BS ISO/IEC 17789:2014

BSI Standards Publication

Information technology — Cloud computing — Reference architecture

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 17789:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/38, Distributed application platforms and services (DAPS).

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 80196 9

ICS 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 17789:2014

BS ISO/IEC 17789:2014

INTERNATIONAL STANDARD

ISO/IEC 17789

First edition
2014-10-15

Information technology — Cloud computing — Reference architecture

Technologies de l'information — Informatique en nuage — Architecture de référence

Reference number
ISO/IEC 17789:2014(E)

© ISO/IEC 2014

Full document details: BS ISO/IEC 17789:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 17789:2014

CONTENTS

Page

1 Scope 1
2 Normative references 1
2.1 Identical Recommendations | International Standards 1
2.2 Additional references 1
3 Definitions 1
3.1 Terms defined elsewhere 1
3.2 Terms defined in this Recommendation | International Standard 1
4 Abbreviations 2
5 Conventions 2
6 Cloud computing reference architecture goals and objectives 3
7 Reference architecture concepts 4
7.1 CCRA architectural views 4
7.2 User view of cloud computing 5
7.3 Functional view of cloud computing 7
7.4 Relationship between the user view and the functional view 8
7.5 Relationship of the user view and functional view to cross-cutting aspects 8
7.6 Implementation view of cloud computing 9
7.7 Deployment view of cloud computing 9
8 User view 9
8.1 Introduction to roles, sub-roles and cloud computing activities 9
8.2 Cloud service customer 10
8.3 Cloud service provider 14
8.4 Cloud service partner 21
8.5 Cross-cutting aspects 23
9 Functional view 29
9.1 Functional architecture 29
9.2 Functional components 30
10 Relationship between the user view and the functional view 38
10.1 General 38
10.2 Overview 38
Annex A – Further details regarding the user view and functional view 44
A.1 The cloud service customer–cloud service provider relationship 44
A.2 The provider–peer provider (or "inter-cloud") relationship 47
A.3 The cloud service developer–cloud service provider relationship 50
A.4 The cloud service provider–Auditor relationship 51
Bibliography 53

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 17789 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Distributed application platforms and services (DAPS)*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. Y.3502 (08/2014).

Documents
Document Sharing Hub

© ISO/IEC 2014 – All rights reserved
Full document details: BS ISO/IEC 17789:2014

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Cloud computing – Reference architecture

1 Scope

This Recommendation | International Standard specifies the cloud computing reference architecture (CCRA). The reference architecture includes the **cloud computing roles**, **cloud computing activities**, and the **cloud computing functional components** and their relationships.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

2.2 Additional references

– ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions in Rec. ITU-T Y.3500 | ISO/IEC 17788 and the following definitions apply.

3.1 Terms defined elsewhere

The following term is defined in ISO/IEC/IEEE 42010:

3.1.1 architecture: Fundamental concepts or properties of a system in its environment embodied in its elements, relationships and in the principles of its design and evolution.

The following term is defined in ISO/IEC 29100:

3.1.2 personally identifiable information (PII): Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other **party**, to identify that natural person.

3.2 Terms defined in this Recommendation | International Standard

This Recommendation | International Standard defines the following terms:

3.2.1 activity: A specified pursuit or set of tasks.

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.

3.2.3 functional component: A functional building block needed to engage in an **activity** (clause 3.2.1), backed by an implementation.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

3.2.4 **peer cloud service**: A **cloud service** of one **cloud service provider** which is used as part of a **cloud service** of one or more other **cloud service providers**.

3.2.5 **peer cloud service provider**: A **cloud service provider** who provides one or more **cloud services** for use by one or more other **cloud service providers** as part of their **cloud services**.

3.2.6 **product catalogue**: A listing of all the **cloud service products** (clause 3.2.2) which **cloud service providers** make available to **cloud service customers**.

3.2.7 **role**: A set of **activities** (clause 3.2.1) that serves a common purpose.

3.2.8 **service catalogue**: A listing of all the cloud services of a particular **cloud service provider**.

3.2.9 **sub-role**: A subset of the **activities** (clause 3.2.1) of a given **role** (clause 3.2.7).

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

API	Application Programming Interface
CaaS	Communications as a Service
CCRA	Cloud Computing Reference Architecture
CPU	Central Processing Unit
CS	Cloud Service
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
KPI	Key Performance Indicator
MSA	Master Service Agreement
NaaS	Network as a Service
PaaS	Platform as a Service
PII	**Personally Identifiable Information**
QoS	Quality of Service
RAM	Random Access Memory
SaaS	Software as a Service
SLA	Service Level Agreement
ToS	Terms of Service
T&C	Terms and Conditions
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VM	Virtual Machine

5 Conventions

The following conventions apply:

1) Diagrams are used throughout this Recommendation | International Standard to help illustrate the CCRA. Figure 5-1 provides the conventions used regarding the content of the diagrams.

