International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3502

(08/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Cloud Computing

Information technology – Cloud computing – Reference architecture

Recommendation ITU-T Y.3502

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**

For further details, please refer to the list of ITU-T Recommendations.

INTERNATIONAL STANDARD ISO/IEC 17789
RECOMMENDATION ITU-T Y.3502

Information technology – Cloud computing – Reference architecture

Summary

Rec. ITU-T Y.3502 | ISO/IEC 17789 provides the reference architecture for cloud computing, which includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3502	2014-08-13	13	11.1002/1000/12209

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

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

**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.

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".

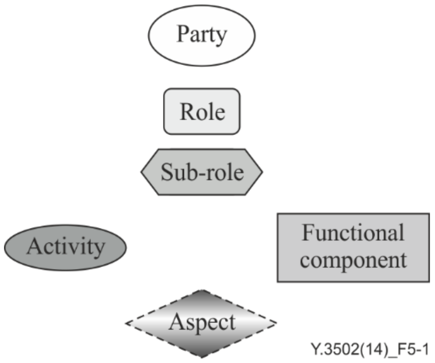


Figure 5-1 – Legend to the diagrams used throughout this Recommendation | International Standard

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.

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.

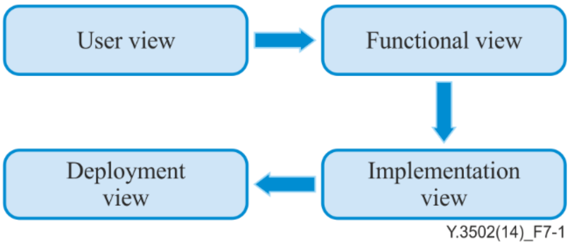


Figure 7-1 – Transformations between architectural views

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.

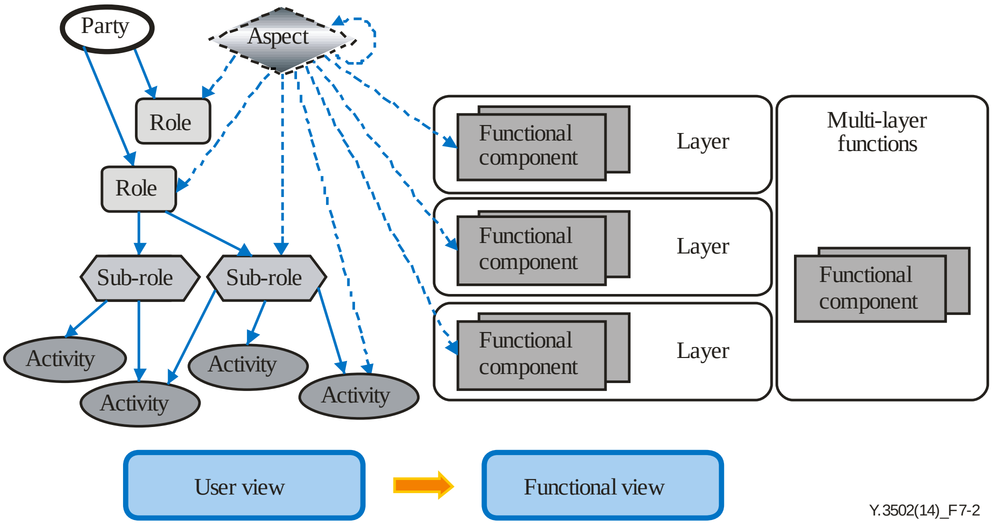


Figure 7-2 – Transition from user view to functional view

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.

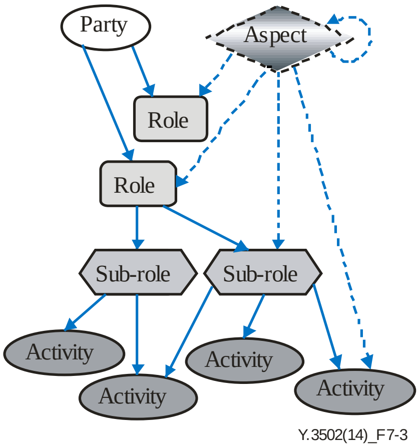


Figure 7-3 – User view entities

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.

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**.

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**.

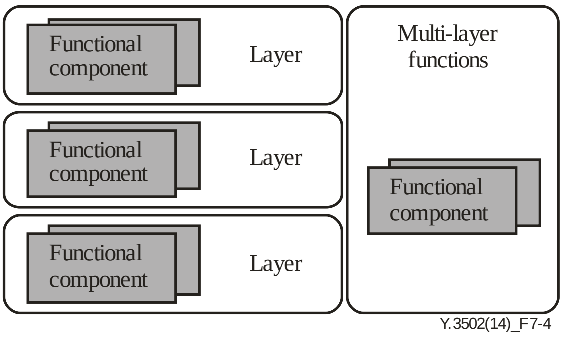


Figure 7-4 – Functional layering

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;

- 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).

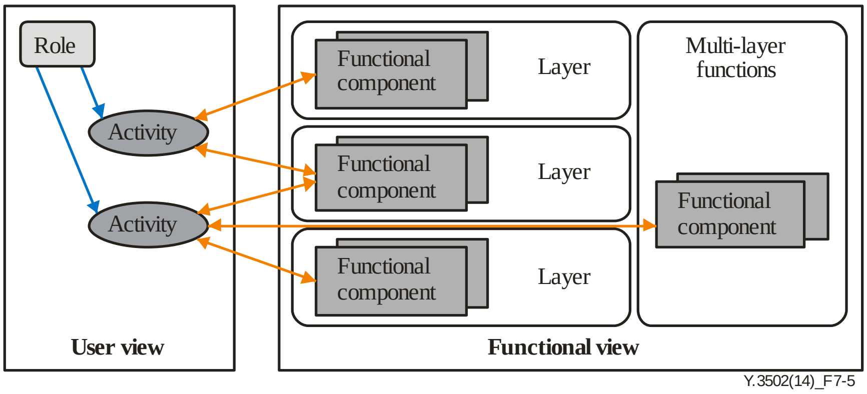


Figure 7-5 – From user view to functional view

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;

- 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).

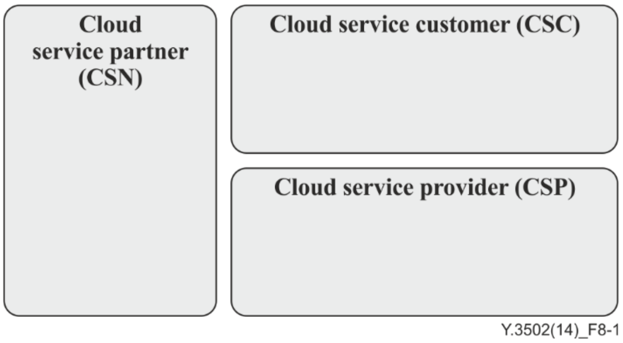

Cloud service partner (CSN)
Cloud service customer (CSC)
Cloud service provider (CSP)
Y.3502(14)_F8-1

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.

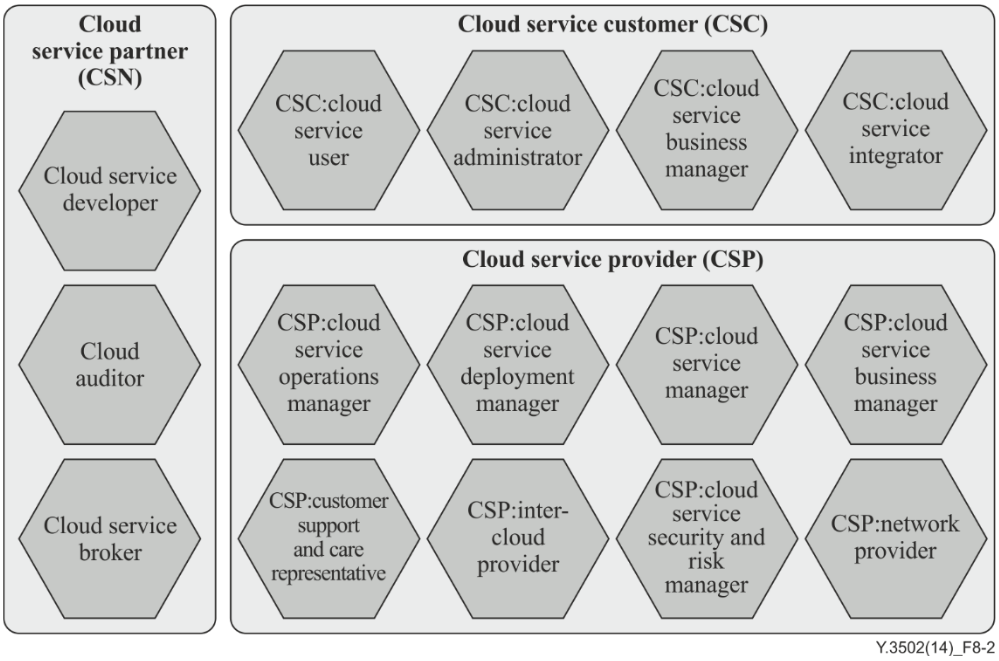

Cloud service partner (CSN)
Cloud service developer
Cloud auditor
Cloud service broker
Cloud service customer (CSC)
CSC:cloud service user
CSC:cloud service administrator
CSC:cloud service business manager
CSC:cloud service integrator
Cloud service provider (CSP)
CSP:cloud service operations manager
CSP:cloud service deployment manager
CSP:cloud service manager
CSP:cloud service business manager
CSP:customer support and care representative
CSP:inter-cloud provider
CSP:cloud service security and risk manager
CSP:network provider
Y.3502(14)_F8-2

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 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.

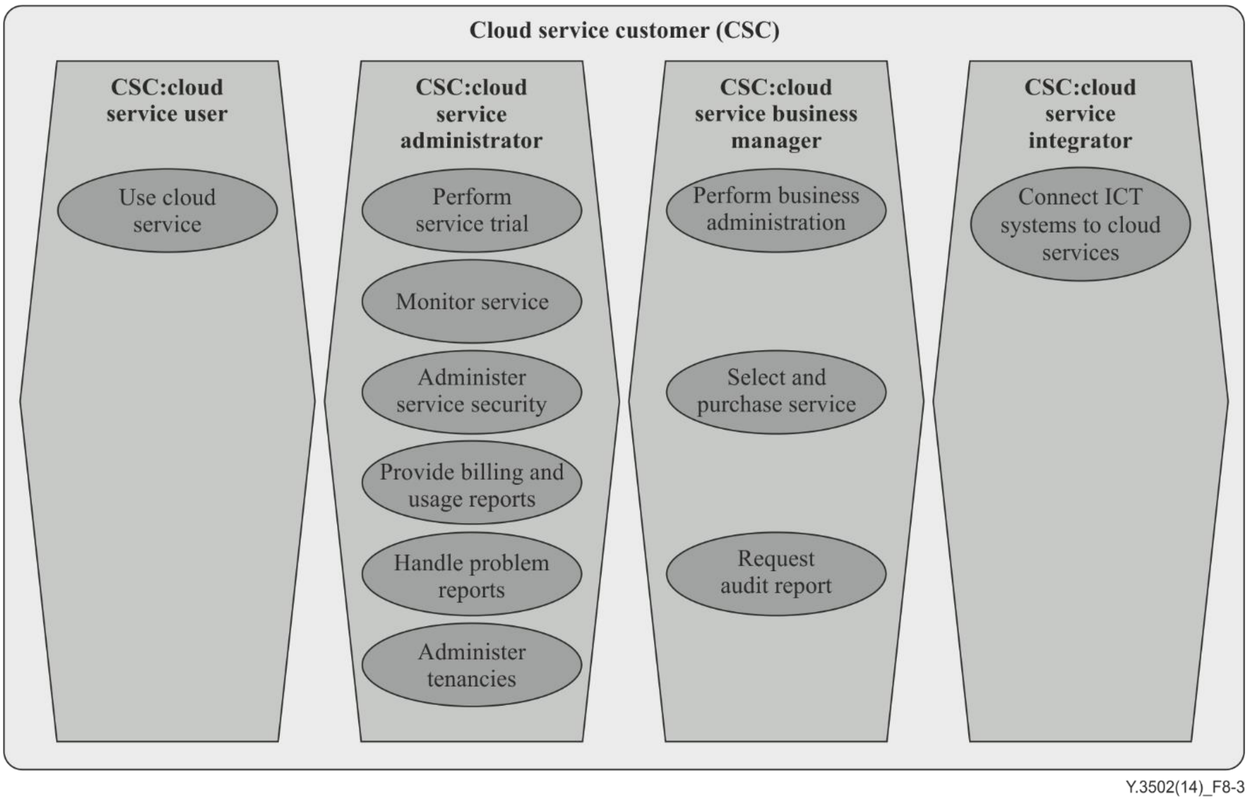

Cloud service customer (CSC)
CSC:cloud service user
Use cloud service
CSC:cloud service administrator
Perform service trial
Monitor service
Administer service security
Provide billing and usage reports
Handle problem reports
Administer tenancies
CSC:cloud service business manager
Perform business administration
Select and purchase service
Request audit report
CSC:cloud service integrator
Connect ICT systems to cloud services
Y.3502(14)_F8-3

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**.

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**;

- 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.

8.3 Cloud service provider

8.3.1 Role

A **cloud service provider** (CSP) makes **cloud services** available to **cloud service customers**. This **role** (and all of its **sub-roles**) focuses on the **cloud computing activities** necessary to provide a **cloud service** and the **cloud computing activities** necessary to ensure its delivery to the **cloud service customer**, as well as **cloud service** maintenance.

The **cloud service provider** is responsible for dealing with the business relationship with **cloud service customers**.

A **cloud service provider's activities** are included beneath the **sub-roles** described in clauses 8.3.1.1 to 8.3.1.8.

8.3.1.1 CSP:cloud service operations manager

The CSP:cloud service operations manager is a **sub-role** of **cloud service provider** which is responsible for performing all operational processes and procedures of the **cloud service provider**, ensuring that all services and associated infrastructure meet operational targets.

The CSP:cloud operations manager's **cloud computing activities** include:

- prepare systems (clause 8.3.2.1);
- monitor and administer services (clause 8.3.2.2);
- manage assets and inventory (clause 8.3.2.3);
- provide audit data (clause 8.3.2.4).

8.3.1.2 CSP:cloud service deployment manager

The CSP:cloud service deployment manager is a **sub-role** of **cloud service provider** which has responsibility for the planning of the deployment of a service into production. This includes defining the operational environment for the service, the initial steps for deployment of the service and its dependencies, and the enablement of operations processes which are used during the running of the service.

The CSP:cloud service deployment manager's **cloud computing activities** include:

- define environment and processes (clause 8.3.2.5);
- define and gather metrics (clause 8.3.2.6);
- define deployment steps (clause 8.3.2.7).

8.3.1.3 CSP:cloud service manager

The CSP:cloud service manager is a sub-role of **cloud service provider** which has responsibility for ensuring that the **cloud service provider**'s services are available for use by **cloud service customers**, and that they function correctly and comply with targets specified in the **service level agreement**. The CSP:cloud service manager is also responsible for ensuring the smooth operation of the **cloud service provider**'s business support system and operational support system, as well as the operation of the other functionalities offered to the **cloud service customers** and **cloud service partners** for management, administration and other **cloud computing activities**.

The CSP:cloud service manager's **cloud computing activities** include:

- provide services (clause 8.3.2.8);
- deploy and provision services (clause 8.3.2.9);
- perform service level management (clause 8.3.2.10).

8.3.1.4 CSP:cloud service business manager

The CSP:cloud service business manager is a **sub-role** of **cloud service provider** which has overall responsibility for the business aspects of offering **cloud services** to **cloud service customers**. The CSP:cloud service business manager creates and tracks the business plan, defines the service offering strategy and manages the business relationship with **cloud service customers**.

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

- manage business plan to provide **cloud services** (clause 8.3.2.11);
- manage customer relationships (clause 8.3.2.12);
- manage financial processing (clause 8.3.2.13).

8.3.1.5 CSP:customer support and care representative

The CSP:customer support and care representative is a **sub-role** of **cloud service provider** that is the main interface for the **cloud service customer** with the **cloud service provider** and is responsible for reacting to customer issues and queries in a timely and cost efficient way, with the goal of maintaining customer satisfaction with the **cloud service provider** and the **cloud services** offered.

The CSP:customer support and care representative's **cloud computing activities** include:

- handle customer requests (clause 8.3.2.14).

8.3.1.6 CSP:inter-cloud provider

The CSP:inter-cloud provider is a **sub-role** of **cloud service provider** that relies on one or more **peer cloud service providers** to provide part or all of the **cloud services** offered to **cloud service customers** by that CSP:inter-cloud provider. The CSP:inter-cloud provider's main activities are the intermediation, aggregation, arbitrage, peering or federation of **peer cloud service providers' cloud services** and their business and administration capabilities from the **cloud service customer** viewpoint so that the **cloud service customer** only uses the service, business and administration interfaces of the inter-cloud service provider.

The CSP:inter-cloud provider's **cloud computing activities** include:

- manage **peer cloud services** (clause 8.3.2.15);
- perform peering, federation, intermediation, aggregation and arbitrage (clause 8.3.2.16).

8.3.1.7 CSP:cloud service security and risk manager

The CSP:cloud service security and risk manager is a **sub-role** of **cloud service provider** which has the responsibility of ensuring that the **cloud service provider** appropriately manages the risks associated with the development, delivery, use and support of **cloud services**. This includes ensuring that the **information security** policies of the **cloud service customer** and the **cloud service provider** are aligned and meet the security requirements stated in the **SLA**.

The CSP:cloud service security and risk manager's **cloud computing activities** include:

- manage security and risks (clause 8.3.2.17);
- design and implement service continuity (clause 8.3.2.18);
- ensure compliance (clause 8.3.2.19).

