account with the cloud service exchange. The CSC specifies its requirements such as type, amount, location, storage capacity, and contract term to solicit the CSPs' bids. Any account holder can select with the option to purchase a basic cloud service. The potential user is at liberty to further negotiate directly with a CSP on customized or expanded services. The cloud exchange account holder can also request assistance from the exchange in certain parts of the process depending on the CSN's business model.

The CSPs, apart from listing the catalogues of products and services, also use the exchange as a channel to entertain bids for their excess capacity in the marketplace. This offers the potential users the opportunity to consider possible advantages from pricing and the flexibility to scale up or down as they need to. CSCs may also consider this as a solution for short-term projects, e.g. a research project with a time limit.

This example is a basic market concept that can be found in many countries. The business model, which is similar to the CSN reselling cloud service packages, is to serve as an interchange connection point for "buyers and sellers" of cloud services. While this same CSN may offer bonus services such as localization, customization of applications or options for expanding management of cloud service as part of securing a business connection, it is not responsible for network connectivity, security, and many other components of a cloud services. The exchange can continue to claim a channel fee as long as the CSC continues using the services from the CSP or CSPs; the CSCs are directed to channel any issues relating to the use of cloud services to the CSP's customer service.

This example can be attractive to private individuals, sole traders, or owners of small businesses seeking to adopt basic cloud services. Many customers of these exchanges may not fully comprehend the roles

and responsibilities to maintain the security, privacy, confidentiality and integrity necessary for using the service that they, the CSN and the CSPs play. The initial contact for any CSC is the online page, and for many CSCs, there is no or little interaction with a live person. The CSCs may overlook any display or hint of standard SLA offered by the CSPs. The cloud service exchange does not have a comprehensive or thorough set-up for CSCs and CSUs to establish an appropriate service level agreement (SLA) with their CSPs.

The exchange may be able to provide a source of information for potential users to research, define and design their strategy for adopting cloud computing. Many cloud computing activities of this CSN can be aligned to a cloud service broker (7.5.3). Table 3 provides an example of activities of the scenario, "cloud services exchange" with mapping to the sub-role from ISO/IEC 17789.

Table 3 — Example of activities of scenario: cloud services exchange

Examples of the activities of a CSN engaged in cloud services exchange	Activities as described in ISO/IEC 17789:2014[a]	
Assess customers' needs for cloud services Provide a source of information	8.4.2.7 8.4.2.6 8.4.2.8	Assess marketplace Acquire and assess customers Set up legal agreement
Request audit data from CSPs Provide audit data	8.3.2.4	Provide audit data
[a]The activities in this table are extracted from ISO/IEC 17789 as a mapping to illustrate the potential activities that a CSN engages in each example.		