NOTE – In Figure 5-1, "Aspect" is to be understood as referring to "Cross-cutting aspect".

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

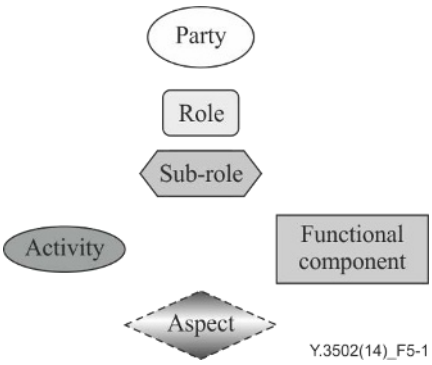

Figure 5-1 – Legend to the diagrams used throughout this Recommendation | International Standard

2) This CCRA uses the term "ICT" and "ICT systems", where the abbreviation ICT stands for "information and communication technology", as defined in clause 3.1332 of ISO/IEC/IEEE 24765. This term is used to make it clear that the CCRA covers not only the compute and storage technologies associated with computer systems, but also the communication networks that link systems together.

3) References to terms defined in clause 3 and in Rec. ITU-T Y.3500 | ISO/IEC 17788 are shown in bold.

6 Cloud computing reference architecture goals and objectives

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand. See Rec. ITU-T Y.3500 | ISO/IEC 17788.

The CCRA presented in this Recommendation | International Standard provides an architectural framework that is effective for describing the **cloud computing roles**, **sub-roles**, **cloud computing activities**, cross-cutting aspects, as well as the functional architecture and **functional components** of **cloud computing**.

The CCRA serves the following goals:

- to describe the community of stakeholders for **cloud computing**;
- to describe the fundamental characteristics of **cloud computing** systems;
- to specify basic **cloud computing activities** and **functional components**, and describe their relationships to each other and to the environment;
- to identify principles guiding the design and evolution of the **CCRA**.

The CCRA supports the following important standardization objectives:

- to enable the production of a coherent set of international standards for **cloud computing;**
- to provide a technology-neutral reference point for defining standards for **cloud computing**;
- to encourage openness and transparency in the identification of **cloud computing** benefits and risks.

The CCRA focuses on the requirements of "what" **cloud services** provide and not on "how to" design cloud-based solutions and implementations. The CCRA does not represent the system architecture of a specific **cloud computing** system, although it could put constraints on a specific system. The CCRA is not tied to any specific vendor products, services or reference implementation; nor does it define prescriptive solutions that inhibit innovation.

The CCRA is also intended to:

- facilitate the understanding of the operational intricacies of **cloud computing**;
- illustrate and provide understanding of various **cloud services** and their provisioning and use;
- provide a technical reference to enable the international community to understand, discuss, categorize and compare **cloud services**;
- be a tool for describing, discussing, and for developing a system-specific architecture using a common framework of reference;
- facilitate the analysis of candidate standards in areas including security, **interoperability**, portability, **reversibility**, reliability and service management, and support analysis of reference implementations.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

7 Reference architecture concepts

This Recommendation | International standard defines a CCRA that can serve as a fundamental reference point for **cloud computing** standardization and which provides an overall framework for the basic concepts and principles of a **cloud computing** system.

This clause provides an overview of the architectural approaches that are used in this Recommendation | International standard.

7.1 CCRA architectural views

Cloud computing systems can be described using a viewpoint approach.

Four distinct viewpoints are used in the CCRA (see Figure 7-1):

- user view;
- functional view;
- implementation view; and
- deployment view.

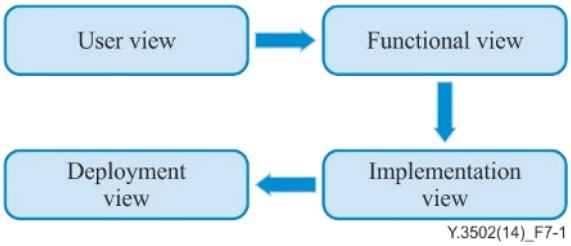

Figure 7-1 – Transformations between architectural views

Table 7-1 provides a description of each of these views.