8.3.1.8 CSP:network provider

The CSP:network provider is a **sub-role** of **cloud service provider** which is to provide network connectivity and network services for the **cloud service customer**, **cloud service partner** and **cloud service provider**. The CSP:network provider may provide network connectivity between systems within the **cloud service provider**'s data centre, or provide network connectivity between the **cloud service provider**'s systems and systems outside the provider's data centre, for example, **cloud service customer** systems or systems belonging to other **cloud service providers**.

The CSP:network provider's **cloud computing activities** include:

- provide network connectivity (clause 8.3.2.20);
- deliver network services (clause 8.3.2.21);
- provide network management services (clause 8.3.2.22).

The CSP:network provider can also choose to offer dynamic control of network connectivity as an **NaaS**.

8.3.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service provider** are shown in Figure 8-4.

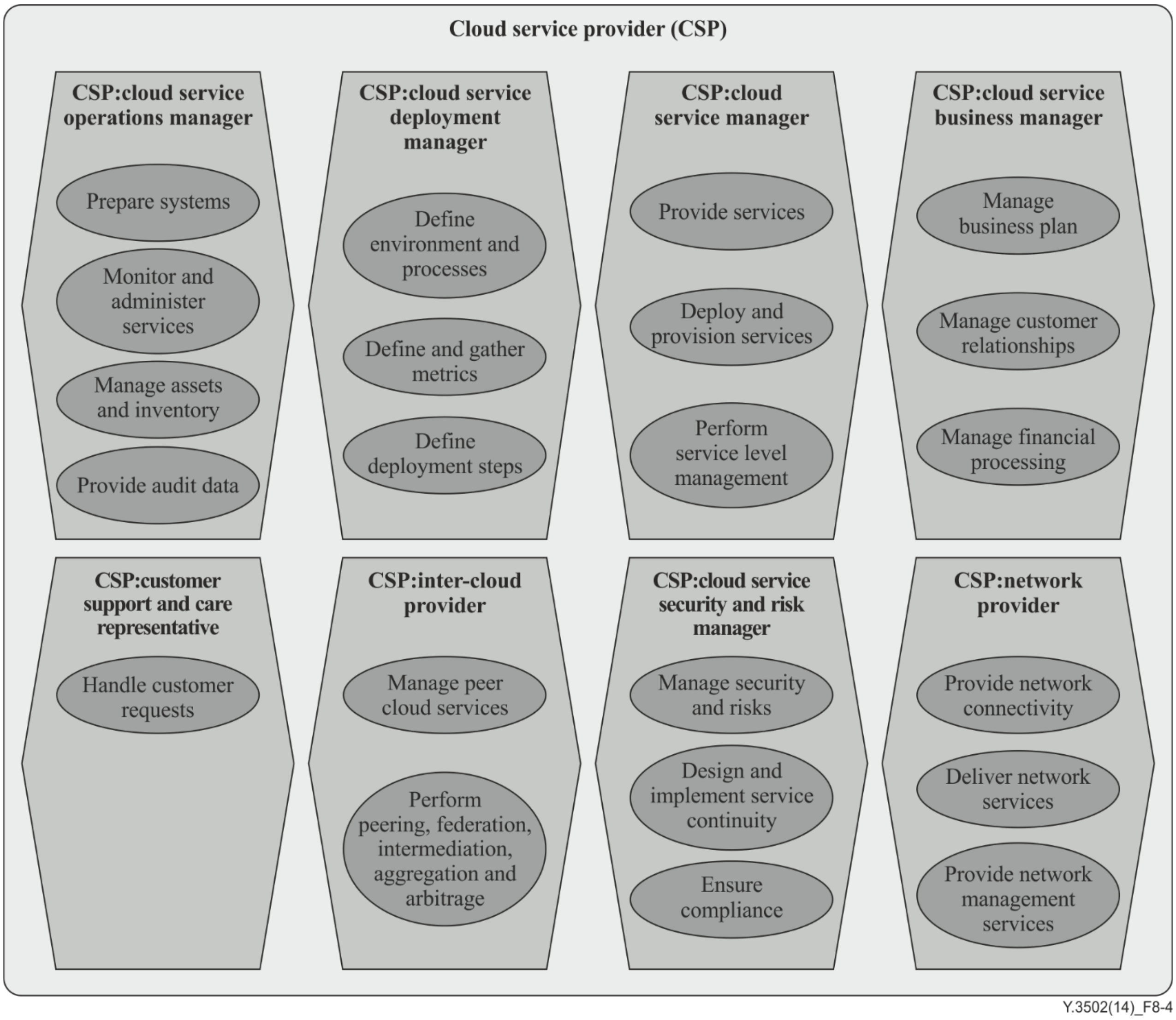

Cloud service provider (CSP)
CSP:cloud service operations manager
Prepare systems
Monitor and administer services
Manage assets and inventory
Provide audit data
CSP:cloud service deployment manager
Define environment and processes
Define and gather metrics
Define deployment steps
CSP:cloud service manager
Provide services
Deploy and provision services
Perform service level management
CSP:cloud service business manager
Manage business plan
Manage customer relationships
Manage financial processing
CSP:customer support and care representative
Handle customer requests
CSP:inter-cloud provider
Manage peer cloud services
Perform peering, federation, intermediation, aggregation and arbitrage
CSP:cloud service security and risk manager
Manage security and risks
Design and implement service continuity
Ensure compliance
CSP:network provider
Provide network connectivity
Deliver network services
Provide network management services
Y.3502(14)_F8-4

Figure 8-4 – Cloud computing activities relating to cloud service provider sub-roles

8.3.2.1 Prepare systems

The prepare systems **activity** is focused on preparing the systems of the provider's environment for new **cloud service** deployments. This **activity** involves:

- assessing the impact of new service deployments or the increase in use of existing services;
- modifying or expanding the resources in the data centre to meet the needs of new deployments.

8.3.2.2 Monitor and administer services

The monitor and administer services **activity** focuses on monitoring and administering services and their associated infrastructure which includes user and system privileges. This **activity** involves:

- monitoring the services and infrastructure of the **cloud service provider**;
- capturing events and data that are significant to the business of the provider and presenting this data in a form that is significant to the CSP:cloud service business manager. Such information includes items such as the usage of the **cloud services** by **cloud service customers** and the cost of provision of those services;
- administering network infrastructure including routers, domain name servers, IP addresses, virtual private networks (VPNs), firewalls and content filtering;
- allocating and administering storage;
- administering user and system privileges;
- configuring and maintaining operating systems and hypervisors;
- administering a virtualization environment;

- monitoring the behaviour of the ICT environment of the **cloud service provider** to ensure that it is running correctly and that provided **cloud services** are meeting the terms of the **SLA**;
- recording problems, reporting problems appropriately (which can involve a message being sent to one or more customers), and following problem resolution processes until the problem is fixed.

8.3.2.3 Manage assets and inventory

The manage assets and inventory **activity** involves:

- keeping track of all compute, storage, network and software assets and the relationship between them. This includes tracking aspects such as versions and patch levels, plus configuration information, where relevant;
- 'on-boarding' of new assets and disposal of old assets. This can include ensuring that new assets are fit for purpose and have been properly checked from a security and manageability standpoint and can include the disposal of assets that are no longer required. This can include appropriate secure disposal of any assets that might hold data.

8.3.2.4 Provide audit data

The provide audit data **activity** is the collection and provision of data relevant to an audit request, such as that relating to security controls or to service performance. The data requested will depend on the auditing scheme or standard that is being used. This **activity** involves:

- creating and sending appropriate audit information from logs, etc.;
- redacting information from any log records or other data that might contain sensitive information or **PII**.

8.3.2.5 Define environment and processes

The define environment and process **activity** focuses on defining the required technical environment and operational processes used when a service is running. This **activity** involves:

- defining the required technical environment in terms of compute, storage and network resources, the software dependencies including configuration;
- defining policies and processes for scaling up and scaling down the use of resources in response to changing usage demand;
- assuring that the **cloud service** adheres to appropriate standards relating to security and business compliance;
- defining the processes to follow when the service is running, including plans for fixes, upgrades and migration.

8.3.2.6 Define and gather metrics

The define and gather metrics **activity** focuses on defining service level metrics and management. This **activity** involves:

- defining the metrics that are used in relation to the operation of **cloud services**, which are typically reflected in the **SLA** relating to those services;
- designing how the metrics are captured for each **cloud service**;
- defining how the metrics are reported and managed, in particular to ensure that **SLA** targets are met.

8.3.2.7 Define deployment steps

The define deployment steps **activity** focuses on defining the steps for the deployment of services. This **activity** involves describing each of the steps that need to be taken by the operations and support teams in order to get the service implementation deployed and ready for use by **cloud service customers**.

8.3.2.8 Provide services

The provide services **activity** involves all steps required to deliver a **cloud service** to its **cloud service customers**. The provide services **activity** includes accepting and processing service invocations from the user with associated authentication and authorization of the user identity. The processing of a service invocation is done by means of an instance of the service implementation, which can in turn involve the composition and calling of other services as determined by the design and configuration of the service implementation.

The provide services **activity** also involves the following:

- managing the service fault handling process;
- managing the business support system and the operational support system;

- maintaining the service and underlying infrastructure;
- automating system processes;
- managing long term capacity and performance trends;
- installing, configuring and performing maintenance updates on required hardware for compute, storage and network capabilities for the **cloud service provider**'s data centre;
- installing and configuring the software required to run the cloud provider's data centre and support **cloud service** implementations. This includes applying fixes, updates and upgrades to that software, as required.

8.3.2.9 Deploy and provision services

The deploy and provision services **activity** involves getting a service implementation running and making it available at a network end point accessible to the CSC:cloud service users and making it able to handle service requests from users. This activity includes:

- following the deployment processes defined for the service.

NOTE – This activity also covers the processes required to un-deploy and de-provision a cloud service.

8.3.2.10 Perform service level management

The perform service level management **activity** focuses on managing compliance with **SLA** targets. This **activity** involves:

- monitoring the metrics for each service and comparing them with the service targets required by the **SLA** for the service;
- taking action when the metrics do not meet the values required by the **SLA**, to bring the service back into compliance with the **SLA,** for example, by following procedures laid down by the CSP:cloud service deployment manager;
- reporting a problem if compliance cannot be maintained.

8.3.2.11 Manage business plan

The manage business plan **activity** involves:

- defining a service offering, describing the technical aspects of the offering (functional interfaces, **SLAs**,…) and the business aspects of the offering;

  NOTE – When establishing the service offering, the **cloud service provider** can take into account aspects related to the interaction with **peer cloud service providers**.
- creating a business plan which covers the offering of one or more **cloud services** to customers, handling both financial and technical aspects of the services, the target customer set, contracts and **SLAs**, channels to market, sales targets;
- tracking the sales and service usage against the plan to ensure that financial targets are achieved for the **cloud service provider;**
- preparing a business plan and adjusting the business plan to provide **cloud services**.

8.3.2.12 Manage customer relationships

The manage customer relationships activity involves the management of the business relationship of the **cloud service provider** with the **cloud service customer** including:

- creating and maintaining content of a **product catalogue**;
- acquiring customers;
- providing the point of contact for the customer for all business matters;
- discussing and resolving concerns or problems raised by the customer;
- processing change requests (e.g., entitlement changes).

8.3.2.13 Manage financial processing

The manage financial processing **activity** involves:

- handling billing updates or challenges;
- generating billing information and/or an invoice for charges relating to the use of **cloud services** and transmitting the billing information or invoice to the **cloud service customer**;
- handling the receipt of payments from the **cloud service customer** and their accounting.

8.3.2.14 Handle customer requests

The handle customer requests **activity** involves:

- handling support requests, reports and incidents from **cloud service customers**, however received. Customers can be provided with a variety of means to communicate, from forums through email, customer support desk systems or web portals to real-time communication with provider support personnel;

NOTE – Some requests or reports can only require the provision of information or the clarification of details. Other requests and reports can require problem analysis, or they can involve the creation of a change request.

8.3.2.15 Manage peer cloud services

The manage peer **cloud services activity** focuses on managing the usage of **cloud services** of a **peer cloud service provider**. This **activity** involves:

- selecting and using one or more services of a **peer cloud service provider**;
- monitoring and managing the **peer cloud service provider's cloud services** to ensure that they meet agreed **SLA** targets including the reporting and resolution of problems with those services;
- managing the business aspects of the **cloud services** of a **peer cloud service provider**, including the business plan and financial processing;
- keeping track of how much use is being made of each **cloud service** of a **peer cloud service provider**, and by which users, and including assurance that the use is appropriate and within the business plan;
- monitoring the integration of the **cloud services** of a **peer cloud service provider** with service implementations to ensure that business goals are being met;
- coordinating identity and security credentials between the **cloud service customer** and all the **peer cloud service providers**.

8.3.2.16 Perform peering, federation, intermediation, aggregation and arbitrage

The perform peering, federation, intermediation, aggregation and arbitrage **activity** involves the use of **peer cloud service provider's cloud services** in particular ways:

- peering is the use of **cloud services** of a **peer cloud service provider**;
- federation involves using the **cloud services** of a group of **peer cloud service providers** who mutually combine their service capabilities in order to provide the set of **cloud services** required by customers;
- intermediation involves a **cloud service provider** offering a **cloud service** which is based on conditioning or enhancing the **cloud service** of a **peer cloud service provider**. Examples of enhancements include managing access to **cloud services**, providing a **cloud service** application programming interface (API) façade, identity management, performance reporting, enhanced security, and so on;
- aggregation involves a **cloud service provider** offering a **cloud service** which is based on the composition of a set of services provided by **peer cloud service providers**;
- arbitrage involves a **cloud service provider** offering a **cloud service** which is based on selecting one service offering from a group offered by **peer cloud service providers**.

8.3.2.17 Manage security and risks

The manage security and risks **activity** focuses on the management of security and risks associated with the development, delivery, use and support of **cloud services**. This **activity** involves:

- defining **information security** policy – taking into consideration the service requirements, statutory and regulatory requirements and contractual and **SLA** obligations;
- defining **information security** risks relating to the **cloud service** and the approach to those risks that meets the business goals of the **cloud service provider.** A significant point here is that managing **information security** risks has an associated cost and that the provider can take a business position of not handling some risks, instead passing over responsibility for those risks to the **cloud service customer** via the service agreement, in order to address the cost requirements of some part of the marketplace.
- selecting design point and associated **information security** controls required to address risks associated with the service and design point chosen. The controls typically cover a set of categories, such as:
  - identity and access management;
  - discover, categorize, protect data and information assets;
  - information systems acquisition, development and maintenance;
  - secure infrastructure against threats and vulnerabilities;

  - problem and **information security** incident management;
  - security governance and compliance;
  - physical and personnel security;
  - security of networks and communications;
  - isolation (between **tenants** in a multi-tenant situation).
- ensuring that the identified controls are in place for the deployed service and the underlying infrastructure;
- designing, implementing and evaluating system and application security;
- managing, designing, implementing and evaluating the security of **cloud services** of **peer cloud service providers**;
- evaluating the effectiveness of the implemented controls and make changes based on experience;
- assuring that operating and business support systems provide data access to **cloud service provider** staff based on the particular **cloud service customers tenants** they provide a service to.

8.3.2.18 Design and implement service continuity

The design and implement service continuity **activity** involves:

- considering potential modes of failure of a **cloud service** and the supporting infrastructure and putting in place recovery processes that will enable the **cloud service** to be available within the terms of the **SLA**, through techniques such as failover and redundancy.

8.3.2.19 Ensure compliance

The ensure compliance **activity** focuses on implementing regulatory and standards compliance. This **activity** involves:

- ensuring that the implementation of the **cloud service** and its supporting infrastructure meets the requirements of any standards that need to be supported, for example, the standards can be required by the target customer set, or can be required by the certification scheme that the provider has chosen to assure the service;
- ensuring that the implementation of the **cloud service** and its supporting infrastructure (including data handling) meets any regulatory requirements that can exist for the service or for the data that is stored or processed by the service.

8.3.2.20 Provide network connectivity

The provide network connectivity **activity** involves the setting up of requested network connections and related capabilities, including (amongst others) connections between the **cloud service customer** and the **cloud service provider's** system and between one **cloud service provider's** system and another **cloud service provider's** system. This can include the establishment of facilities such as a VPN or of dedicated bandwidth connections.

Network capabilities include the ability to provide appropriate bounded delay, jitter, bandwidth, quality of service and reliability for all **cloud service categories** and for both cloud and non-cloud purposes in the case of **NaaS**.

8.3.2.21 Deliver network services

The deliver network services **activity** involves the provision of network related services such as firewalls or load balancing.

8.3.2.22 Provide network management services

The provide network management services **activity** focuses on managing the network infrastructure used to carry **cloud services**. This **activity** provides methods, tools and procedures allowing the operation, administration, maintenance and provisioning of the cloud network infrastructure. It includes tasks for:

- keeping the network up and running smoothly;
- keeping track of resources in the network and how they are allocated;
- performing repairs and upgrades, for example, when equipment must be replaced or upgraded with new functions;
- configuring resources in the network to support a **cloud service**.

8.4 Cloud service partner

8.4.1 Role

A **cloud service partner (CSN)** is 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 cloud service partner's cloud computing activities vary depending on the type of partner and their relationship with the **cloud service provider** and the **cloud service customer**.

8.4.1.1 Cloud service developer

The cloud service developer is a **sub-role** of **cloud service partner** which is responsible for designing, developing, testing and maintaining the implementation of a **cloud service**. This can involve composing the service implementation from existing service implementations.

The cloud service developer's **cloud computing activities** include:

- design, create and maintain service components (clause 8.4.2.1);
- compose services (clause 8.4.2.2);
- test services (clause 8.4.2.3).

NOTE 1 – Cloud service integrator and cloud service component developer describe **sub-roles** of cloud service developer, where the cloud service integrator deals with the composition of a service from other services, and where cloud service component developer deals with the design, creation, testing and maintenance of individual service components.

NOTE 2 – This includes service implementations and service components that involve interactions with **peer cloud service providers**.