10.4 Management of cloud service

10.4.1 CSN – CSC: Managing the CSC use of cloud service

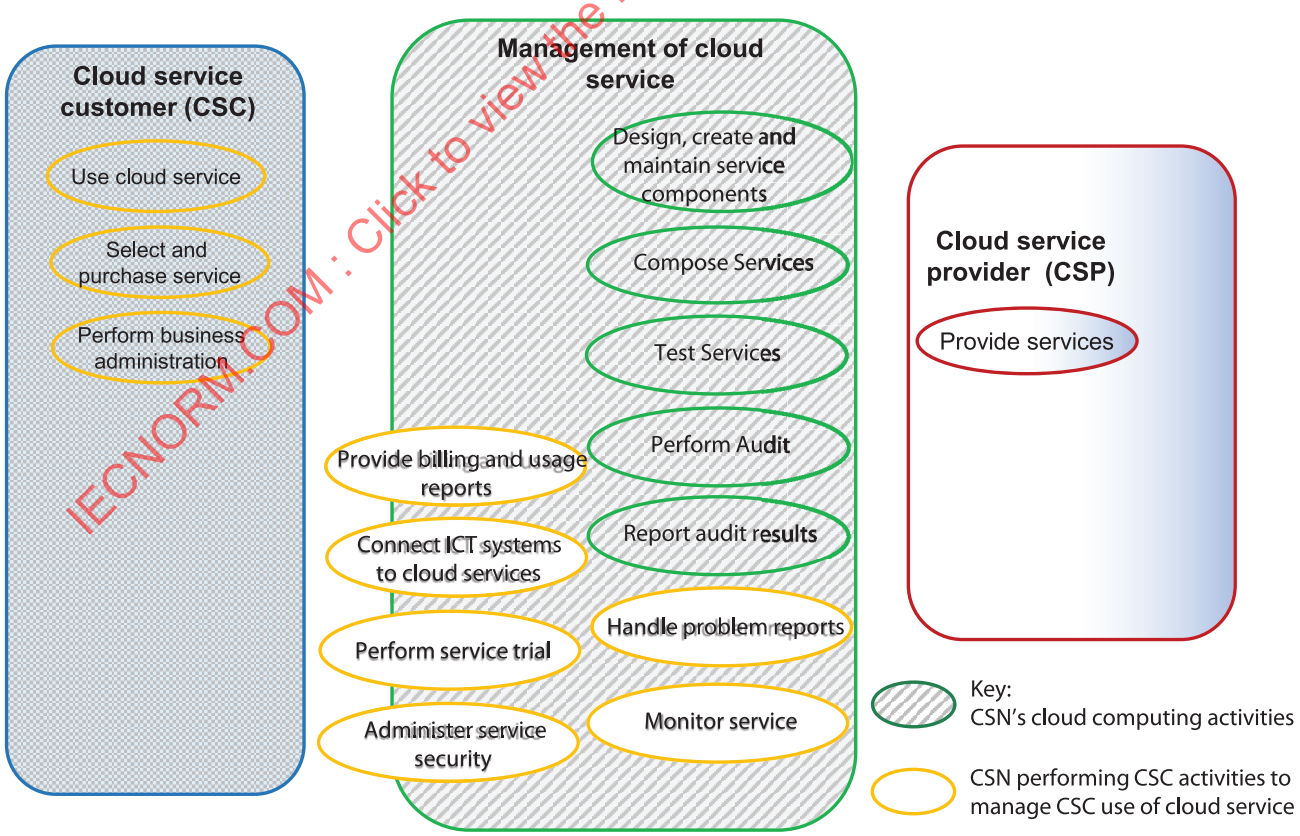


Figure 11 — Management of a cloud service

Figure 11 describes a CSN that is engaged in assisting the CSC directly or indirectly to manage the use of their cloud services. Alternatively, the CSC may engage the CSN to implement as well as to manage the cloud service. The CSC will then contract the CSN to manage the entire process of planning, implementing and managing any part of the cloud service. The scope of activities is dependent on the agreement between the CSC and CSP with this CSN, and whether the cloud service(s) are contracted directly with a CSP.

In some cases, the CSP has a business arrangement with the CSN that includes providing extensive training and allowing exclusive rights to the CSN to market and deliver the CSP's cloud service products (see 10.4.2). Based on the CSC's needs, the CSN designs a solution or solutions that can include one or more cloud services from one or more CSPs.

When the CSC engages the CSN to manage its cloud service, this is independent from the cloud service agreement between the CSC and CSP. The CSN will then assume many activities on behalf of the CSC with the CSP(s) to ensure cloud services are supplied to the CSC according to the cloud SLA made between CSC and CSP. Figure 11 shows the CSC owning those activities displayed within the boundaries of the CSC. As an illustration, it is suggested that the activities in between CSC and the CSN are either shared and the CSN is responsible for performing those activities on the right side of the CSN in Figure 11. Table 4 provides examples of activities of the scenario, "cloud service management" with mapping to the activities from ISO/IEC 17789.

Table 4 — Example of activities of scenario: management of cloud service

Example of the activities of a CSN engaged in management of a cloud services	Activities as described in ISO/IEC 17789:2014[a]	
Directly or indirectly manage the use of cloud services	8.2.2.2	Perform service trial
	8.2.2.3	Monitor service
	8.2.2.4	Administer service security
	8.2.2.5	Provide billing and usage reports
	8.2.2.6	Handle problem reports
Request audit data from CSPs Provide audit data	8.2.2.8	Perform business administration
	8.2.2.10	Request audit report(s)
	8.3.2.4	Provide audit data
	8.4.2.4	Perform audit
	8.4.2.5	Report audit results
Assist CSP to provide the cloud computing products to CSC	8.4.2.1	Design, create and maintain service components
	8.4.2.2	Compose services
	8.4.2.3	Test services
[a] The activities in this table extracted from ISO/IEC 17789 as a mapping to illustrate the potential activities that a CSN engages in each example.		