Table 7-1 – CCRA views

CCRA view	Description of the CCRA view	Scope
User view	The system context, the **parties**, the **roles**, the **sub-roles** and the **cloud computing activities**	Within scope
Functional view	The functions necessary for the support of **cloud computing activities**	Within scope
Implementation view	The functions necessary for the implementation of a **cloud service** within service parts and/or infrastructure parts	Out of scope
Deployment view	How the functions of a **cloud service** are technically implemented within already existing infrastructure elements or within new elements to be introduced in this infrastructure	Out of scope
NOTE – While details of the user view and functional view are addressed within this Recommendation | International Standard, the implementation and deployment views are related to technology and vendor-specific **cloud computing** implementations and actual deployments, and are therefore out of the scope of this Recommendation | International Standard.		

Figure 7-2 shows the transition from the user view to the functional view. Details are presented in clause 7.4.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

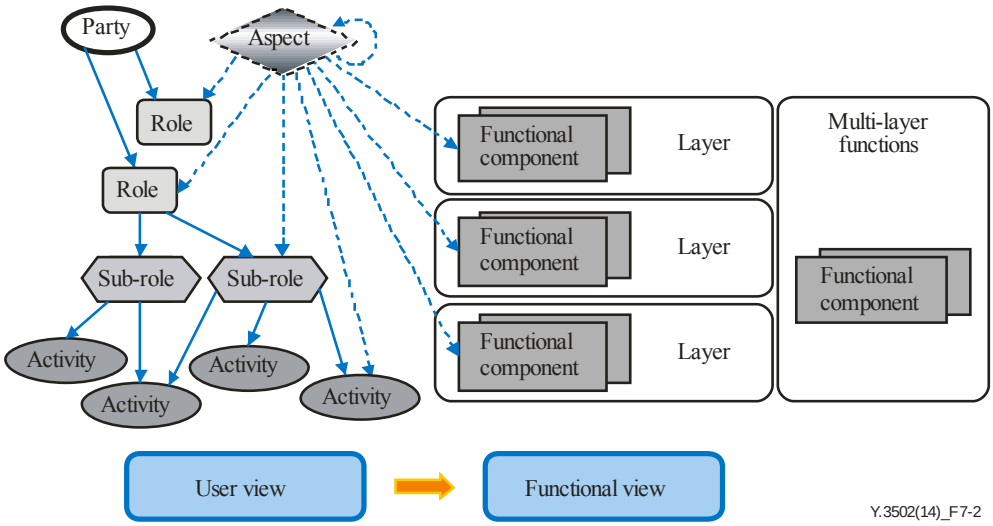

Figure 7-2 – Transition from user view to functional view

7.2 User view of cloud computing

The user view addresses the following **cloud computing** concepts:

- **cloud computing activities**;
- **roles** and **sub-roles**;
- **parties**;
- **cloud services**;
- **cloud deployment models**;
- cross-cutting aspects.

Figure 7-3 illustrates the entities that are defined for the user view.

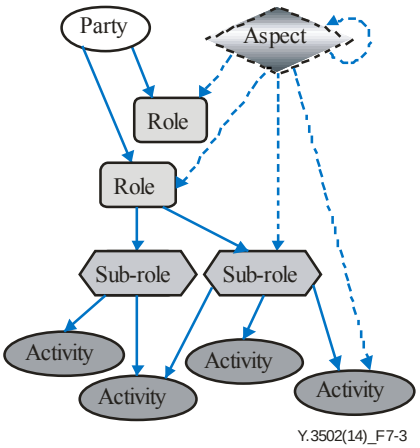

Figure 7-3 – User view entities

7.2.1 Cloud computing activities

A **cloud computing activity** is defined as a specified pursuit or set of tasks.

Cloud computing activities need to have a purpose and deliver one or more outcomes.

Activities in a **cloud computing** system are conducted using **functional components** (see clause 7.3.1).

Cloud computing activities are identified and described in more detail in clause 8.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

7.2.2 Roles and sub-roles

A **role** is a set of **cloud computing activities** that serve a common purpose.

In the CCRA, three **roles** have been defined:

- **cloud service customer (CSC)**: A **party** which is in a business relationship for the purpose of using **cloud services**.
- **cloud service provider (CSP)**: A **party** which makes **cloud services** available.
- **cloud service partner (CSN)**: A **party** which is engaged in support of, or auxiliary to, **activities** of either the **cloud service provider** or the **cloud service customer**, or both.

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**.

Descriptions of the **cloud computing roles** and **sub-roles** are provided in clause 8.

7.2.3 Parties

A **party** is a natural person or legal person, whether or not incorporated, or a group of either. **Parties** in a **cloud computing** system are its stakeholders.