8.4.1.2 Cloud auditor

The **cloud auditor** is a **sub-role** of **cloud service partner** with the responsibility of conducting an audit of the provision and use of **cloud services**. A cloud audit typically covers operations, performance and security, and examines whether a specified set of audit criteria are met. There are a variety of specifications for the audit criteria, for example, ISO/IEC 27002 addresses security considerations.

The **cloud auditor's cloud computing activities** include:

- perform audit (clause 8.4.2.4);
- report audit results (clause 8.4.2.5).

8.4.1.3 Cloud service broker

The **cloud service broker** is a **sub-role** of **cloud service partner** that negotiates relationships between **cloud service customers** and **cloud service providers**. The **cloud service broker** is not itself a **cloud service provider** and should not be confused with the role of inter-cloud provider (see clause 8.3.1.6). The **cloud service broker** role could be combined with or operate independently of the role of inter-cloud provider.

The **cloud computing activities** of a **cloud service broker** include:

- acquire and assess customers (clause 8.4.2.6);
- assess marketplace (clause 8.4.2.7);
- set up legal agreement (clause 8.4.2.8);

The marketplace assessment can happen prior to customer acquisition, creating pre-agreements with **cloud service providers** and this can enable **cloud service customers** to select **cloud service providers** from a **service catalogue**, possibly negotiating service details (e.g., service level objectives) at selection time.

In either case, the **cloud service broker** only acts during the contracting phase of the service, between the **cloud service customer** and **cloud service provider**. The **cloud service broker** is not involved during the consumption of the service. In such cases, the **activities** involve **cloud service provider's activities**.

8.4.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service partner** are shown in Figure 8-5.

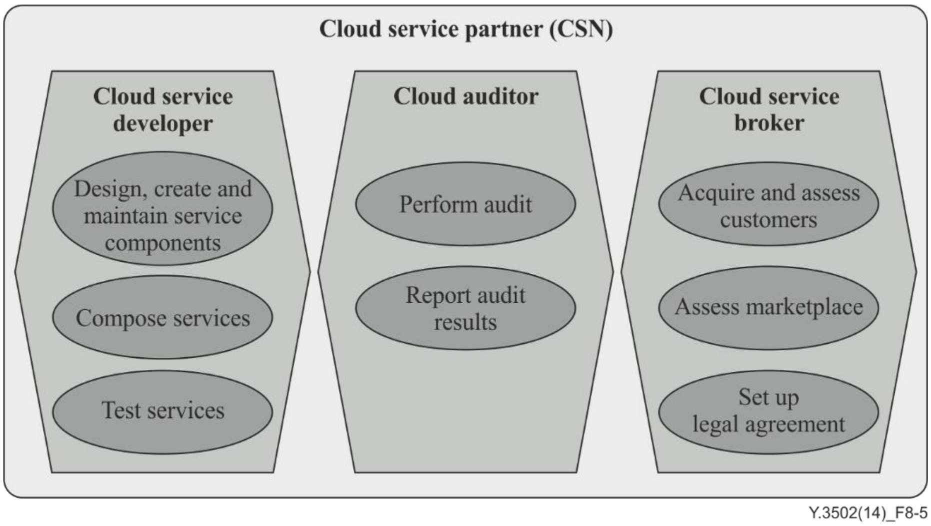


Figure 8-5 – Cloud computing activities related to cloud service partner sub-roles

8.4.2.1 Design, create and maintain service components

The design, create and maintain service components **activity** involves:

- designing and creating software components that are part of the implementation of a service;
- creating the functionality which is offered to users of the service, which also involves connecting the service components to the provider's operational support systems, so that the service implementation can be monitored and controlled;
- processing problem reports relating to the operation of a service implementation;
- providing fixes to service implementations;
- providing enhancements to service implementations.

8.4.2.2 Compose services

The compose services **activity** focuses on composing services using existing services. This **activity** involves:

- creating service functionality by means of composing together one or more existing services provided elsewhere;
- describing the technical aspects of the service (functional interfaces, **SLAs**,…);
- designing an interface to the **cloud service customer** representing the composed services from across multiple **cloud service provider** offerings;
- performing composition which can involve intermediation, aggregation or arbitrage of the existing services.

8.4.2.3 Test services

The test services **activity** focuses on testing the components and services created by the cloud service developer. This **activity** involves:

- performing tests of the components that make up a service implementation to assure that they perform the functionality of the service completely and correctly;
- ensuring **interoperability** with the **cloud services** provided by a **peer cloud service provider**;
- testing which should include checking that the connections to the **cloud service provider's** operational support systems operate correctly – as a result, it is typically necessary to perform some of the testing in a test area of the **cloud service provider's** data centre.

8.4.2.4 Perform audit

The perform audit **activity** involves:

- requesting or obtaining audit evidence;
- conducting any required tests on the system being audited;
- obtaining evidence programmatically, through a set of interfaces provided by the system being audited;

- redacting the evidence, if necessary, in order to protect sensitive information or information subject to regulatory control (e.g., **PII**);
- comparing the obtained audit evidence against the audit criteria as described by the audit scheme or standard that is being used.

The type of audit evidence required and the criteria used to evaluate it are determined by the audit scheme or standard being used. Examples include data relating to security controls and performance data for particular services. In addition to obtaining data, the perform audit **activity** can be asked to evaluate the services provided by a **cloud service provider** which includes security controls, privacy impact, performance, and other **cloud service** related **cloud computing activities** identified by the audit requester. The request can come from the **cloud service provider** itself, where the **cloud service provider** wants proof of the quality of its **cloud services** which can then be presented to potential **cloud service customers**.

8.4.2.5 Report audit results

The report audit results **activity** involves providing a documented report of the results of performing an audit, for example on a given **cloud service** or on a **cloud service provider** or on a **cloud service customer's** use of a **cloud service**. The form of the documented report can be prescribed by the audit scheme that is being used. The results of the audit might be given to the **cloud service provider**, or possibly on request to a **cloud service customer**, depending on the business situation or the legal context.

8.4.2.6 Acquire and assess customers

The acquire and assess customers **activity** includes the tasks required to market and sell **cloud services** up to the point where a **cloud service customer** agrees a contract to use one or more services. This **cloud computing activity** includes:

- providing information to potential customers about available services and associated **SLAs** and contract terms;
- negotiating terms and prices with customers;
- assessing the customer's needs and requirements for **cloud services**.

NOTE – The **cloud service customer** needs assessment activity includes the actions taken to determine and address the **cloud service customer**'s requirements as identified by a gap analysis performed by looking at the customer's current capabilities and their desired future capabilities.

8.4.2.7 Assess marketplace

The assess marketplace **activity** focuses on assessing the current **cloud services** marketplace to find **cloud service** (s) that meet the customers' requirements. This **cloud computing activity** includes:

- surveying the product offerings of **cloud service providers**, obtaining both technical and business information;
- subscribing to and receiving notifications of changes to the content of **cloud service providers' product catalogues**.
- matching the product offerings to the customer's needs and requirements, including technical, business and regulatory aspects.

8.4.2.8 Set up legal agreement

The set up legal agreement **activity** concerns the service agreement between the **cloud service customer** and the chosen **cloud service provider**(s). This involves negotiating the service agreement between the **cloud service customer** and the chosen **cloud service provider**(s), aiming to meet the customer's needs.

8.5 Cross-cutting aspects

8.5.1 General

Cross-cutting aspects include both architectural and operational considerations. Cross-cutting aspects apply to multiple elements within the description of the CCRA or in connection with its operation as an instantiated system. These cross-cutting aspects are shared issues across the **roles**, **activities** and **functional components**. For example, security is a cross-cutting aspect because it applies to infrastructure, services, **cloud service providers**, **cloud service customers** and **cloud service partners** (**cloud auditors**, cloud service developers etc.). All of these need to be secured, but how they are secured is different based on what is being secured. So, securing infrastructure and infrastructure services is very different from securing software services.

Some cross-cutting aspects can apply to other cross-cutting aspects, for example, governance applies to functional elements as well as to the cross-cutting aspects of performance and security.

Cross-cutting aspects often affect the **cloud computing activities** performed by **roles**. **Roles** can coordinate supporting a cross-cutting aspect amongst themselves and their **cloud computing activities**. Supporting cross-cutting aspects also needs **functional components** to provide support for **cloud computing activities**, technical capabilities and implementations.

For each cross-cutting aspect, a set of **cloud computing activities** and **functional components** are defined to support them. Different **roles** and solutions can use different subsets of these.

Cross-cutting aspects include:

- auditability (clause 8.5.2);
- **availability** (clause 8.5.3);
- governance (clause 8.5.4);
- **interoperability** (clause 8.5.5);
- maintenance and versioning (clause 8.5.6);
- performance (clause 8.5.7);
- portability (clause 8.5.8);
- protection of **personally identifiable information** (clause 8.5.9);
- regulatory;
- resiliency (clause 8.5.10);
- **reversibility** (clause 8.5.11);
- security (clause 8.5.12);
- service levels and **service level agreement** (clause 8.5.13).

8.5.2 Auditability

Auditability is the capability of collecting and making available necessary evidential information related to the operation and use of a **cloud service**, for the purpose of conducting an audit. Related to the governance of **cloud services** is the assurance that those services are provided and used in consistency with the associated service agreements between the **cloud service customers, cloud service providers and cloud service partners**. This assurance is most often achieved by means of independent audits of services. An audit typically consists of an audit report or audit certification made available to the parties of the associated service agreements: the **cloud service customers**, the **cloud service providers** and the **cloud service partners**.

The audit itself depends upon data and evidence being available, relating to the usage, environment, **availability** and performance of services and associated resources. Such data and evidence includes records and logs of activities and conditions of the operational environments of all parties of the governing agreements. These records and logs need to be collected and maintained in a secure manner.

8.5.3 Availability

Availability is the property of being accessible and usable upon demand by an authorized entity. The "authorized entity" is typically a **cloud service customer**.

8.5.4 Governance

Governance is the system by which the provision and use of **cloud services** are directed and controlled.

The term internal cloud governance is used for the application of design-time and run-time policies to ensure that **cloud computing** based solutions are designed and implemented, and **cloud computing** based services are delivered according to specified expectations. These expectations can cover any or all of the cross-cutting aspects.

The individual governance practices used by **cloud service customers** and **cloud service providers** exist on a continuum from simple to sophisticated and are encapsulated within their **role**. It is the responsibility of each **role** to implement governance according to their needs. Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with **SLAs** and other contractual elements of the **cloud service customer** to **cloud service provider** relationship.

The term external cloud governance is used for some form of agreement between the **cloud service customer** and the **cloud service provider** concerning the use of **cloud services** by the **cloud service customer**. The agreement can make reference to a **service level agreement** which provides detailed information about functional and non-functional aspects of the services.

8.5.5 Interoperability

Interoperability in the context of **cloud computing** includes the ability of a **cloud service customer** to interact with a **cloud service** and exchange information according to a prescribed method and obtain predictable results. Typically, **interoperability** implies that the **cloud service** operates according to an agreed specification, one that is possibly standardized. The **cloud service customer** should be able to use widely available ICT facilities in-house when interacting with **cloud services**, avoiding the need to use proprietary or highly specialized software.

Interoperability also includes the ability for one **cloud service** to work with other **cloud services**, either through a CSP:inter-cloud provider relationship, or where a **cloud service customer** uses multiple different **cloud services** in some form of composition to achieve their business goals.

Interoperability stretches beyond the **cloud services** themselves and also includes the interaction of the **cloud service customer** with the **cloud service** management facilities of the **cloud service provider**. Ideally, the **cloud service customer** should have a consistent and interoperable interface to the **cloud service** management functionality and be able to interact with two or more **cloud service providers** without needing to deal with each provider in a specialized way.

Standards are implemented in order to support **interoperability** between components or to support the portability of data or of program components. The implementations should support the evolution of the standards used, both from an earlier version of a standard to a later version, or from one standard to a different one, while minimizing disruptive changes.

8.5.6 Maintenance and versioning

A significant item relating to governance is the maintenance of services and underlying resources. Maintenance can take place for a variety of reasons, including the need to fix faults and also the need to upgrade or extend facilities for business reasons. Maintenance actions can have the effect of changing the behaviour of **cloud services** – in particular changes can affect how a service operates when used by a customer.

It is important to distinguish between maintenance performed by the **cloud service provider** and maintenance performed by the **cloud service customer**. In the case of an **SaaS** service, it is likely that virtually all maintenance actions will be performed by the provider. In the case of **IaaS** and **PaaS** services, the application components belong to the **cloud service customer** and the **cloud service customer** is responsible for the maintenance of those components. The provider is responsible for the environment in which the application components run, which varies depending on the details of the service, but which might include such elements as the hardware resources, operating system or middleware.

On the one hand, it can be in the customer's interests that a service or service platform be upgraded or fixed. On the other hand, any changes to the behaviour of a service can have a negative impact on the customer, possibly requiring changes to application components and to customer ICT systems or calling for retraining of customer service users. As a result, it is important that maintenance of services is subject to governance practices that are transparent to the customer.

Maintenance practices should be documented in the **SLA** for the **cloud services** and should include the capability for the customer to report problems and request fixes and also a mechanism for the **cloud service provider** to notify the customer of pending maintenance changes and their schedule.

Versioning is the appropriate labelling of a service (or of components of a service, such as the operating system level used in an **IaaS** service), so that it is clear to the customer that a particular version is in use. It is important that the service be given a new version label when maintenance of a **cloud service** occurs.

Where significant changes are made to a service between two versions, the older version of the service should be available in parallel with the new versions for an agreed period of time.

8.5.7 Performance

Performance includes a set of non-functional facets relating to the operation of a **cloud service** such as:

- **availability** of the service;
- response time to complete service requests;
- transaction rate at which service requests are executed;
- latency for service requests;
- data throughput rate (input and output);
- number of concurrent service requests (scalability);
- capacity of data storage;
- (for **IaaS** and **PaaS**) the number of concurrent execution threads available to an application;
- (for **IaaS** and **PaaS**) the amount of memory (RAM) available to the running program;
- data centre network IP address pool and/or VLAN range capacity.

Where the service involves running an application (**IaaS**, **PaaS**), the same facets of performance apply to the behaviour of the application running in the **cloud service provider**'s environment.

Depending on the charging model, the ability of the **cloud service** to scale its use of resources in accordance with the terms of the **SLA** can also be an important facet of performance. Performance should have metrics defined in the **SLA** for each performance condition identified and these metrics should be monitored during operation of the **cloud service** to ensure that the service meets the performance terms of the **SLA**.

8.5.8 Portability

Portability is significant in **cloud computing** since prospective **cloud service customers** are interested in avoiding lock-in when they choose to use **cloud services**. **Cloud service customers** need to know that they can move **cloud service customer data** or their applications between multiple **cloud service providers** at low cost and with minimal disruption. The amount of cost and disruption that is acceptable can vary based upon the type of **cloud service** that is being used.

For example if a **cloud service customer** organization is considering moving from one **IaaS cloud service provider** to another, the **cloud service customer** should be able to take its data and the virtual machine (VM) image and get it up and running on an equivalent **IaaS** service in a relatively straightforward manner. In an **SaaS** environment, when a **cloud service customer** organization wants to move an **SaaS** application to a different **cloud service provider** (i.e., switch **SaaS** service providers), the **cloud service customer** needs to be able to take their data with them, but the rest of the switching cost will include exporting, mapping and importing the data into the new **cloud service provider**'s **SaaS** application, and that cost is a function of how well the data models and formats of the two **SaaS cloud service providers** line up. Ideally, **SaaS cloud service providers** should adopt standard data interchange format(s) relevant to their application domain. Changing between **SaaS** applications can also involve the **cloud service customer** adapting to a new service interface (which relates to the **interoperability** of the service).

However, since different **cloud capabilities types** can have different requirements related to portability, it is more useful to focus on specific types of portability such as **cloud data portability** and **cloud application portability**.

Cloud service customer data is a class of data objects under the control of the **cloud service customer**. **Cloud data portability** allows the **cloud service customers** the ability to copy **cloud service customer data** into or out of a **cloud service** through network access or by physical transfer of storage devices.

Cloud application portability allows the migration of items such as a fully-stopped virtual machine instance or a machine image (**IaaS** service) from one **cloud service provider** to another **cloud service provider**, or the migration of application components (**PaaS** service) from one **cloud service provider** to another. In both cases, there is a related aspect of the support of portability of metadata relating to the application components, providing information about the relationships of program components and about the required infrastructure for the program components (e.g., load balancing configuration, firewall settings).

8.5.9 Protection of personally identifiable information (PII)

Cloud service providers should protect the assured, proper and consistent collection, processing, communication, use and disposition of **personally identifiable information (PII)** in relation to **cloud services**.

According to established guidelines, one of an organization's key business imperatives is to ensure the protection of **personally identifiable information (PII)**. Though **cloud computing** provides a flexible solution for shared resources, software and information, it also poses additional **confidentiality** challenges to **cloud service customers** using **cloud services,** and also for **cloud service providers**.

In many jurisdictions, there are strict rules and regulations applied to the handling of **PII** – any use of **cloud services** to store and process **PII** often has to conform to those rules and regulations.

Statutory, regulatory and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both **cloud service customers** and **cloud service providers**. Compliance with such requirements is often related to governance and risk management **activities**.

8.5.10 Resiliency

Resiliency is the ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.

Resiliency describes the set of monitoring, preventive and responsive processes that enable a **cloud service** to provide continuous operations, or predictable and verifiable outages, through failure and recovery actions. These can include hardware, communication and/or software failures, and can occur as isolated incidents or in combination, including serial failure. These processes can include both automated and manual actions, usually spanning multiple systems, and thus their description and realization are part of the overall cloud infrastructure, not an independent function.

Inherent in resiliency is the realization of risk management – since resiliency is determined by the least resilient component in the system, and cost/performance or other factors can limit the extent to which resiliency is possible or practical. The association of risk to value is realized in the implementation choices to provide resiliency.