10.4.2 CSN – CSP: partnership with a CSP to deliver cloud service

Figure 12 includes an illustration of partnership between a CSN and a CSP whereby the CSP has an arrangement or agreement with a CSN to market and deploy the CSP's cloud service products to a CSC. The CSP works with the CSN in establishing itself as a certified representative of the CSP's cloud service products. The business arrangement may allow the CSN to assume the activities of some of the sub-roles of the CSP, as described in ISO/IEC 17789, as suggested for those sub-roles – cloud service manager, cloud service administrator, customer support and care representative and business manager. The CSN may engage a cloud service developer to develop the implementation and testing of the cloud services before deployment of the cloud service. The CSN, in serving as a partner of the CSP, performs the activities to assess the marketplace, acquire and assess customers, and set up legal agreement. The activities would include working with the cloud auditor to gather the necessary audit reports.

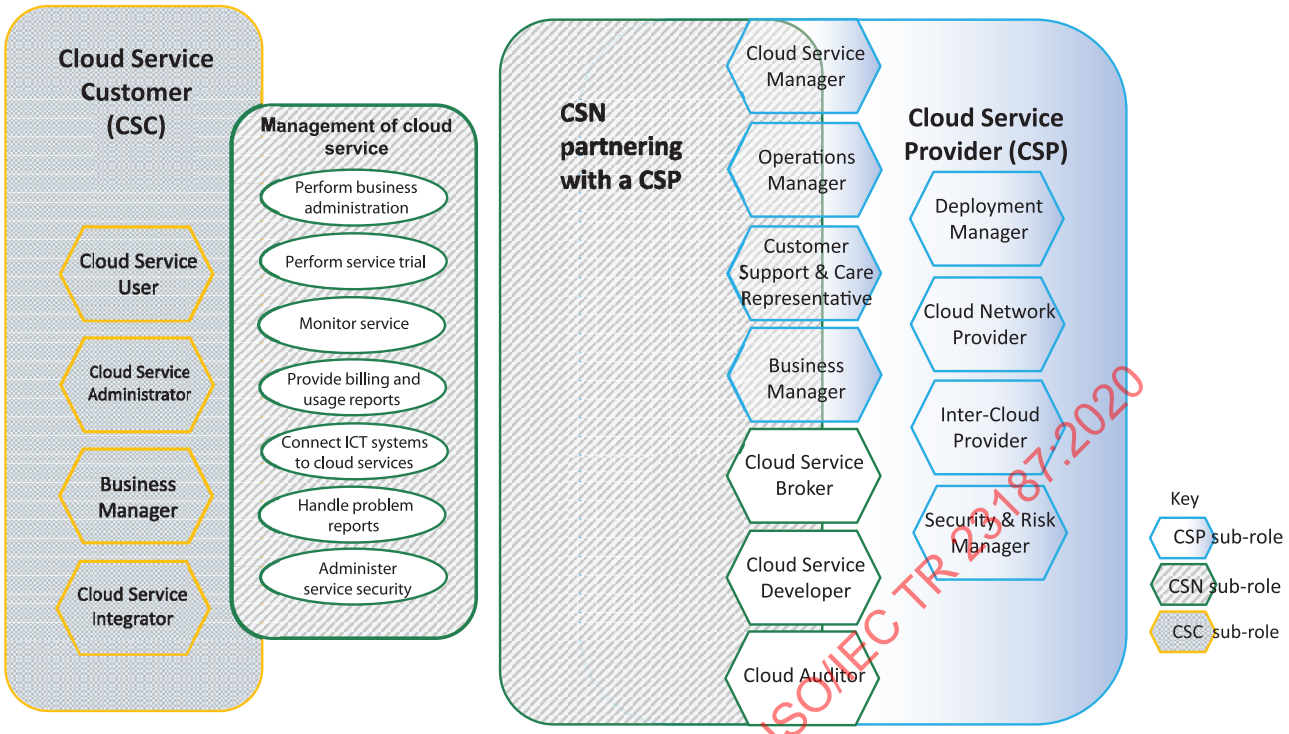


Figure 12 — Partnership between a CSN and a CSP

In this example, the CSC uses the cloud service as illustrated in the functional component relationship in ISO/IEC 17789:2014, Figure A.1. The CSN may assume the activities of the cloud service business manager as shown in ISO/IEC 17789:2014, Figure A.2. Table 5 provides examples of activities of the scenario, "partnership with a CSP" with mapping to the activities from ISO/IEC 17789.