A **party** can assume more than one **role** at any given point in time and can engage in a specific subset of **activities** of that **role**. Examples of parties include, but are not limited to, large corporations, small and medium sized enterprises, government departments, academic institutions and private citizens.

7.2.4 Cloud services

Cloud services are the essential elements of **cloud computing. Cloud services** are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788. This clause provides a summary.

Cloud services can be described in terms of the **cloud capabilities types** which they offer, based on the resources provided by the **cloud service**. There are three **cloud capabilities types**:

- **application capabilities type**;
- **platform capabilities type**;
- **infrastructure capabilities type**.

Cloud capabilities types and **cloud service categories** are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788.

Cloud services are also grouped into categories, where each category is a group of **cloud services** that possess a common set of qualities. The services in these categories can include capabilities from one or more of the **cloud capabilities types** above.

Representative **cloud service categories** include:

- **Infrastructure as a service (IaaS)**;
- **Platform as a service (PaaS)**;
- **Software as a service (SaaS)**;
- **Network as a service (NaaS)**.

Other **cloud service categories** are described in Rec. ITU-T Y.3500 | ISO/IEC 17788.

7.2.5 Cloud deployment models

Cloud deployment models are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788. This clause provides a summary.

Cloud deployment models are a way in which **cloud computing** can be organized based on the control and sharing of physical or virtual resources.

The **cloud deployment models** include:

- **public cloud**;
- **private cloud**;
- **community cloud**;
- **hybrid cloud**.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

7.2.6 Cross-cutting aspects

Cross-cutting aspects are behaviours or capabilities which need to be coordinated across **roles** and implemented consistently in a **cloud computing** system.

Cross-cutting aspects can be shared and can impact multiple **roles**, **cloud computing activities** and **functional components**.

Cross-cutting aspects apply to multiple individual **roles** or **functional components**.

An example of a cross-cutting aspect is security.

A description of the cross-cutting aspects is provided in clause 8.5.

7.3 Functional view of cloud computing

The functional view is a technology-neutral view of the functions necessary to form a **cloud computing** system. The functional view describes the distribution of functions necessary for the support of **cloud computing activities**.

The functional architecture also defines the dependencies between functions.
The functional view addresses the following **cloud computing** concepts:

- **functional components**;
- functional layers; and
- multi-layer functions.

Figure 7-4 illustrates the concepts of functions, layers and **functional components**.

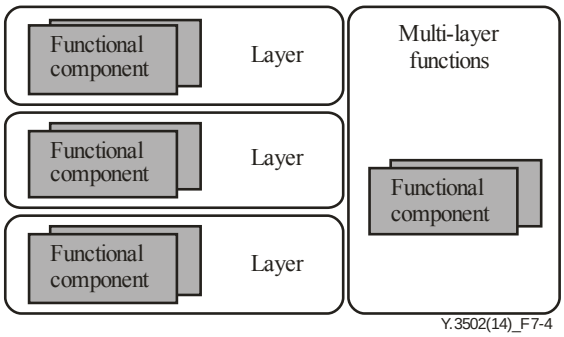

Figure 7-4 – Functional layering

The **cloud computing** functional architecture is described in clause 9.1.

7.3.1 Functional components

A **functional component** is a functional building block needed to engage in an **activity**, backed by an implementation.

The capabilities of a **cloud computing** system are fully defined by the set of implemented **functional components**.

Functional components are further described in clause 9.2.

7.3.2 Functional layers

A layer is a set of **functional components** that provide similar capabilities or serve a common purpose.

The functional architecture is partially layered (i.e., has layers and a set of multi-layer functions).

There are four distinct layers defined in the CCRA:

- user layer, which includes **functional components** that support the **cloud computing activities** of **cloud service customers** and **cloud service partners**;
- access layer, which includes **functional components** that facilitate function distribution and interconnection;
- service layer, which includes **functional components** that provide the **cloud services** themselves plus related administration and business capabilities, and the orchestration capabilities necessary to realize them;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

- resource layer, which includes the **functional components** that represent the resources needed to implement the **cloud computing** system.

Note that not all layers or **functional components** are necessarily instantiated in a specific **cloud computing** system.

7.3.3 Multi-layer functions

The multi-layer functions include **functional components** that provide capabilities that are used across multiple functional layers.

Multi-layer functions are grouped into subsets.

The following subsets of multi-layer functions are defined:

- development support;
- integration;
- security systems;
- operational support systems;
- business support systems.

Functional components of the multi-layer functions are described in clause 9.2.5.