8.5.11 Reversibility

Reversibility is a term which applies to the process for **cloud service customers** to retrieve their **cloud service customer data** and application artefacts and for the **cloud service provider** to delete all **cloud service customer data,** as well as contractually specified **cloud service derived data** after an agreed period. The principle is the "right to be forgotten", in that the **cloud service customer** has a right to expect that once they indicate to the **cloud service provider** that their use of the service(s) will cease, there will be an orderly process for the **cloud service customer** to retrieve **cloud service customer data** and their application artefacts and that the **cloud service provider** will delete all copies and not retain any materials belonging to the **cloud service customer** after an agreed period.

The activity related to **reversibility** will in most cases involve a series of steps, typically requiring the **cloud service customer** to retrieve their data and inform the **cloud service provider** that the **cloud service provider** can delete their copies of the **cloud service customer data** – safeguarding backup copies until that point in case of failures in the exit process. These steps would also necessarily apply to any peer services that are used by the **cloud service provider** to support the **cloud service provider**'s services.

8.5.12 Security

8.5.12.1 General

It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all views of the reference model, ranging from physical security to application security. Therefore, security in **cloud computing** architecture is not solely a cross-cutting aspect under the control of **cloud service providers**, but also affects **cloud service customers**, **cloud service partners** and their **sub-roles**.

Cloud computing systems can address security requirements such as authentication, authorization, **availability**, **confidentiality**, non-repudiation, identity management, **integrity**, audit, security monitoring, incident response, and security policy management. This clause describes **cloud computing** specific perspectives to help analyse and implement security in a **cloud computing** system.

Security capabilities for **cloud services** include: access control, **confidentiality**, **integrity** and **availability**. Security for **cloud computing** is described in detail in other specifications.

Security capabilities also include the management and administration functions which are used to control **cloud services**, underlying resources and the use of **cloud services**, with particular attention applied to access control for users of these functions. This is in addition to:

- facilities to enable early detection, diagnosis and fixing of **cloud service** and resource related problems;
- secure logging of access records, activity reports, session monitoring and packet inspections on the network;
- provision of firewalling, and malicious attack detection and prevention for the **cloud service providers**' systems. One user should not be able to disrupt other users' use of **cloud services**.

Intranet level security should be provided on the network connecting the **cloud service customer** to the **cloud service provider** (for example, through the use of VPN capabilities).

Security measures in **cloud computing** exist to address a series of threats that relate to the use of **cloud services** by **cloud service customers**, which affect both **cloud service customers** and **cloud service providers**. These threats are more fully described in other specifications, such as ISO/IEC 27018.

8.5.12.2 Distribution of security responsibilities

A **cloud service provider** and a **cloud service customer** have differing degrees of control over the computing resources in a **cloud computing** system. Compared to traditional information technology systems, where one organization has control over the whole stack of computing resources and the entire life cycle of the systems, **cloud service providers** and **cloud service customers** collaboratively design, build, deploy and operate **cloud computing** systems.

The split of control means that both **roles** now share the responsibilities of providing adequate protections to the **cloud computing** systems. Security is a shared responsibility. Security controls, i.e., measures used to provide protections, need to be analysed to determine which **role** is in a better position to implement such controls. This analysis needs to include considerations from a service category perspective, where different **cloud service categories** imply different degrees of control between **cloud service providers** and **cloud service customers**. It is important to provide a clear definition of the responsibilities of both the customer and the provider and to ensure that all aspects of security are covered, to avoid responsibility ambiguity.

For example, account management controls for initial system privileged users for an **IaaS** service are typically performed by the **IaaS cloud service provider;** meanwhile, application user account management for the application deployed to that **IaaS** service is typically the responsibility of the **cloud service customer** who deploys the application using the **IaaS** service. By contrast, for an **SaaS** application service, the account management controls for all types of users are in the hands of the **cloud service provider** (although the **cloud service customer** can provide capabilities such as third-party authentication).

8.5.12.3 Cloud service category perspectives

A **cloud service category** defined in Rec. ITU-T Y.3500 | ISO/IEC 17788 is a group of **cloud services** that possess a common set of qualities. **Cloud service categories** present **cloud service customers** with different types of service management operations and expose different entry points into **cloud computing** systems, which in turn also create different attack surfaces for adversaries. Hence, it is important to consider the impact of **cloud service categories** and their different issues in security design and implementation.

For example, **SaaS** provides users with accessibility of **cloud computing** offerings using a network connection, possibly over the Internet and through a web browser. There has been an emphasis on web browser security in **SaaS cloud computing** system security considerations. CSC:cloud service users of **IaaS** services are typically provided with virtual machines (VMs) that are executed on hypervisors on the hosts; therefore, hypervisor security for achieving VM isolation has been studied extensively for **IaaS cloud service providers** that use virtualization technologies.

8.5.12.4 Implications of cloud deployment models

The different **cloud deployment models** have important security implications. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of **tenants** in the deployment model. A **private cloud** is dedicated to one **cloud service customer** organization, whereas a **public cloud** could have **tenants** from many different organizations co-existing with each other.

Another way to analyse the security impact of **cloud deployment models** is to use the concept of access boundaries. For example, an on-site **private cloud** system can or cannot need additional boundary controllers at the **cloud service** boundary when the **private cloud** system is hosted on site within the **cloud service customer** organization's network boundary, whereas an outsourced **private cloud** tends to require the establishment of such perimeter protection at the boundary of the **cloud services**.

8.5.12.5 Data protection strategy and responsibility

Protection of data assumes a new dimension in **cloud computing**. An organization can opt to store its data in a **cloud service** but then the data protection responsibility and accountability needs to be agreed upon clearly. The first step that the **cloud service customer** takes is to properly catalogue the data and identify its sensitivity and the risk to the business of its leakage, loss or corruption. (See ISO/IEC 27002 as a reference for how to identify the sensitivity of data).

Ideally, it should be the **cloud service customer's** responsibility to secure the data before it is moved to a **cloud computing** system. However, the provider would be accountable for any data tampering or theft. Encryption is a potential technique to use but then key management has to be given consideration where the **cloud service customer** or any third party manages the keys. If the keys are managed by the **cloud service provider** then they are responsible for the logical and physical control of the keys, as well as the data.

8.5.13 Service levels and service level agreements

Service level agreements are important components of **cloud computing** governance and represent measurable elements needed to assure an agreed upon quality of service between a **cloud service customer** and a **cloud service provider**.

The **cloud computing service level agreement** (cloud **SLA**) is a **service level agreement** between a **cloud service provider** and a **cloud service customer** based on a taxonomy of **cloud computing** specific terms to set the quality of the cloud services delivered. It characterizes the quality of the **cloud services** delivered in terms of:

- a set of measurable properties specific to **cloud computing** (business and technical);
- a given set of **cloud computing roles** (**cloud service customer** and **cloud service provider** and related **sub-roles**).

For instance, **cloud service customers** need a cloud **SLA** to specify the technical performance requirements of one or more **cloud services**. A cloud **SLA** can cover terms regarding the quality of service, security, performance and remedies for failures to meet the terms of the **SLA**. A **cloud service provider** can also list within the cloud **SLA** a set of promises explicitly not made to **cloud service customers**, i.e., limitations and obligations that **cloud service customers** need to accept. A cloud **SLA** should define the classification of data objects (i.e., **cloud service customer data**, **cloud service provider data**, and **cloud service derived data**), who has access and control of data objects in these data classifications and how they will be used.

The **service level agreement** should specify information relating to the **availability** of the services, the **confidentiality** and **integrity** of the services and the access controls which apply to the services. The **service level agreement** should specify how any **personally identifiable information** will be handled in relation to the **cloud service**s.

The service agreement – alternatively known as the master service agreement (MSA), terms of service (ToS), terms and conditions (T&C), or simply "the contract" – is the higher order document in agreements between parties and the **service level agreement** (**SLA**) is subservient. This is an important distinction because the **SLA** acronym is frequently, and incorrectly, used to reference the contractual relationship as a whole – a **role** that an **SLA** alone is incapable of performing. The service agreement addresses the whole of the contractual relationship and therefore contains contractual elements not directly related to **cloud computing**.

9 Functional view

9.1 Functional architecture

The functional architecture for **cloud computing** describes **cloud computing** in terms of a high level set of **functional components**. The **functional components** represent sets of functions that are required to perform the **cloud computing activities** described in clause 8 for the various **roles** and **sub-roles** involved in **cloud computing**.

The functional architecture describes **functional components** in terms of a layering framework where specific types of functions are grouped into each layer and where there are interfaces between the **functional components** in successive layers.

9.1.1 Layering framework

The layering framework used in the CCRA has four layers, plus a set of functions which spans across the layers. The four layers are:

- user layer;
- access layer;
- service layer;
- resource layer.

The functions which span the layers are called the multi-layer functions.

The layering framework is shown diagrammatically in Figure 9-1.

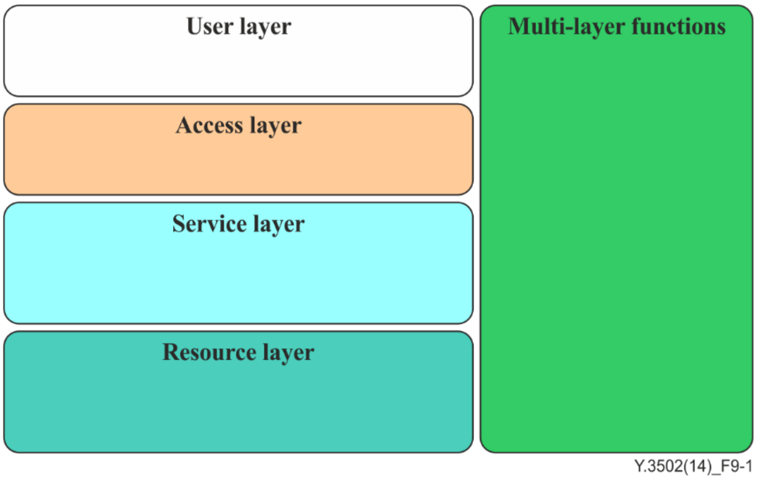


Figure 9-1 – Cloud computing layering framework

Each of the layers in the framework is described in the following subclauses.

9.1.1.1 User layer

The user layer is the user interface through which a **cloud service customer** interacts with **cloud service provider** and with **cloud services**, performs customer related administrative **activities**, and monitors **cloud services.** It can also offer the output of **cloud services** to another resource layer instance.

9.1.1.2 Access layer

The access layer provides a common interface for both manual and automated access to the capabilities available in the services layer. These capabilities include both the capabilities of the services and also the administration and business capabilities.

The access layer is responsible for presenting **cloud service** capabilities over one or more access mechanisms – for example, as a set of web pages accessed via a browser, or as a set of web services which can be accessed programmatically, on secure communication. Another responsibility of the access layer is to apply appropriate security functionality to the access to **cloud service** capabilities. The access layer is responsible for authenticating the request through the use of user credentials and for validating the authorization of the user to use particular capabilities. The access layer is also responsible for handling encryption and checking for request **integrity**, where required.

The access layer can also be responsible for enforcing QoS policies on the traffic coming from the user layer (e.g., service requests to the **cloud service provider**) and the traffic towards the user layer (e.g., output of **cloud services**).

The access layer passes on validated requests to the components in the services layer. The access layer accepts **cloud service customer** or **cloud service provider**'s **cloud service** consumption requests to access **CSP**s' services and resources.

9.1.1.3 Service layer

The service layer contains the implementation of the services provided by a **cloud service provider**. The service layer contains and controls the software components that implement the services (but not the underlying hypervisors, host operating systems, device drivers, etc.), and arranges to offer the **cloud services** to users via the access layer.

The service implementation software in the service layer in turn relies upon the capabilities available in the resource layer to provide the services that are offered and to ensure that the requirements of any **SLA** relating to the services are met, for example, through the use of sufficient resources.

9.1.1.4 Resource layer

The resource layer is where the resources reside. This includes equipment typically used in a data centre such as servers, networking switches and routers, storage devices, and also the corresponding non-cloud-specific software that runs on the servers and other equipment such as host operating systems, hypervisors, device drivers and generic systems management software.

The resource layer also represents and houses the cloud transport network functionality which is required to provide underlying network connectivity between the **cloud service provider** and the users, as well as within the **cloud service provider** and between **peer cloud service providers**.

Note that for a **cloud service provider** to provide services consistent with the **SLA**, it can require dedicated and/or secure connections between users and the **cloud service provider**.

9.1.1.5 Multi-layer functions

The multi-layer functions include a series of **functional components** that interact with **functional components** of the above four other layers to provide supporting capabilities including and not limited to:

- operational support systems capabilities (runtime administration, monitoring, provisioning and maintenance);
- business support systems capabilities (**product catalogue**, billing and financial management);
- security systems capabilities (authentication, authorization, auditing, validation, encryption);
- integration capabilities (linkage of different components to achieve the required functionality);
- development support capabilities (involving the creation, testing and life-cycle management of services and service components).

9.2 Functional components

This clause describes the cloud architecture in terms of the common set of **cloud computing functional components**. A **functional component** is a functional element of the CCRA which is used to perform an **activity** or some part of an **activity** and which has an implementation artefact in a concrete realization of the architecture, e.g., a software component, a subsystem or an application.

Figure 9-2 presents a high level overview of the CCRA **functional components** organized by means of the layering framework.

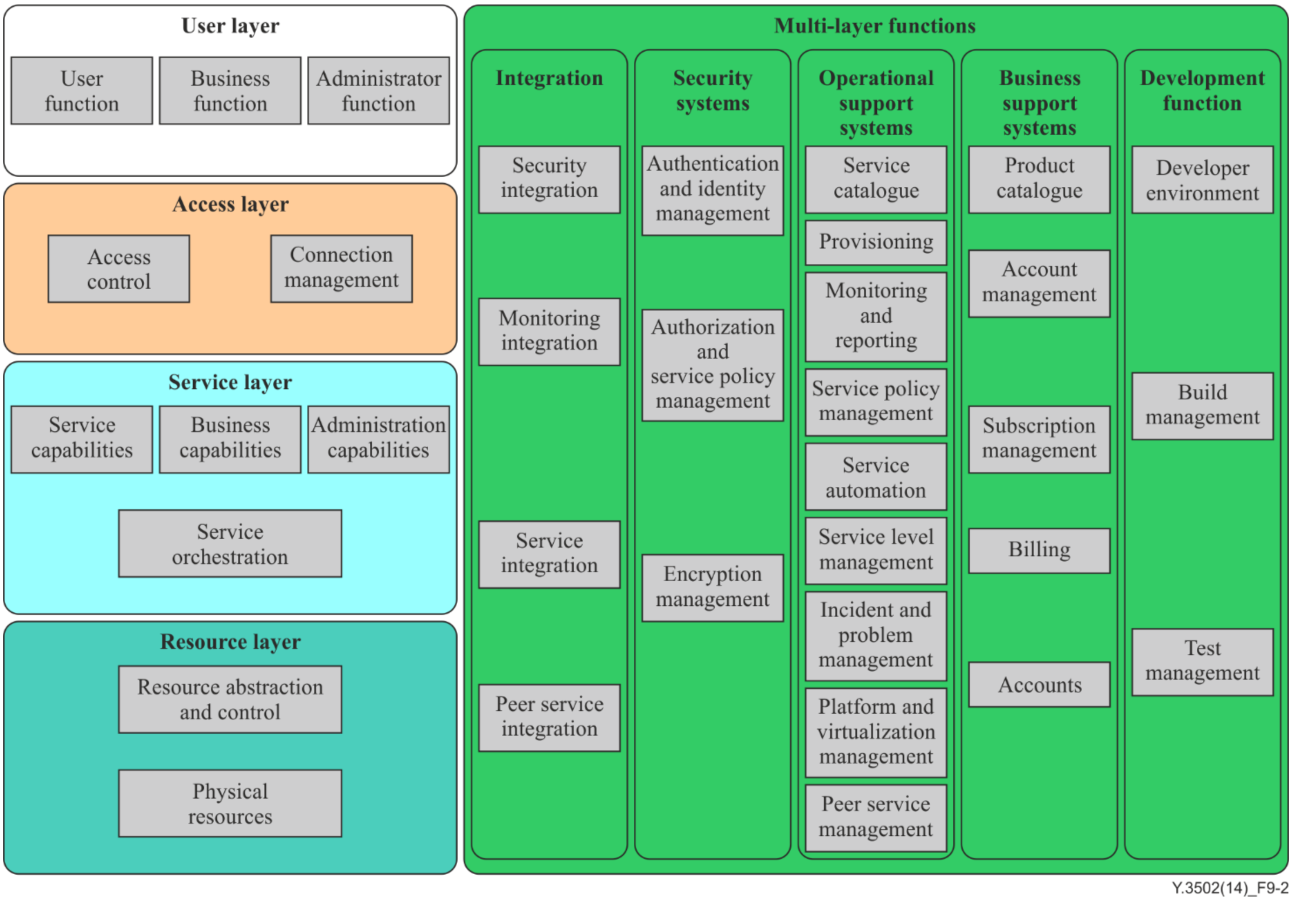


Figure 9-2 – Functional components of the CCRA

9.2.1 User layer functional components

The user layer **functional components** include:

- user function;
- business function;
- administrator function.

The **cloud services** that are presented to CSC:cloud service users can be broken down into two major categories, functional services and self-service management services. The latter can be further divided into business and administration services.

The interface that is presented to the user of the **cloud service** encompasses the primary function of the **cloud service**. This is distinct from the interface that is used to manage the use of the **cloud service**. But all cases are **cloud services**, tailored for different types of capabilities.

9.2.1.1 User function

The user function **functional component** supports the CSC:cloud service user to access and use **cloud services** (the ***use service*** **activity**). In some cases, the user function **functional component** could be as simple as a browser running on a user device. However, in other cases, it might involve a sophisticated enterprise system running business processes, applications, middleware and associated infrastructure.