Table 5 — Example of activities of scenario: partnership with a CSP

Example of the activities of a CSN engaged in a partnership with a CSP	Activities as described in ISO/IEC 17789:2014[a]	
Partnership with CSP to provide cloud computing products	8.3.2.8 8.3.2.9 8.3.2.10 8.3.1.2	Provide services; deployment and provision of services; perform service level management Liaison and consultation between CSC and CSP(s) during initial planning
Partnership with CSP to manage customers and customer relationships	8.4.2.6 8.4.2.7 8.4.2.8 8.3.2.1 8.3.2.12 8.3.2.14	Acquire and assess customers Assess marketplace Set up legal agreement Assess customers' needs and requirements for cloud services Manage customer relationships Handle customer requests

Table 5 *(continued)*

Example of the activities of a CSN engaged in a partnership with a CSP	Activities as described in ISO/IEC 17789:2014[a]	
Support CSP to deploy CSP's cloud service products depending on the scope of partnership agreement with the CSP	8.3.2.15	Manage peer cloud services
	8.3.2.17	Manage security and risks
	8.3.2.18	Design and implement service continuity
	8.3.2.19	Ensure compliance
	8.3.2.20	Provide network connectivity
	8.3.2.22	Provide network management services
	8.4.2.4	Perform audit
	8.4.2.5	Report audit results
	8.4.2.1	Design, create and maintain service components
	8.4.2.2	Compose services
	8.4.2.3	Test services
[a] The activities in this table are extracted from ISO/IEC 17789 as a mapping to illustrate the potential activities that a CSN engages in each example.		

10.5 Cloud data management service

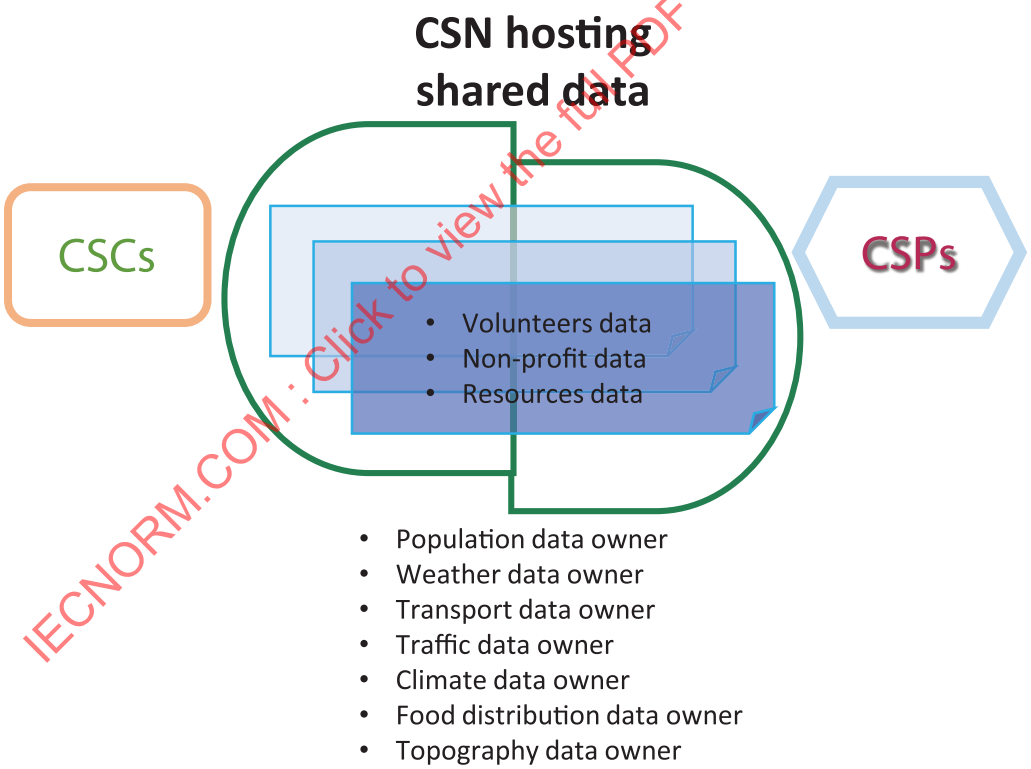


Figure 13 — Cloud data management

This example as described in Figure 13 presents a CSN as a host for gathering data from various data owners, e.g. emergency services and a restaurant reservation service. This situation involves two or more CSPs in the delivery of a cloud service to a CSC as well as the use of inter-cloud as described in ISO/IEC 17789. A CSN acts as a single point of access to the resources that can be gathered from a group of CSPs. All members can interact with the cloud service and access the resources. This CSN could perform the activities of both the CSC and the CSP as described in ISO/IEC 17789, as the administrator

and operation manager of the service. Table 6 provides examples of activities of the scenario, "cloud data management" with mapping to the activities from ISO/IEC 17789.