7.4 Relationship between the user view and the functional view

Figure 7-5 illustrates how the user view provides the set of **cloud computing activities** that are represented within the functional view (and realized using the technologies of the implementation view).

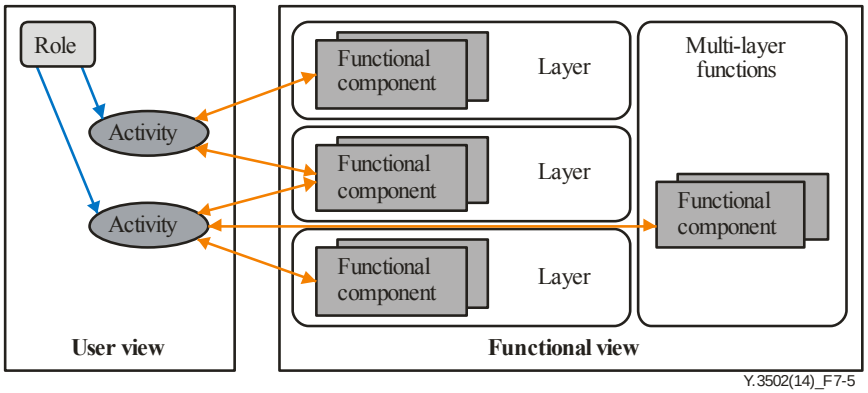

Figure 7-5 – From user view to functional view

Further details on the relationship between the user view and functional view can be found in clause 10.

7.5 Relationship of the user view and functional view to cross-cutting aspects

Cross-cutting aspects, as their name implies, apply across both the user view and across the functional view of **cloud computing**.

Cross-cutting aspects apply to **roles** and **sub-roles** in the user view and they directly or indirectly affect the **activities** which those **roles** perform.

Cross-cutting aspects also apply to the **functional components** within the functional view, which are used when performing the **activities** described in the user view.

Cross-cutting aspects of **cloud computing** described in clause 8.5 include:

- auditability;
- **availability**;
- governance;
- **interoperability**;
- maintenance and versioning;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

- performance;
- portability;
- protection of **personally identifiable information**;
- regulatory;
- resiliency;
- **reversibility**;
- security;
- service levels and **service level agreement**.

7.6 Implementation view of cloud computing

While details of the user view and functional view are addressed within this Recommendation | International Standard, the implementation view is out of the scope of this Recommendation | International Standard.

7.7 Deployment view of cloud computing

While details of the user view and functional view are addressed within this Recommendation | International Standard, the deployment view is out of the scope of this Recommendation | International Standard.

8 User view

8.1 Introduction to roles, sub-roles and cloud computing activities

Given that distributed services and their delivery are at the core of **cloud computing**, all **cloud computing** related **activities** can be categorized into three main groups: **activities** that use services, **activities** that provide services and **activities** that support services.

This clause contains descriptions of some of the common **roles** and **sub-roles** associated with **cloud computing**.

It is important to note that a **party** can play more than one **role** at any given point in time. When playing a **role**, the **party** can restrict itself to playing one or more **sub-roles**. **Sub-roles** are a subset of the **cloud computing activities** of a given **role**.

As shown in Figure 8-1, the **roles** of **cloud computing** are:

- **cloud service customer** (clause 8.2);
- **cloud service provider** (clause 8.3);
- **cloud service partner** (clause 8.4).

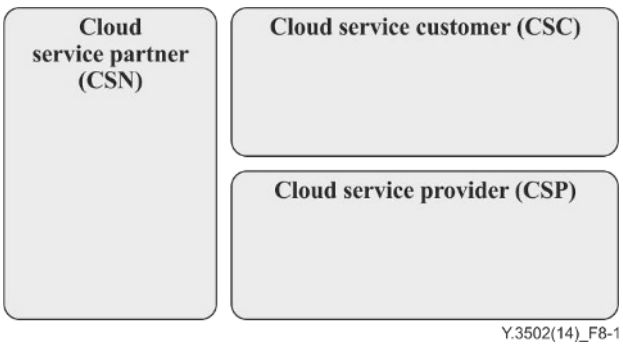

Figure 8-1 – Cloud computing roles

Figure 8-2 shows the **roles** of **cloud computing**, with their associated **sub-roles**. Each of the **sub-roles** shown in the figure is described in more detail in the following clauses.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