9.2.1.2 Business function

The business function **functional component** supports the **cloud computing activities** of the CSC:business manager including the selection and purchase of **cloud services**; the accounting and financial management relating to the use of **cloud services**. It should be noted that business capabilities are themselves offered via **cloud services**.

9.2.1.3 Administrator function

The administrator function **functional component** supports the **cloud computing activities** of the CSC:cloud service administrator. This includes functions for the administration of user identities and profiles, the monitoring of service activity and usage, event handling and problem reporting. Cloud administration capabilities are only accessed using **cloud services**.

9.2.2 Access layer functional components

Figure 9-3 shows the access layer **functional components** which include:

- access control:
  - service access;
  - business access;
  - administration access;
  - development access.
- connection management.

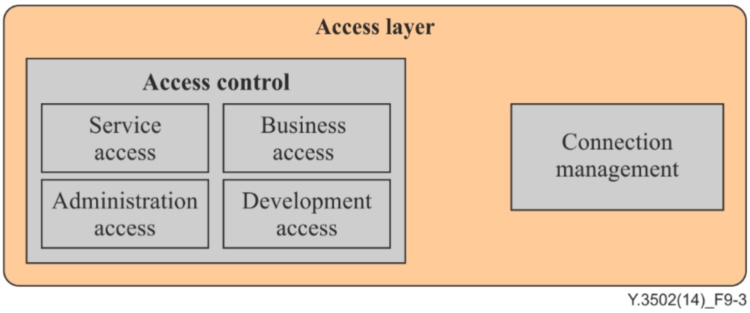


Figure 9-3 – Access layer functional components

9.2.2.1 Access control

Access control limits users to the use of particular services. Principally, access control involves the authentication of a user through the presentation and validation of credentials, followed by the authorization of this authenticated user to use specific services. Associated with this is identity management.

Access control for **cloud services**, the resources they depend on, and the related control functions should be provided.

9.2.2.2 Service access

The service access **functional component** provides access to the **cloud services** offered by the **cloud service provider**.

9.2.2.3 Business access

The business access **functional component** provides access to business capabilities offered by the **cloud service provider**, as implemented by the business support systems.

9.2.2.4 Administration access

The administration access **functional component** provides access to administration capabilities offered by the **cloud service provider**, as implemented by the operational support systems.

9.2.2.5 Development access

The development access **functional component** provides access to a set of capabilities within the provider's system that supports the development, test and maintenance of **cloud service** implementations.

9.2.2.6 Connection management

The connection management functional component provides enforcement of QoS policies regarding the traffic from and/or to the user layer **functional components**. The connection management **functional component** interacts with the multi-layer functions to retrieve policies stored there and enforces them locally in the access layer.

9.2.3 Services layer functional components

The services layer **functional components** include:

- service capabilities;
- business capabilities;
- administration capabilities;

- service orchestration.

9.2.3.1 Service capabilities

The service capabilities **functional component** consists of the necessary software required to implement the service offered to **cloud service customers**. It implements the functionality defined by the service interface, i.e., the interface offered to **cloud service customers**, independent of the service implementation.

9.2.3.2 Business capabilities

The business capabilities **functional component** provides a set of capabilities for accessing the business function related to the provision of **cloud services**. The business function itself is contained within the business support systems **functional components**.

9.2.3.3 Administration capabilities

The administration capabilities **functional component** provides a set of capabilities for accessing the administration function related to the provision of cloud services.

The administration function itself is contained within the operations support systems and business support systems **functional components**.

9.2.3.4 Service orchestration

The service orchestration **functional component** provides coordination, aggregation and composition of multiple service components in order to deliver the **cloud service**.

9.2.4 Resource layer functional components

The resource layer **functional components** include:

- resource abstraction and control;
- physical resources.

9.2.4.1 Resource abstraction and control

The resource abstraction and control **functional component** is used by **cloud service providers** to provide access to the physical computing resources through software abstraction. Resource abstraction needs to ensure efficient, secure and reliable usage of the underlying infrastructure. The control feature of the **functional component** enables the management of the resource abstraction features.

The resource abstraction and control **functional component** enables a **cloud service provider** to offer qualities such as rapid elasticity, **resource pooling** and **on-demand self-service**. The resource abstraction and control **functional component** can include software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing.

The resource abstraction and control **functional component** enables control functionality, enabling monitoring and management capabilities implemented in the operational support systems **functional component** (see clause 9.2.5.3). For example, there can be a centralized algorithm to control, correlate and connect various processing, storage and networking units in the physical resources so that together they deliver an environment where **NaaS**, **IaaS**, **PaaS** or **SaaS cloud service categories** can be offered. The controller might decide which CPUs and/or racks contain which virtual machines executing which parts of a given **cloud service**'s workload, and how such processing units are connected to each other, and when to dynamically and transparently reassign parts of the workload to new units as conditions change.

The decision as to whether the physical resources are virtualized or not depends on the workload characteristics to be run. For many **cloud services'** workloads (e.g., related to **Compute as a Service** and **Data Storage as a Service**), it is convenient to virtualize the underlying physical resources, especially since virtualization enables some scenarios which basically cannot be realized with a physical infrastructure (e.g., scenarios related to image management or dynamic scaling of CPU capacity as needed). For other workloads (e.g., analytics and/or search) it is required to have maximum compute capacity and use hundreds or thousands of nodes to run a single specialized workload. In such cases non-virtualized physical resources can be more appropriate.

9.2.4.2 Physical resources

The physical resources **functional component** represents the elements needed by the **cloud service provider** to run and manage the **cloud services** that they offer.

Physical resources include hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and network connectors, storage components (hard disks) and other physical computing infrastructure elements. These resources can include those that reside inside cloud data centres (e.g., computing servers, storage servers, and intra-data centre networks), and those that reside outside of data centres, typically networking resources, such as inter-data centre networks and core transport networks.

All the elements of the physical resources are managed from the operational support systems **functional component**, with the capability to place instances of each **cloud service** onto the resources as required to satisfy customer requirements. Note that typically, the operational support systems **functional component** itself runs on some part of the physical resources.

9.2.5 Multi-layer functions

9.2.5.1 Integration functional components

The integration **functional components** are responsible for connecting **functional components** in the architecture to create a unified architecture. The integration **functional components** provide message routing and message exchange mechanisms within the cloud architecture and its **functional components** as well as with external **functional components**. Message routing can be based on various criteria, e.g., context, policies.

The integration **functional components** include:

- security integration;
- monitoring integration;
- service integration;
- peer service integration.

9.2.5.1.1 Security integration

The security integration **functional component** provides integration to security capabilities including authentication, authorization, encryption and **integrity** verification and to policy mechanisms that relate to security capabilities.

9.2.5.1.2 Monitoring integration

The monitoring integration **functional component** provides connection from **functional components** in the access layer, services layer and resource layer to the monitoring and reporting capabilities of the operational support systems.

9.2.5.1.3 Service integration

The service integration **functional component** provides connections to services running within the provider's environment. The service integration **functional component** is an essential aspect of virtualizing the services so that, for example, their location and implementation details are hidden from the components that depend on those services.

9.2.5.1.4 Peer service integration

The peer service integration **functional component** is used to connect to services of **peer cloud service providers** in a controlled fashion, with appropriate security and with appropriate accounting for the usage, linking back to the identity of the **cloud service customer**. The peer service integration **functional component** also virtualizes the links to the target services, so that the details of those services can change dynamically without impact on the **functional components** that reference the services.

9.2.5.2 Security systems functional components

The security systems **functional components** are responsible for applying security related controls to mitigate the security threats in **cloud computing** environments. The security systems **functional components** encompass all the security facilities required to support **cloud services**.

The security systems **functional components** include:

- authentication and identity management;
- authorization and security policy management;
- encryption management.

9.2.5.2.1 Authentication and identity management

The authentication and identity management **functional component** provides capabilities relating to user identities and the credentials required to authenticate users when they access **cloud services** and their related administration and business capabilities.

Identity management can involve federated identity management to permit users to employ the same identity and credentials to access multiple **cloud services**, providing capabilities such as "single sign-on".

9.2.5.2.2 Authorization and security policy management

The authorization and security policy management **functional component** provides capabilities for the control and application of authorization for users to access specific capabilities or data. Service policy management provides for the definition and application of security policies which relate to **cloud services**.

9.2.5.2.3 Encryption management

The encryption management **functional component** provides capabilities relating to the encryption of data, whether data at rest or data in motion. Encryption key management and encryption scheme selection are some of the capabilities provided.

9.2.5.3 Operational support systems functional components

The operational support systems **functional components** encompass the set of operational related management capabilities that are required in order to manage and control the **cloud services** offered to customers.

The operational support systems **functional components** include:

- **service catalogue**;
- provisioning;
- monitoring and reporting;
- service policy management;
- service automation;
- service level management;
- incident and problem management;
- platform and virtualization management;
- peer service management.

9.2.5.3.1 Service catalogue

The **service catalogue functional component** provides a listing of all the **cloud services** of a particular **cloud service provider**. A **service catalogue** can contain/reference all relevant technical information required to deploy, provision and run a **cloud service**.

9.2.5.3.2 Provisioning

The provisioning **functional component** provides the capabilities for provisioning services, both in terms of the provisioning of service implementations and of access end points and the workflow required to ensure that elements are provisioned in the correct sequence.

9.2.5.3.3 Monitoring and reporting

The monitoring and reporting **functional component** provides capabilities for:

- monitoring the **cloud computing activities** of other **functional components** throughout the **cloud service provider's** system. This includes the **functional components** that are involved in the direct use of **cloud services** by the CSC:cloud service users such as the service access and service implementation (e.g., the invocation of a **cloud service** operation by a particular user). This also includes **functional components** involved in the support of **cloud services**, such as **functional components** in the OSS itself like the service automation **functional component** (e.g., the provisioning of a service instance for a particular customer);
- providing reports on the behaviour of the **cloud service provider**'s system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data);
- storage and retrieval of monitoring and event data as logging records.

There is a need to guarantee the **availability**, **confidentiality** and **integrity** of the logging records held by the monitoring and reporting **functional component**. For multi-tenant **cloud services**, there is also a need to design access to the records so that particular **tenants** can only gain access to information about their own tenancy and about no other tenancy.

9.2.5.3.4 Service policy management

The service policy management **functional component** provides capabilities to define, store and retrieve policies that apply to **cloud services**. Policies can include business, technical, security, privacy and certification policies that apply to **cloud services** and their usage by **cloud service customers**.

Some policies can be general and apply to a **cloud service** irrespective of the customer concerned. Other policies can be specific to a particular customer.

9.2.5.3.5 Service automation

The service automation **functional component** provides capabilities for service delivery including the management and execution of service templates and the orchestration of services. The service automation **functional component** holds the service templates which define the **cloud computing activities** and workflows required to provision and deliver a specific entry in the **service catalogue**.

Cloud service provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Cloud service administration **activities** of the **cloud service customer** can be capable of being automated and need not require any intervention by the **cloud service provider**.

The service automation **functional component** works with the provisioning **functional component** and service integration **functional component** to achieve its goals.

9.2.5.3.6 Service level management

The service level management **functional component** provides capabilities for managing the service levels of a particular **cloud service**, aiming to ensure that the **cloud service** meets the requirements of the **SLA** which applies to the service.

The service level management **functional component** manages the capacity and performance relating to a **cloud service**.

This can involve the application of service policies (e.g., a placement rule which aims to avoid single points of failure).

The service level management **functional component** obtains monitoring information from the monitoring and reporting **functional component** in order to measure and record key performance indicators (KPIs) for the **cloud service**. Capacity is allocated or de-allocated based on the basis of these KPIs.

The service level management **functional component** also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against **cloud service** performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

9.2.5.3.7 Incident and problem management

The incident and problem management **functional component** provides capabilities for the capture of incident or problem reports and managing those reports through to resolution.

Incidents and problems can be detected and reported by the **cloud service provider**'s systems, or they can be detected and reported by **cloud service customers**.

9.2.5.3.8 Platform and virtualization management

The platform and virtualization management **functional component** provides the capabilities for managing the underlying resources of the **cloud service provider** (compute, storage, networking) and for virtualizing the use of those resources (e.g., by means of hypervisors).

The resources are typically organized into resource pools with key characteristics:

- standardized hardware componentry and configuration;
- readily expandable through the additional of new hardware capacity;
- automated shifting of resources as workload needs change;
- protection and isolation of neighbouring workloads and data;
- reduce and/or eliminate downtime through movement of workloads and data between resources;
- manage resource consumption based on goals (e.g., performance, **availability**, licences, energy use).

9.2.5.3.9 Peer service management

The peer service management **functional component** provides capabilities for connecting the provider's operational support systems and business support systems to the administration capabilities and business capabilities of **peer cloud service providers**, in respect of **peer cloud services** that are used by the provider.

The peer service management **functional component** is responsible for establishing the communication path(s) required, and for passing appropriate identity and credentials with requests made to the **peer cloud service providers**.

9.2.5.4 Business support systems components

The business support systems **functional components** encompass the set of business-related management capabilities dealing with customers and supporting processes.

The business support systems **functional components** include:

- **product catalogue**;
- account management;
- subscription management;
- billing;
- accounts.

9.2.5.4.1 Product catalogue

The **product catalogue functional component** provides capabilities for **cloud service customers** to browse a list of available service offerings which they can purchase, plus a set of capabilities for the management of the content of the catalogue which are available to staff of the **cloud service provider**.

Product catalogue entries consist of technical information about each of the service offerings (capabilities provided by the service, interface definitions for the service including available service operations, security information), plus related business information such as pricing or rating.

9.2.5.4.2 Account management

The account management **functional component** provides capabilities for managing **cloud service customer** relationships, including:

- management of contracts;
- subscriptions to **cloud services**;
- entitlements;
- service pricing, which can involve customer-specific terms such as discounts;
- the policies that apply to the treatment of **cloud service customer data**.

The account management **functional component** and its related database(s) are subject to stringent requirements for **availability** and security due to the importance and the sensitivity of the data related to customer accounts.

9.2.5.4.3 Subscription management

The subscription management **functional component** handles subscriptions from **cloud service customers** to particular **cloud services**, aiming to record new or changed subscription information from the customer and ensure the delivery of the subscribed service(s) to the customer.

9.2.5.4.4 Billing

The billing **functional component** has capabilities for:

- the metering and rating of the use of **cloud services** by **cloud service customers** – where metering is the measurement of the consumption of **cloud services** by each **cloud service customer** and rating is the application of pricing schedules to the metering data. The form of the metering data depends on the nature of the **cloud service** and the pricing schedules can involve customer-specific terms (e.g., discounts) and require algorithmic application against the metering data;
- the generation of invoices based on the charges for the use of **cloud services** created by the metering and rating function, and the transmission of the invoices to the **cloud service customers**. Invoice data is also lodged with the accounts **functional component** and the account management **functional component**.

9.2.5.4.5 Accounts

The accounts **functional component** holds the capabilities relating to general ledger and general accounting functions, including accounts receivable and accounts payable. Note that the accounts **functional component** is used for accounting for the **cloud service provider** organization itself and does not deal with the maintenance of individual customer accounts (those are handled by the account management **functional component**).

9.2.5.5 Development support functional components

The development support **functional components** support the **cloud computing activities** of the cloud service developer. This includes support of the development and/or composition of service implementations, build management and test management.

The development support **functional components** include:

- developer environment;
- build management;
- test management.

9.2.5.5.1 Developer environment

The developer environment **functional component** provides the capabilities to support the development of the service implementation software. Development of software components for the service is supported, plus tools which assist in composing the service from a set of other services.

The developer environment **functional component** supports the use of the capabilities provided by the **cloud service provider**'s environment, including connections to resources and network, integration with other services (including services of **peer cloud service providers**), integration with monitoring and management capabilities, integration with security capabilities.

The developer environment **functional component** also supports the creation of configuration metadata relating to the service being developed and also supports the creation of scripts and related artefacts that are used by the provider's operational support systems to provision and configure the service.

9.2.5.5.2 Build management

The build management **functional component** supports the building of a ready-to-deploy software package which can be passed to the **cloud service provider** for deployment into the **cloud service** environment. The software package consists of both the service implementation software and also the configuration metadata and scripts.

9.2.5.5.3 Test management

The test management **functional component** supports the execution of test cases against any build of the service implementation. The test management **functional component** produces reports of the executed tests and these can be communicated to the **cloud service provider** along with a build of the service implementation.

It is typical for testing to be performed in a specialized test environment, which closely approximates to the production environment without interfering with the production environment. For **cloud computing**, the test environment can be made available by the **cloud service provider**.

10 Relationship between the user view and the functional view

10.1 General

As well as specifying the **roles** and **cloud computing activities** view in clause 8 and the functional view including architectural **functional components** in clause 9, this Recommendation | International Standard describes in this clause the logical relationships of the **roles** and **cloud computing activities** to the **functional components**.

Standards can be relevant to some of these relationships. Standards associated with a relationship can be used to (i) specify degrees of information flow or other types of **interoperability**; and/or (ii) ensure specified degrees of quality (e.g., security or service level).

Logical relationships defined in this architecture are a significant part of specifying the CCRA and its behaviour. The relationship describes matters such as the required information flows between the **functional components** in the CCRA.

10.2 Overview

Figure 10-1 provides an overview of the major elements of the CCRA – **roles, cloud computing activities** and **functional components**, in a common configuration.

Figure 10-1 uses the graphical conventions introduced in clause 5. The boxes with continuous rounded edges represent **roles**, the hexagons represent **sub-roles**, the rounded edged dotted boxes represent **cloud computing activities**, and the square ones with bricks are **functional components**. The "L" shaped boxes inside the service capabilities **functional**

component represents the **cloud service** interfaces based on the fundamental **cloud capabilities types**. In Figure 10-1, it is apparent that **roles** are collections of **cloud computing activities**, and **cloud computing activities** themselves are implemented or realized by means of **functional components**.