Table 6 — Example of activities of scenario: cloud data management

Example of the activities of a CSN engaged in cloud data management	Activities as described in ISO/IEC 17789:2014[a]	
Activities as the administrator and operation manager of the service	8.3.1.2	Liaison and consultation between CSC and CSP(s) during initial planning
	8.3.2.1	Assess customers' needs and requirements for cloud services
	8.3.2.14	Handle customer requests
	8.4.2.1	Design, create and maintain service components
	8.4.2.2	Compose services
	8.4.2.3	Test services
	8.2.1.2	Perform service trial, monitor service, administer service security, provide billing and usage reports, handle problem reports, administer tenancies
[a] The activities in this table are extracted from ISO/IEC 17789 as a mapping to illustrate the potential activities that a CSN engages in each example.		

10.6 Shared services management

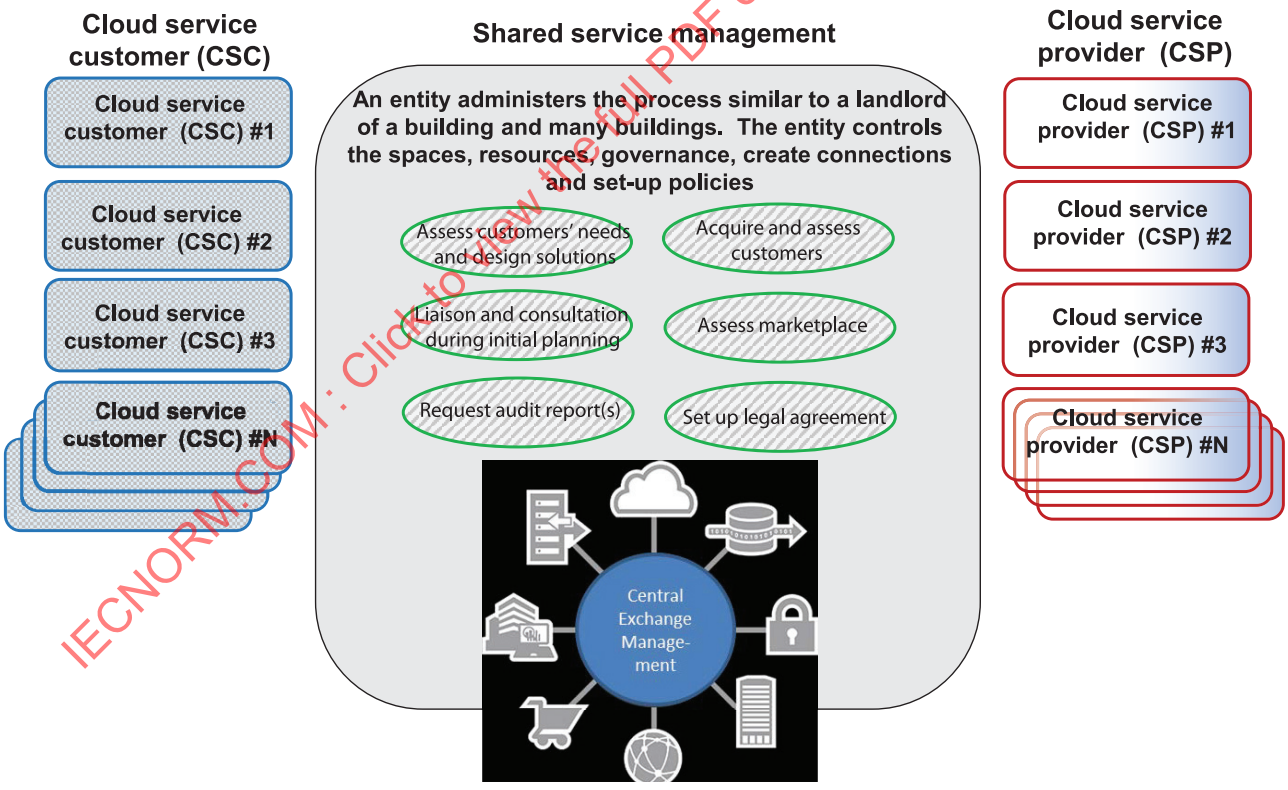


Figure 14 — Illustration of shared services management

The example is similar to tenants of a building that is managed by a landlord. The landlord is responsible for resources for the tenants to live within the building and connecting the tenants to services outside the building. The tenants can customize specific needs with the landlord, e.g. storage facility outside the building. To this end, the cloud SLA varies for every cloud service "tenant" with the "landlord." Table 7 provides a cross-reference to the activities and sub-role from ISO/IEC 17789.