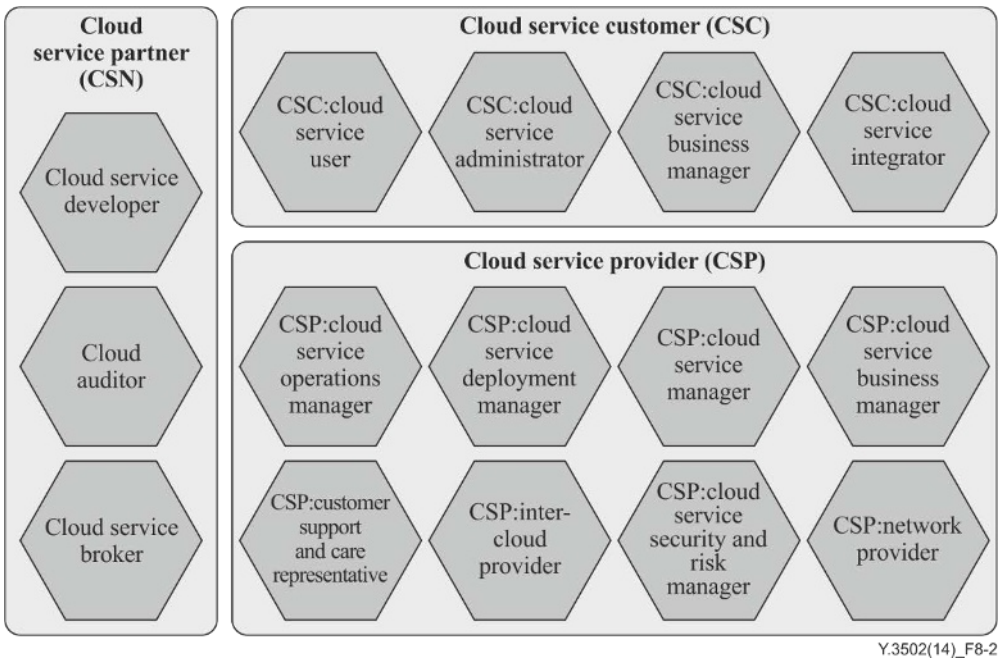

Figure 8-2 – Roles and sub-roles

8.2 Cloud service customer

8.2.1 Role

A **cloud service customer** (CSC) has a business relationship with a **cloud service provider** for the purpose of using **cloud services**. A **cloud service customer** can also have a business relationship with a **cloud service partner** for a variety of purposes.

A **cloud service customer's activities** are included beneath the **sub-roles** described in clauses 8.2.1.1 to 8.2.1.4.

8.2.1.1 CSC:cloud service user

The CSC:cloud service user is a sub-role of **cloud service customer** corresponding to a natural person or an entity acting on their behalf, associated with a **cloud service customer** that uses **cloud services**.

The CSC:cloud service user's **cloud computing activities** include:

- use **cloud service** (clause 8.2.2.1).

8.2.1.2 CSC:cloud service administrator

The CSC:cloud service administrator is a **sub-role** of **cloud service customer,** whose main goal is to ensure the smooth operation of the customer's use of **cloud services,** and that those **cloud services** are running well with the customer's existing ICT systems and applications. The CSC:cloud service administrator oversees all the operational processes relating to the use of **cloud services** and acts as the focal point for technical communications between the **cloud service customer** and the **cloud service provider**.

The CSC:cloud service administrator's **cloud computing activities** include:

- perform service trial (clause 8.2.2.2);
- monitor service (clause 8.2.2.3);
- administer service security (clause 8.2.2.4);
- provide billing and usage reports (clause 8.2.2.5);
- handle problem reports (clause 8.2.2.6);
- administer tenancies (clause 8.2.2.7).

8.2.1.3 CSC:cloud service business manager

The CSC:cloud service business manager is a **sub-role** of **cloud service customer** which aims to meet the business goals of the **cloud service customer** through the acquisition and use of **cloud services** in a cost efficient way. The main

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

responsibilities of the CSC:cloud service business manager concern financial and legal aspects of the use of **cloud services**, including approval, on-going ownership and accountability.

The CSC:cloud service business manager's **cloud computing activities** include:

- perform business administration (clause 8.2.2.8);
- select and purchase service (clause 8.2.2.9);
- request audit report (clause 8.2.2.10).

8.2.1.4 CSC:cloud service integrator

The CSC:cloud service integrator is a **sub-role** of **cloud service customer** which is responsible for the integration of **cloud services** with a **cloud service customer**'s existing ICT systems, including application function and data.

The CSC:cloud service integrator's **cloud computing activities** include:

- connect ICT systems to **cloud services** (clause 8.2.2.11).

8.2.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service customer** are shown in Figure 8-3.