The proximity of the graphical elements representing roles to each other is meaningful, and represents close interaction between roles assuming neighbouring **roles**. For example, the **cloud service provider role** is at the centre of the diagram to emphasize that it interacts with all other **roles**. The same is true about the positioning of the **cloud computing activities** inside a given **role**, as well as the relative positioning of **functional components** inside a given **activity**. For example, the service capabilities **functional component** is positioned above the resource abstraction and control **functional component**, to signal the dependency of the former on the latter.

The cross-cutting aspects of auditability, **availability**, governance, **interoperability**, maintenance and versioning, performance, portability, protection of **personally identifiable information**, regulatory, resiliency, **reversibility**, security, and service levels and **service level agreement** are indicated by the outermost box in Figure 10-1, which is intended to show that the cross-cutting aspects apply to all the other elements in Figure 10-1 – **roles, activities** and **functional components**. As an example, the CSC:cloud service user must have an identity, along with a set of credentials, which must be given to the user function **functional component** when performing the use cloud service **activity**. The identity and the credentials are presented to the access control **functional component** and authentication and authorization performed as part of the provide services **activity**, invoking the appropriate security **functional component** capabilities before the **cloud service** is provided to the CSC:cloud service user.

The service capabilities **functional component** of Figure 10-1 represents the implementation of the **cloud service** itself.

10.2.1 Service capabilities functional component

The **cloud service** is offered via a service interface and can offer one or more of the **cloud capabilities types**, represented by the "inverted L" shapes within the service capabilities **functional component**. The topmost L shape represents the **application capabilities type**, while the next lower L shape represents the platform capabilities type and the bottom L shape represents the infrastructure capabilities type.

The implication of the L shapes is that an **application capabilities type** can be implemented using the platform capabilities type or not (at the choosing of the **cloud service provider**) and that the platform capabilities type can be implemented using the infrastructure capabilities type or not.

For **SaaS** or **CaaS cloud service categories**, the service capabilities **functional component** contains the application-specific software or the communication applications which are deployed onto the resource layer in such a way that the service levels identified in the **SLA** are achieved.

For other **cloud service categories**, see cloud computing overview and vocabulary in Rec. ITU-T Y.3500 | ISO/IEC 17788.

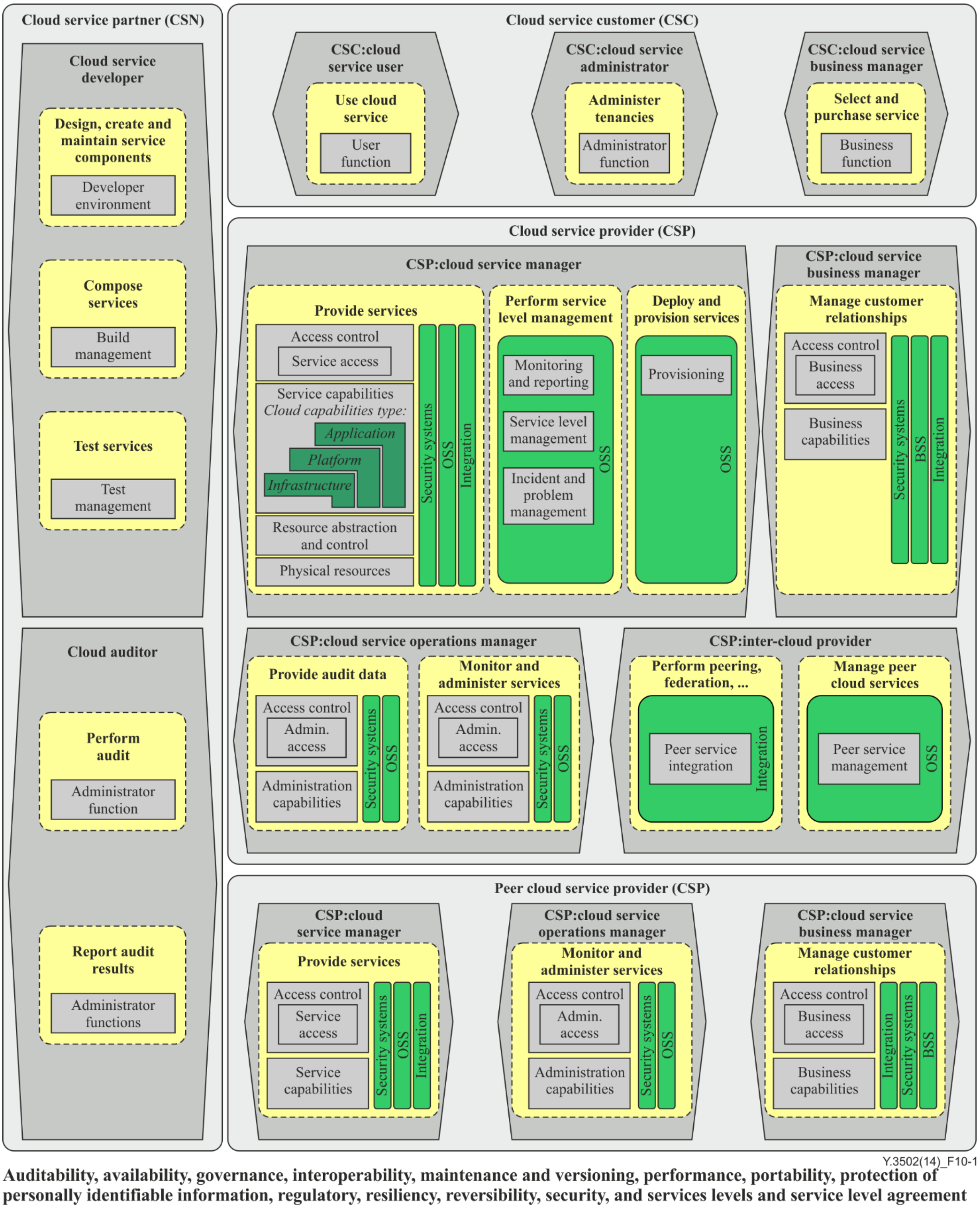

Cloud service partner (CSN)
Cloud service developer
Design, create and maintain service components
Developer environment
Compose services
Build management
Test services
Test management
Cloud auditor
Perform audit
Administrator function
Report audit results
Administrator functions
Cloud service customer (CSC)
CSC:cloud service user
Use cloud service
User function
CSC:cloud service administrator
Administer tenancies
Administrator function
CSC:cloud service business manager
Select and purchase service
Business function
Cloud service provider (CSP)
CSP:cloud service manager
Provide services
Access control
Service access
Service capabilities
Cloud capabilities type:
Application
Platform
Infrastructure
Resource abstraction and control
Physical resources
Security systems
OSS
Integration
Perform service level management
Monitoring and reporting
Service level management
Incident and problem management
OSS
Deploy and provision services
Provisioning
OSS
CSP:cloud service business manager
Manage customer relationships
Access control
Business access
Business capabilities
Security systems
BSS
Integration
CSP:cloud service operations manager
Provide audit data
Access control
Admin. access
Administration capabilities
Security systems
OSS
Monitor and administer services
Access control
Admin. access
Administration capabilities
Security systems
OSS
CSP:inter-cloud provider
Perform peering, federation, ...
Peer service integration
Integration
Manage peer cloud services
Peer service management
OSS
Peer cloud service provider (CSP)
CSP:cloud service manager
Provide services
Access control
Service access
Service capabilities
Security systems
OSS
Integration
CSP:cloud service operations manager
Monitor and administer services
Access control
Admin. access
Administration capabilities
Security systems
OSS
CSP:cloud service business manager
Manage customer relationships
Access control
Business access
Business capabilities
Integration
Security systems
BSS
Y.3502(14)_F10-1
Auditability, availability, governance, interoperability, maintenance and versioning, performance, portability, protection of personally identifiable information, regulatory, resiliency, reversibility, security, and services levels and service level agreement

Figure 10-1 – Common view of roles, cloud computing activities and functional components

10.2.2 Common roles, activities and functional components

In Figure 10-1, the **cloud service provider** has a **sub-role**, CSP:cloud service manager, which performs the provide services **activity**, which provides the service for the CSC:cloud service user of the **cloud service customer** to actually use. But before the service can be used, the **cloud service** needs to be developed and deployed to be operational.

Two **sub-roles** of **cloud service partner** are involved in this case, cloud service developer and **cloud auditor**. The cloud service developer develops the implementation of the **cloud services** using the development tools **functional component** and tests the service using the test management **functional component**. The **cloud service** is then packaged with deployment information and given to the CSP:cloud service manager to perform the deploy and provision services **activity** resulting in a service capabilities **functional component** being offered in the provide services **activity**. The **cloud auditor**, in the meantime, performs the perform audit and report audit results **activities** on the cloud service developer, **cloud service provider** or **cloud service customer** according to the policies and governance regimens of each.

After the CSP:cloud service manager performs the deploy and provision services **activity**, the provide services **activity** uses the service capabilities **functional component**, which is the implementation of the service and which in turn uses the resource layer **functional components** for the compute, storage and network resources required to run the service. The provide services **activity** also involves integrating the service capabilities **functional component** with the security systems **functional component** to provide security and protection of **personally identifiable information** capabilities such as data encryption. The operational support systems **functional component** supports management, monitoring, automation and configuration for the services and resources. In addition, the CSP:cloud service manager performs the perform service level management **activity**. The perform service level management **activity** manages the **availability** and performance of the **cloud service** so that it meets the objectives defined in the **SLA** which applies to the **cloud service**. The service level management **functional component**, the monitoring and reporting **functional component**, and the incident and problem management **functional component** are used to accomplish this.

Sometimes, CSP:cloud service managers provide the service in collaboration with another CSP:cloud service manager, invoking **cloud services** in that **peer cloud service provider**. The CSP:cloud service manager then performs the manage **peer cloud services activity** to set up the contracts and **SLAs** for using the **peer cloud service**. The **peer cloud service provider** also offers administrative and use **cloud computing activities**: the provide services and the perform service level management **cloud computing activities**, just like any other **cloud service provider**.

These are a common set of **cloud computing activities** for a CSP:cloud service manager, but there are additional **cloud computing activities** that could be performed and are documented in this specification.

Once a **cloud service** is available for use, two **cloud service customer sub-roles** perform various activities. First, the CSC:cloud service administrator performs the administer tenancies activity using the administrator function **functional component**, to set up the tenancy and to grant access rights to CSC:cloud service users. Once this is done, CSC:cloud service users perform the use cloud service activity by leveraging the user function **functional component** to interact with the **cloud service**. Meanwhile, the CSC:cloud service administrator typically monitors the service to ensure that it is running correctly and meeting the terms of the **SLA**, again using the administrator function **functional component**.

Figure 10-2 provides a view of **roles**, **cloud computing activities** and **functional components** drawing links between **cloud computing activities** of multiple **roles**. Annex A provides a description of each of these relationships.

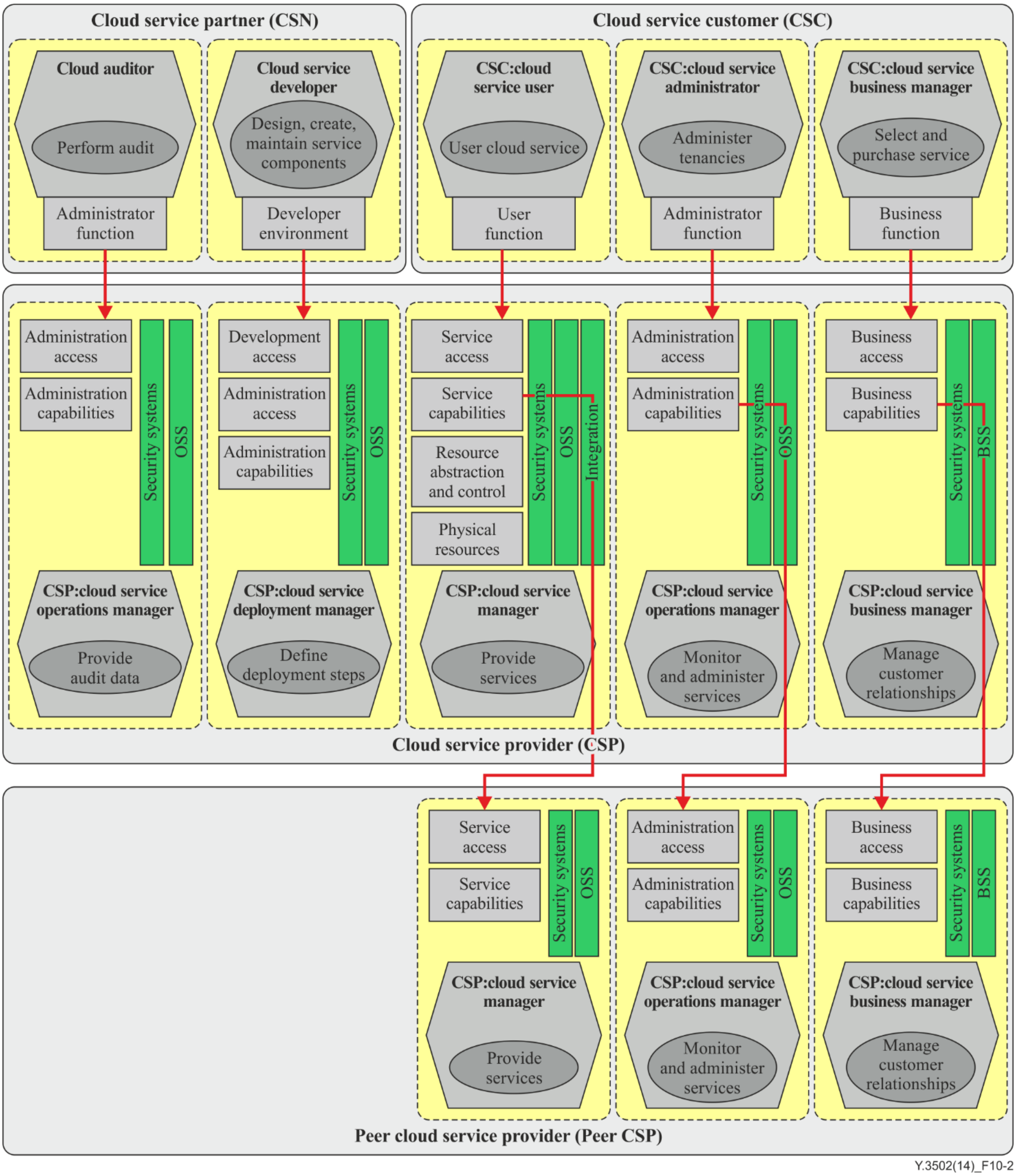

Cloud service partner (CSN)
Cloud service customer (CSC)
Cloud auditor
Perform audit
Administrator function
Cloud service developer
Design, create, maintain service components
Developer environment
CSC:cloud service user
User cloud service
User function
CSC:cloud service administrator
Administer tenancies
Administrator function
CSC:cloud service business manager
Select and purchase service
Business function
Administration access
Administration capabilities
Security systems
OSS
Development access
Administration access
Administration capabilities
Service access
Service capabilities
Resource abstraction and control
Physical resources
Integration
BSS
Business access
Business capabilities
CSP:cloud service operations manager
Provide audit data
CSP:cloud service deployment manager
Define deployment steps
CSP:cloud service manager
Provide services
Monitor and administer services
CSP:cloud service business manager
Manage customer relationships
Cloud service provider (CSP)
Peer cloud service provider (Peer CSP)
Y.3502(14)_F10-2

Figure 10-2 – Examples of relationships and interactions between activities and functional components

10.2.3 Multi-tenancy and isolation

Cloud computing involves the sharing of some resources, and this typically means the sharing of those resources with other customers of the **cloud services** involved. The terms **tenancy** and **multi-tenancy** are used to describe the situation where resources are shared.

A **tenant** of a **cloud service** is not quite the same as a **cloud service customer** – a **tenant** is a group of CSC:cloud service users sharing access to a set of physical and virtual resources. Typically, the group of CSC:cloud service users will be associated with a particular **cloud service customer**, but a **cloud service customer** can well have multiple **tenants** – groups of users from different departments within the customer organization, for example.

Multi-tenancy is the allocation of physical or virtual resources so that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. In other words, the users who belong to one tenancy should be completely unaware of the presence of users from another tenancy.

Multi-tenancy does not only affect the **cloud services** themselves; it also affects the business and administration capabilities offered to **cloud service customers** by the **cloud service provider**. Information about user accounts, subscriptions, usage and billing must all be kept isolated and visible only to the customers who own the related tenancies. Particular care must be taken in relation to resources such as log files, which can contain records relating to multiple **tenants**. If a particular customer needs to access the log records, for example when an incident occurs, then the log records must be filtered so that the customer can only see records relating to its tenancies.

Annex A

Further details regarding the user view and functional view

(This annex forms an informative part of this Recommendation | International Standard.)

This annex provides further details regarding the relationship of the user view and functional view.

A.1 The cloud service customer–cloud service provider relationship

There are three key elements in the **cloud service customer**–**cloud service provider** relationship:

1) the CSC:cloud service user using provider **cloud services** to achieve their business goals;
2) the CSC:business manager using **cloud service provider** business capabilities to subscribe to **cloud services** and manage their use from a business perspective;
3) the CSC:cloud service administrator using the **cloud service provider** administration capabilities to administer the use of the **cloud services** from the **cloud service customer** perspective.

A.1.1 Functional relationship

The **cloud service** is made available to CSC:cloud service users via an end point and interface enabled by the service access **functional component**. The functions of this interface and the associated information flows are domain specific to the **cloud service** and are thus not in the scope of the reference architecture. However, there are some broad aspects that should be reflected in the service interface, in particular the need to identify and authenticate the CSC:cloud service user.

The CSC:cloud service user performs the use cloud service **activity** through the user function **functional component**, which then invokes the **cloud service** through the service access **functional component**. The service access **functional component** performs any authentication of the CSC:cloud service user and establishes authorization to use particular capabilities of the **cloud service**. If authorized, the service access **functional component** invokes the **cloud service** implementation which performs the request.

Figure A.1 illustrates the **functional component** relationships involved in the use **cloud service activity** of the CSC:cloud service user.