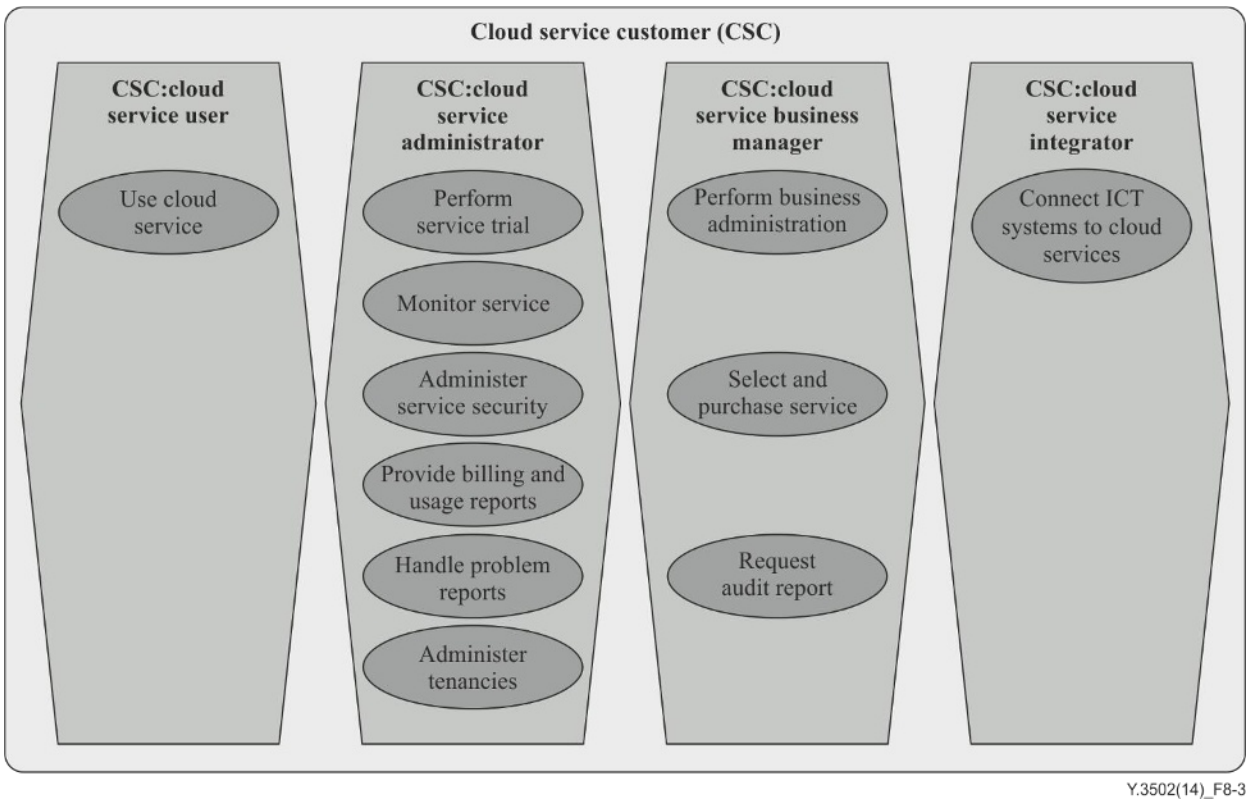

Figure 8-3 – Cloud computing activities relating to cloud service customer sub-roles

8.2.2.1 Use cloud service

The use **cloud service activity** involves using the services of a **cloud service provider** in order to accomplish some tasks.

The use **cloud service activity** typically involves:

1) the provision of user credentials to enable the **cloud service provider** to authenticate the user and grant access to the **cloud service**;
2) the invocation of the **cloud service**, which then operates and delivers its specified outcomes.

8.2.2.2 Perform service trial

The perform service trial **activity** involves using the services of a **cloud service provider** in order to ensure that the **cloud service** is fit for the **cloud service customer**'s business needs. The **cloud services** are used on a trial basis, with mutual agreement and understanding between the **cloud service provider** and **cloud service customer**.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

The perform service trial **activity** involves:

1) The provision of the user credentials to enable the **cloud service provider** to authenticate the user and grant access to the "trial" **cloud service**;
2) The invocation of the "trial" **cloud service**, which can be tested by the **cloud service customer** for business purposes.

8.2.2.3 Monitor service

The monitor service **activity** monitors the delivered service quality with respect to service levels as defined in the **service level agreement** (**SLA)** between **cloud service customer** and **cloud service provider**. This **activity** utilizes intrinsic monitoring functions of the cloud system. This **activity** involves:

- keeping track of how much use is being made of each **cloud service**, and by which users. This includes assurance that the use is appropriate;
- monitoring the integration of the **cloud services** with customer's existing ICT systems to ensure that business goals are being met;
- defining measurement points and performance indicators related to the service in question (e.g., service **availability**, service outage frequency, mean time to repair, responsiveness of the provider's help desk, etc.);
- monitoring, analysing and archiving of these indicator data;
- comparing the actual service quality that is delivered with the agreed service quality.

8.2.2.4 Administer service security

The administer service security **activity** involves:

- ensuring appropriate security for **cloud service customer data** that is placed into a **cloud computing** environment
- putting in place plans for data backup and recovery, and potentially for data duplication and failover;
- administering security policies;
- defining encryption and **integrity** technologies to apply to the **cloud service customer data** both at rest and also in motion;
- defining the handling of any **personally identifiable information (PII)** in the **cloud service customer data**.

8.2.2.5 Provide billing and usage reports

The provide billing and usage reports **activity** involves preparing reports of the usage of **cloud services** by the customer organization and associated reports of the billing/invoice data which relate to that usage. These reports are provided to the CSC:business manager.

8.2.2.6 Handle problem reports

The handle problem reports **activity** involves the customer-side handling of any reported problems associated with the usage of **cloud services.** This includes:

- assessing the impact of each problem;
- troubleshooting to determine the cause(s) of the problem;
- opening a problem report(s) with the **cloud service provider** and tracking to resolution;
- developing workarounds to address the problem;
- escalating problems that are not fixed within agreed timescales or which have serious business impacts.

8.2.2.7 Administer tenancies

The administer tenancies **activity** involves administering the tenancies of the **cloud service customer** with the **cloud service provider**. This **activity** involves:

- configuring and controlling security aspects including user accounts, security **roles**, identities and permissions;
- identifying and controlling data that is shared between users within the tenancy;
- creating and removing **tenants**;
- managing users and allocated resources of **tenants**;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014

- defining enforcement policies for each **tenant**.

8.2.2.8 Perform business administration

The perform business administration **activity** involves the management of the business aspects of the use of **cloud services** including accounting and financial management. This **activity** includes:

- adjusting business plan to accommodate the use of **cloud services**;
- tracking the use of the services and dealing with accounting and financial management;
- handling billing/invoices received from the **cloud service provider** for the use made of **cloud services**;
- ensuring that billing matches the actual usage of **cloud services** made by the **cloud service customer**;
- making payments to the **cloud service provider**;
- keeping accounts in relation to the use of **cloud services**.

8.2.2.9 Select and purchase service

The select and purchase service **activity** involves:

- examining the **cloud service** offerings of (one or more) **cloud service providers** to determine if the service offered meets the business and technical requirements of the **cloud service customer**. This typically involves the reading of a **product catalogue** and the documentation for each service, which can include technical information about the service and its **SLAs**, plus business information including pricing;
- negotiating the terms for the **cloud service** (if the **cloud service provider** permits variable terms for the service);
- accepting the contract for the **cloud service** and performing registration with the **cloud service provider**.

8.2.2.10 Request audit report

The request audit report **activity** involves the **cloud service customer** requesting the report of an audit of the **cloud service**, typically conforming to a particular audit standard or scheme. The **cloud service customer** can request the report from a **cloud auditor**, or possibly from the **cloud service provider**, although it is expected that the audit report is prepared by an entity independent of the **cloud service provider** both before a purchase is completed and also periodically once the service is in use.

8.2.2.11 Connect ICT systems to cloud services

The connect ICT systems to **cloud services activity** includes the integration between existing ICT systems and **cloud services** and involves the connection of existing ICT component(s) and applications with the target **cloud service**(s) and also the connection of the customer monitoring and management systems with the **cloud service provider 's** monitoring and control of **cloud services**.

The connection of existing ICT components and applications with the target **cloud service**(s) involves:

- assessing the impact of **cloud service**(s) on existing processes, systems and services;
- mapping business data between **cloud service customer's** existing ICT systems and **cloud services**;
- invoking **cloud service** operations from existing ICT components and applications, with the supply of input data and the handling of output data;
- provisioning of access rights for CSC:cloud service users;
- defining and implementing security related requirements, including the **confidentiality** and **integrity** of data flows;
- integrating customer facilities for the administration of user accounts, security **roles**, identities and permissions with the equivalent facilities for the **cloud services**;
- creating and monitoring specific user accounts and identities for the use of management interfaces for **cloud services**;
- integrating logging and security incident management between **cloud services** and **cloud service customer** monitoring and management infrastructure.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 17789:2014