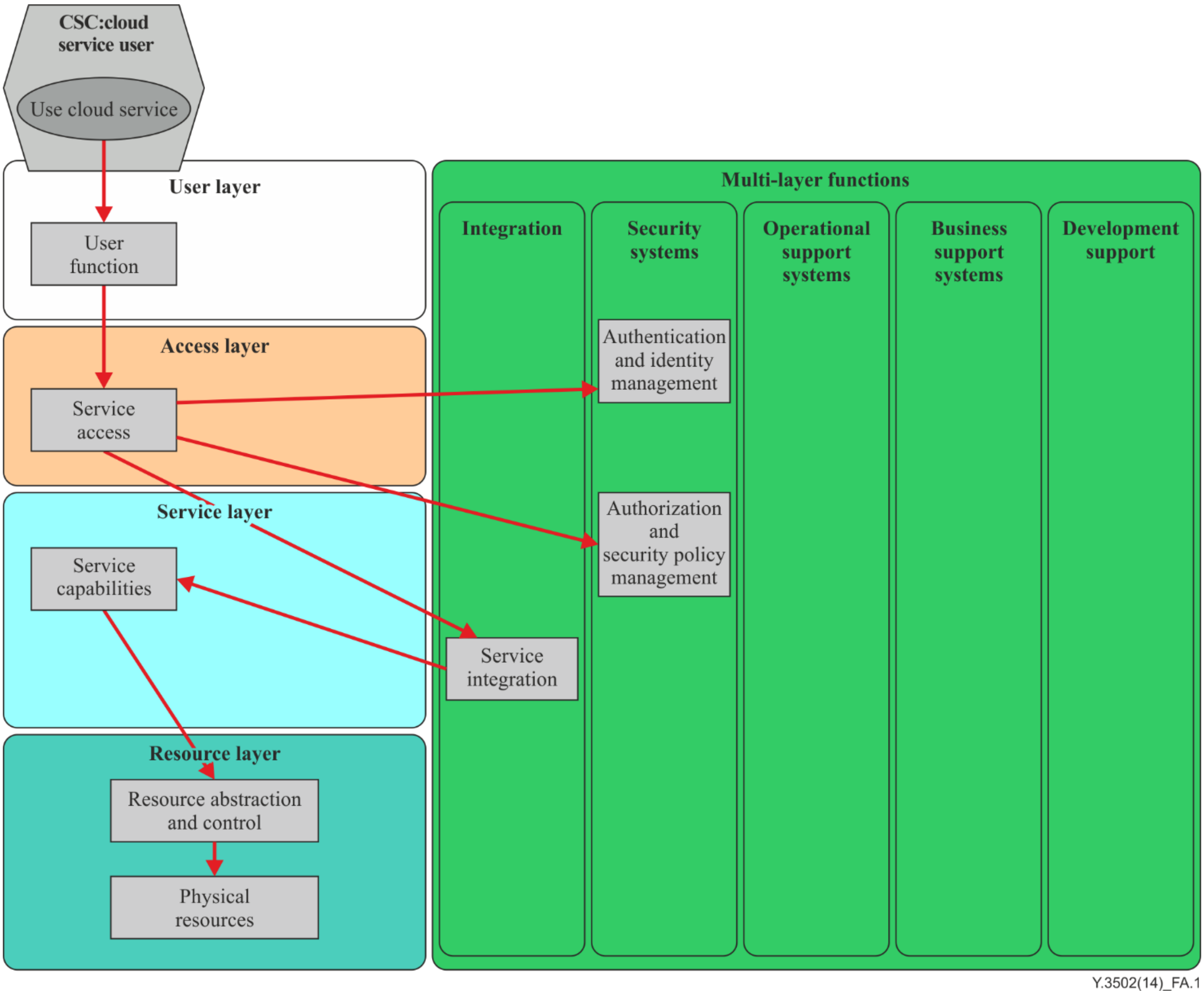


Figure A.1 – CSC:cloud service user relationship for the "use cloud service" activity

A.1.2 Business relationship

The CSC:cloud service business manager performs the **cloud computing activities** select and purchase service, perform business administration and request audit report through the business function **functional component** of the user layer. The business function **functional component** invokes the business capabilities of the **cloud service provider** through an end point and interface enabled by the business access **functional component**.

The business access **functional component** performs any authentication of the cloud CSP:cloud service business manager and establishes authorization to use particular functions of the business capabilities. The business capabilities **functional component** interacts with business support systems **functional components** to carry out requests made by the CSC:cloud service business manager – including the **product catalogue**, account management and subscription management **functional components**.

The information that relates to the business capabilities is typically:

- **product catalogue** entries for available **cloud services**, with related technical information, pricing, terms and conditions;
- subscription information concerning which service(s) the customer is subscribing to, with associated quantitative information, if relevant (e.g., numbers of users, volumes of data, amount of processing, etc.);
- billing information, which can include information about usage charges, payments and account status.

Figure A.2 illustrates the **functional component** relationships involved in the select and purchase service **activity** of the CSC:cloud service business manager.

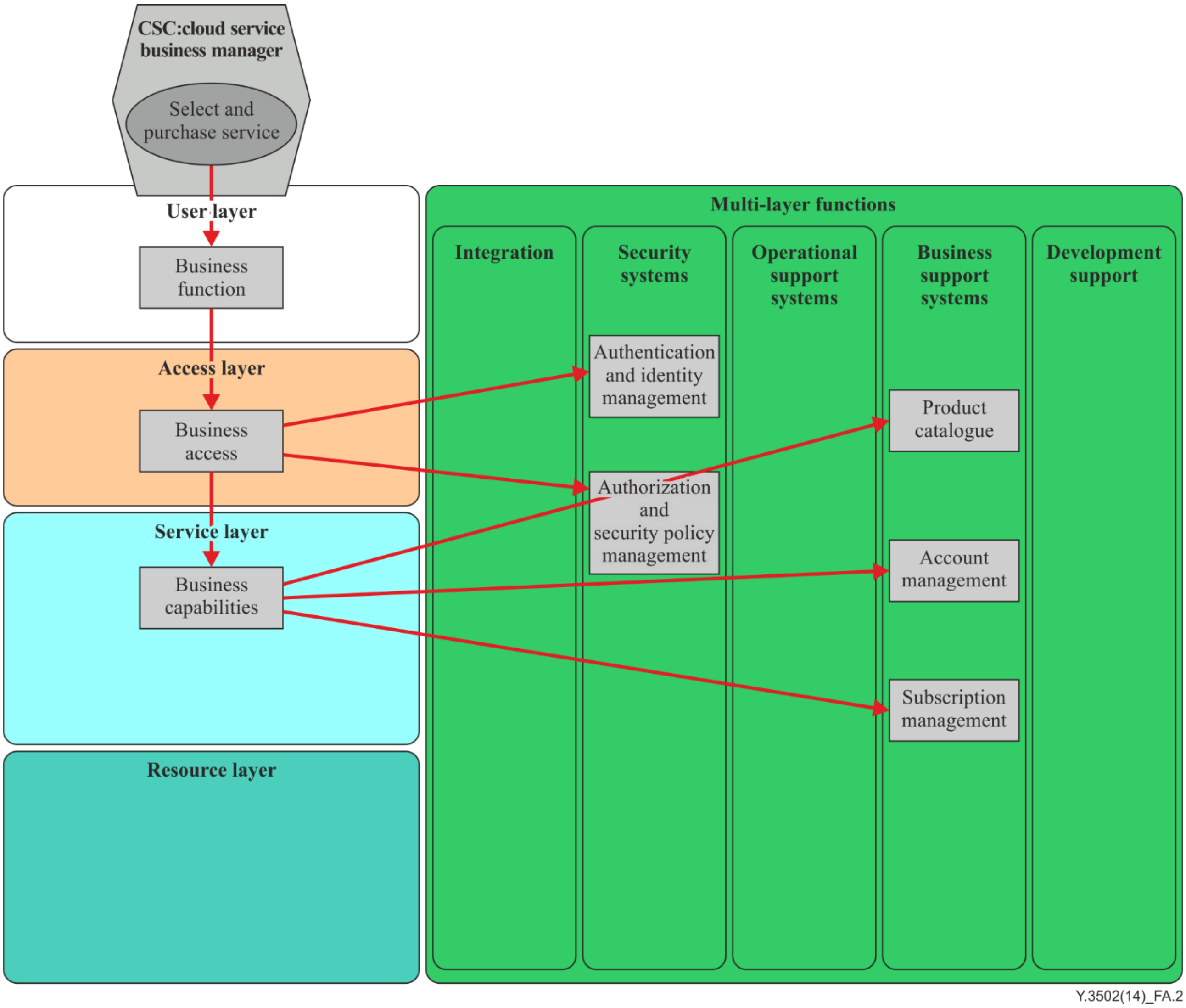


Figure A.2 – CSC:cloud service business manager relationship for " select and purchase service " activity

A.1.3 Administration relationship

The CSC:cloud service administrator performs the following cloud computing activities through the administrator function **functional component**:

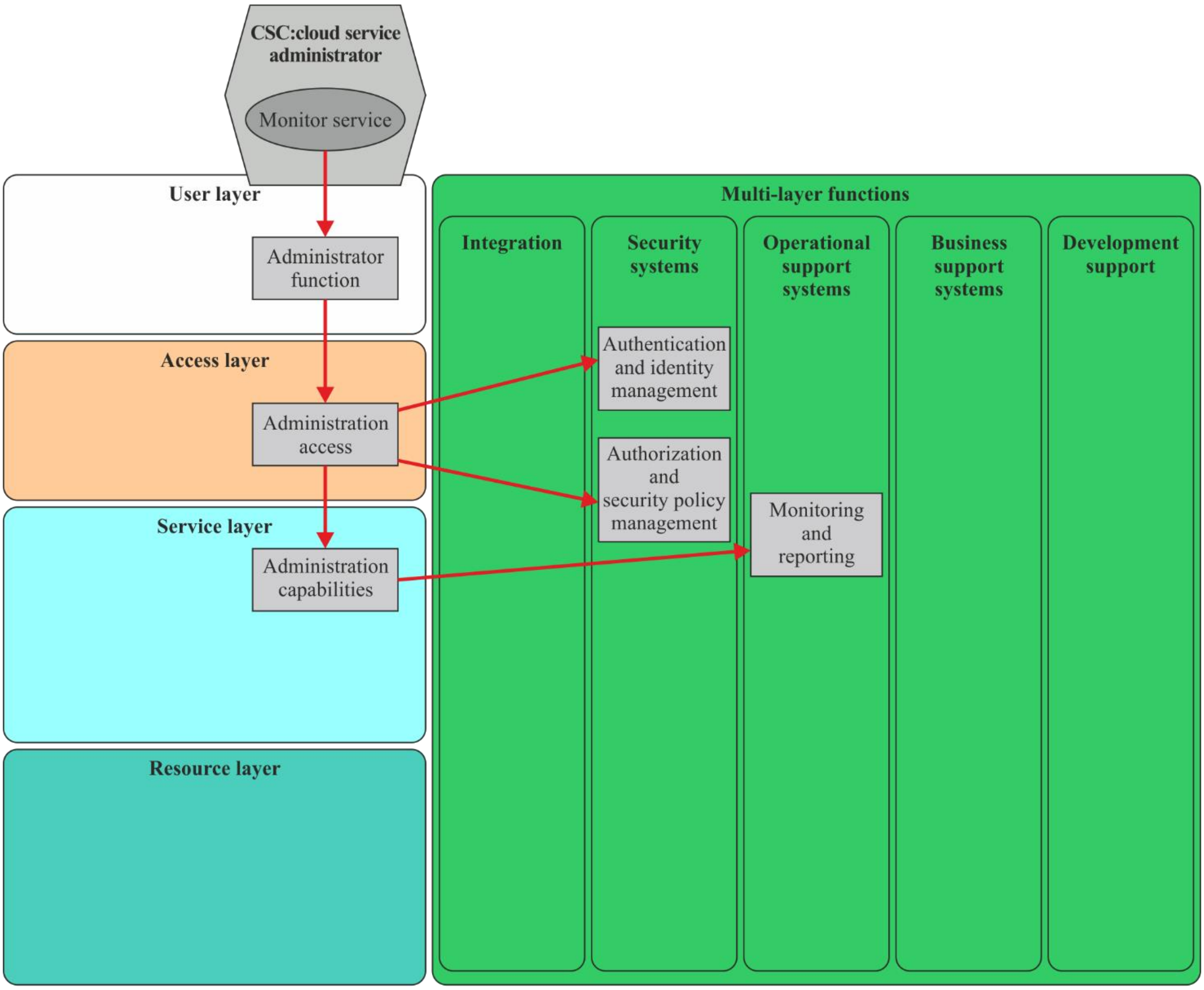
- monitor service;
- provide billing and usage reports;
- administer tenancies;
- administer service security;
- handle problem reports. The administrator function functional component invokes the administration capabilities functional component of the **cloud service provider** through an end point and interface enabled by the administration access functional component.

The administration access **functional component** performs any authentication of the CSC:cloud service administrator and establishes authorization to use particular functions of the administration capabilities **functional component**. The administration capabilities **functional component** interacts with operational support systems **functional components** to carry out requests made by the CSC:cloud service administrator, for example, the monitoring and reporting **functional component**.

The information that relates to the administration capabilities includes:

- security information such as the set-up of user accounts and authorization data, the encryption of data;
- notifications concerning usage of services including statistics of usage, log records (e.g., for security purposes);
- exception reports/events (e.g., where some service **SLA** target is breached or a security incident occurs).

Figure A.3 illustrates the **functional component** relationships involved in the monitor service **activity** of the CSC:cloud service administrator.



Y.3502(14)_FA.3

Figure A.3 – CSC:cloud service administrator relationship for the "monitor service" activity

Other elements relevant to the **cloud service customer**–**cloud service provider** relationship can include a customer to provider agreement, which can include an **SLA**, intellectual property issues and regulated matters such as the appropriate protection of personal data.

A.2 The provider–peer provider (or "inter-cloud") relationship

A **cloud service provider** can make use of one or more **cloud services** which are provided by other **cloud service providers**. This is described as a provider to **peer cloud service provider** relationship, or alternatively as an "inter-cloud" relationship – the provider making use of the services is termed a primary **cloud service provider** while a provider whose services are being used is termed a secondary **cloud service provider**.

As is the case with the **cloud service customer-cloud service provider** relationship there are two functional components to the relationship between two **cloud service providers**:

- the use of secondary provider **cloud services** by a primary provider;
- the use of secondary provider's business and administration capabilities by the primary provider's CSP:cloud service operations manager and CSP:cloud service manager to establish and control the use of the secondary provider's **cloud service**s.

For the secondary provider, the primary provider assumes the role of a **cloud service customer**. Services of the secondary **cloud service provider** are offered to and used by customers of the primary **cloud service provider**. The resulting linkage between the secondary **cloud service provider** and the **cloud service customer** of the primary provider requires specific consideration of issues such as security, protection of **PII**, and data ownership.

It is essential that the primary provider ensures that the **SLA** offered by the secondary provider's services is suitable for the requirements of the primary provider's services – and that any breaches of the **SLA** are managed appropriately.

There are three interfaces involved in the provider–peer provider relationship – the administration interface, the business interface and the service interface(s), which broadly provide the same capabilities as the equivalent interfaces in the **cloud service customer–cloud service provider** relationship. The way in which the administration interface is used is shown in Figure A.4 and the way in which the service interface is used is shown in Figure A.5 and the way in which the business interface is used is shown in Figure A.6.

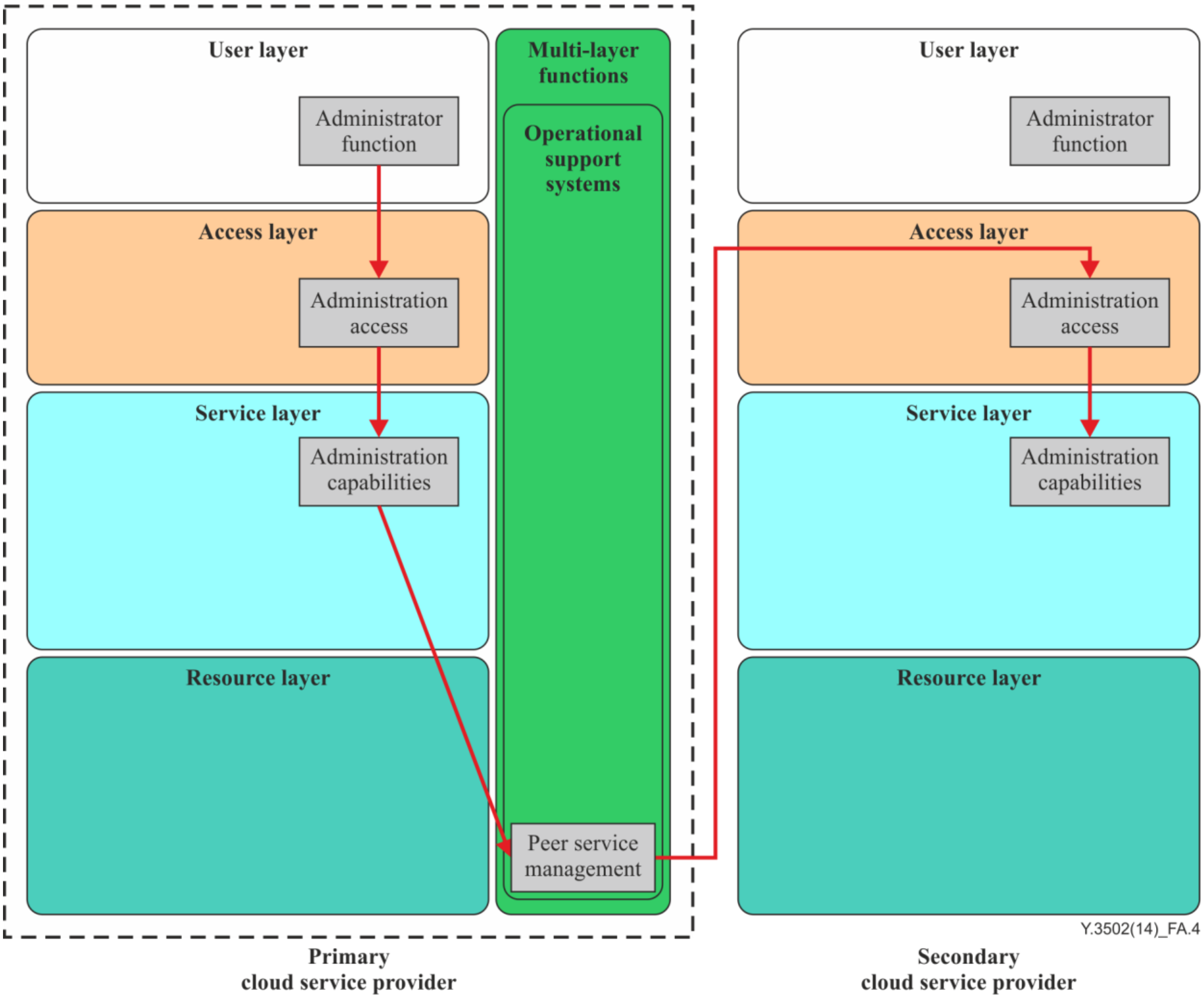


Figure A.4 – Provider–peer provider relationship for administrator activity

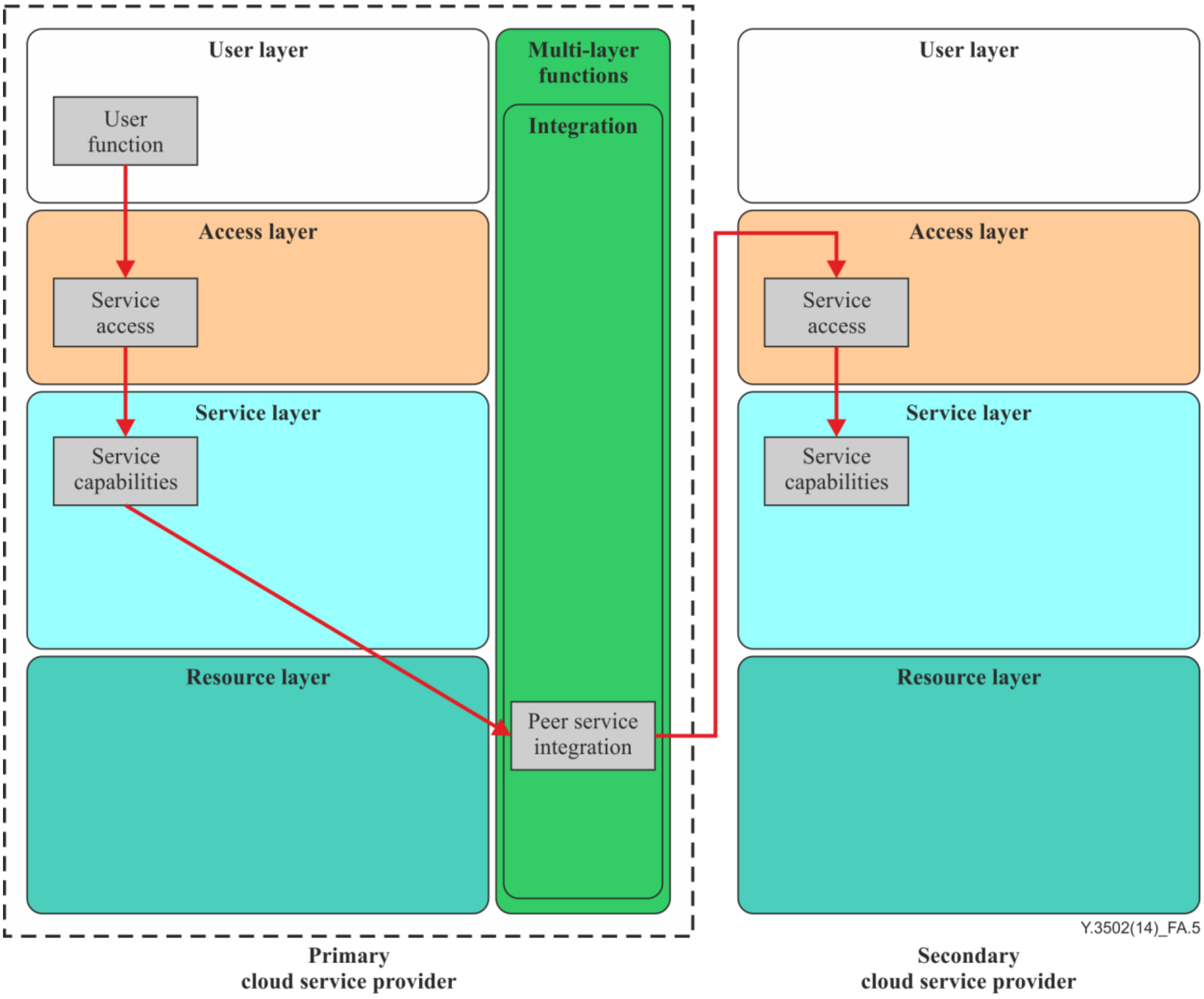


Figure A.5 – Provider–peer provider relationship for use service activity

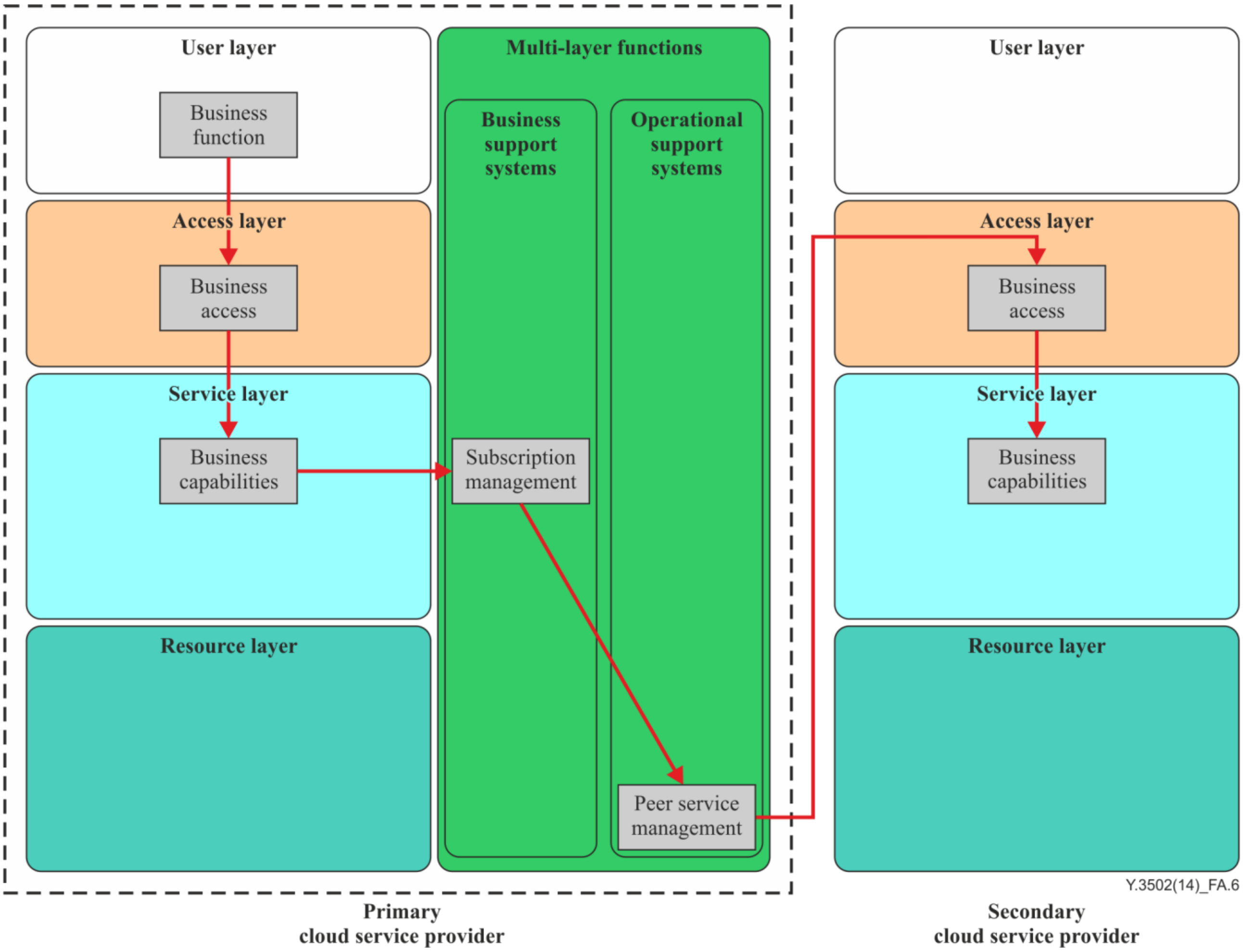


Figure A.6 – Provider–peer provider relationship for business interface

A.3 The cloud service developer–cloud service provider relationship

Cloud service developers create and package service implementations and hand them to **cloud service providers** for deployment and operation. Therefore, the cloud service developer interacts with the **cloud service provider** to:

1) inspect the **cloud service provider's** environment for service execution;
2) test service implementations;
3) hand over service implementation packages.

The development support **functional components** support the **cloud computing activities** of the cloud service developer, including the develop service, test service and maintain service **cloud computing activities**. These **cloud computing activities** depend on the development environment, build management and test management **functional components**.

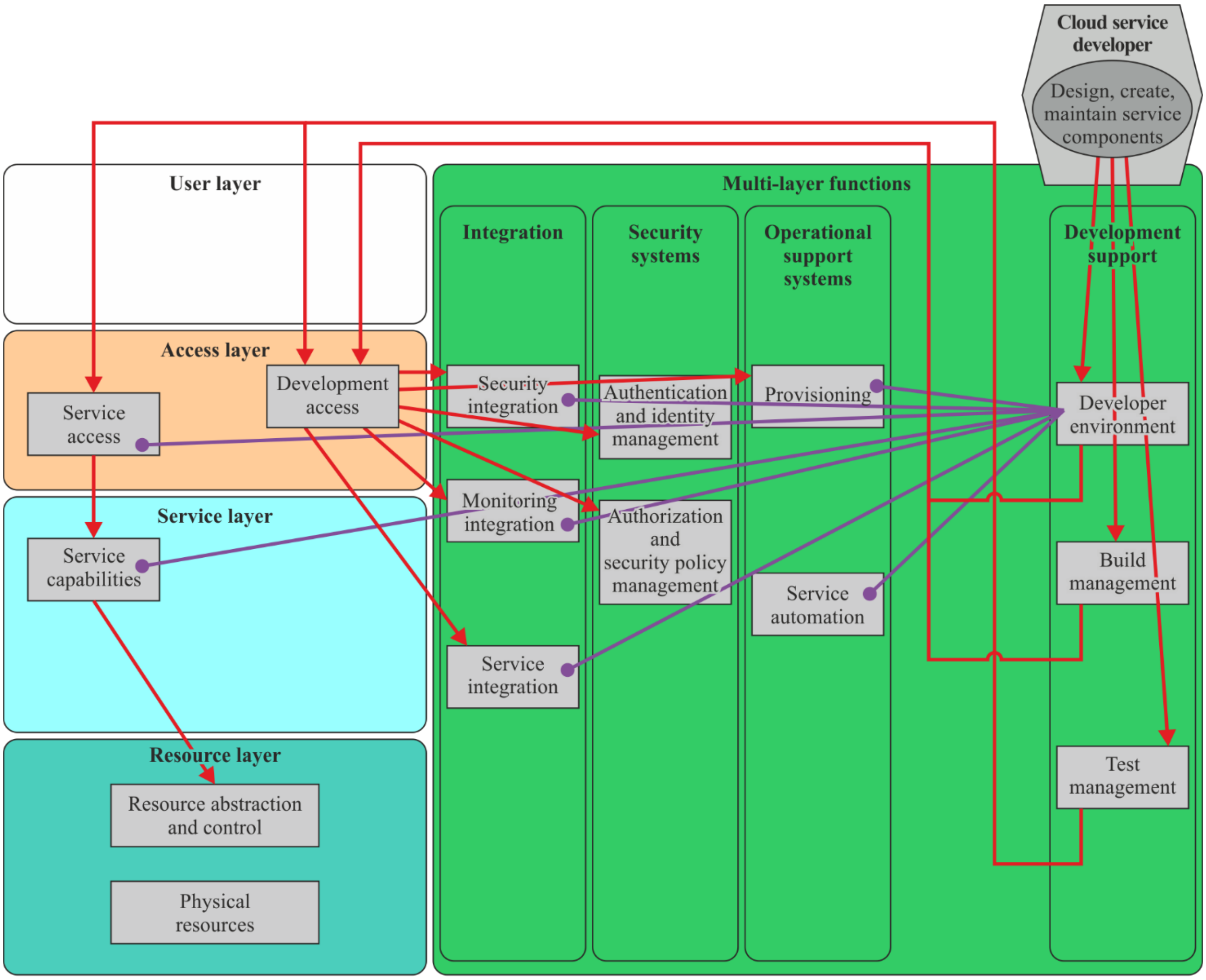
The lines in radiating from the developer environment component in Figure A.7 show that the cloud service developer develops the implementation of a **cloud service** and composes the service using the development environment **functional component** and then uses the build management system to build the service and its related artefacts into a deployable package. The arrows to/from the test management **functional component** indicate that the test management system performs appropriate testing against the built package, fetching the package from the build management system and interacting with the provider's environment via the development access **functional component** to deploy a test version of the service and execute the tests.

In Figure A.7, the lines from the development environment show that the development environment and build management system are used to create the software and related artefacts of the service implementation which offers the service interface. The cloud service developer can also create the service access implementation.

In order for the service implementation and service access to run in the target execution environment, the correct enablement for security, monitoring, management and automation needs to be developed, as well as enablement for integration into the service execution environment. The cloud service developer discovers the appropriate enablement for monitoring integration, security integration and service integration by using the development access capabilities. In addition, information and requirements for enabling authentication and identity management, as well as authorization and security policy management, is retrieved via the development access **functional component**.

The enablement of the **cloud service** implementation for deployment and provisioning is also done using the development environment and build management system (e.g., via scripts and configuration metadata files). The cloud service developer uses the development access **functional component** to discover what the provisioning and deployment requirements are.

The service implementation is packaged with the deployment and provisioning information and passed to the CSP:cloud service manager to perform the deploy services **activity** resulting in the service being available for use by customers in the provide services **activity**.



Y.3502(14)_FA.7

Figure A.7 – The cloud service developer–cloud service provider relationship

A.4 The cloud service provider–Auditor relationship

A **cloud auditor** should audit to agreed specifications, policies and agreements.

Audit specifications could be standards set by the **cloud service provider**, set by the auditor, or standards set independently, possibly as required by law. Whichever standard is used can depend on who the target of the auditor's audit result is. If the target of the audit result is a **cloud service customer** who wants some independent assurance then the audit should use an independently set standard.

Policies are set by the provider for auditing the provider's infrastructures and services. These policies are set by the business during the governance processes.

The **cloud service** agreement can include terms relating to the audit of the **cloud service provider** and possibly of the **cloud service customer**. Similar agreements can be in place between a primary **cloud service provider** and secondary **cloud service providers.** The responsibilities of the auditor are the same in each case.

The **cloud auditor's cloud computing activities** are security audit, privacy impact audit and performance audit. For all of these **cloud computing activities**, the **cloud auditor** can obtain audit evidence from the **cloud service provider**. The form of the audit evidence will vary depending on the type of audit and the standard(s) that apply to the audit. The evidence might take the form of procedural documents, or the form of log records. In any case, the **cloud service provider** can have a means by which the **cloud auditor** can obtain the required evidence.

In Figure 10-2, the perform audit **activity** of the **cloud auditor** makes requests for audit evidence to the **cloud service provider** through the administration access **functional component** of the **cloud service provider**, invoking the necessary administration capabilities.

A.4.1 Security audit

Various standards exist for system security audit. ISO/IEC 27001 is one such standard, covering **information security** management. There are also many other organizations which provide auditable standards for cloud security.

A.4.2 Privacy impact audit

Various data protection authorities (e.g., the Privacy Commissioner in Canada and the Information Commissioner in the UK) publish guidelines on the assessment and/or audit of the privacy impact of programs, policies or systems. The **protection of PII** is typically subject to regulation and/or legislation, but one of the issues relating to the **cloud service** is that the **cloud service customer** can be in a different jurisdiction to that which applies to the **cloud service provider**. The situation can be made more complex if the **cloud service provider** operates multiple data centres in different jurisdictions and moves data or service execution between these data centres (e.g., for the purposes of service continuity or for the efficient use of resources).

ISO/IEC 27018 is a standard which defines the **information security** controls applicable to a **cloud service provider** when acting as a data processor. ISO/IEC is also dealing with the wider aspects of privacy (see the ISO/IEC 29100 series of standards, for example).

A **cloud auditor** should assess the protection of **personally identifiable information** aspects of a **cloud service** and the **cloud service provider**'s operations against data protection regulations of the appropriate jurisdictions, following the guidelines issued by the data protection authorities and relevant standards.

A.4.3 Performance audit

Performance audit assesses the ability of the **cloud service provider** to meet the performance targets specified for their **cloud services**, typically documented in the **SLA**.

Bibliography

- ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.
- ISO/IEC 27002:2013, *Information technology – Security techniques – Information security management systems – Code of practice for information security management*.
- ISO/IEC 27018:2014, *Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
- ISO/IEC/IEEE 24765:2010, *Systems and software engineering – Vocabulary*.
- ISO/IEC/IEEE 42010:2011, *Systems and software engineering – Architecture description*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014