INTERNATIONAL STANDARD

ISO/IEC 22123-3

First edition
2023-09

Information technology — Cloud computing —

Part 3: Reference architecture

Technologies de l'information — Informatique en nuage — Partie 3: Architecture de référence

Reference number
ISO/IEC 22123-3:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

This first edition of ISO/IEC 22123-3 cancels and replaces ISO/IEC 17789:2014, which has been technically revised.

The main changes are as follows:

— added differentiation between cloud computing parties and role;

— Figures 13, 14, and 15 were removed.

A list of all parts in the ISO/IEC 22123 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Information technology — Cloud computing —

Part 3:
Reference architecture

1 Scope

This document specifies the cloud computing reference architecture (CCRA).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

ISO/IEC 22123-2, *Information technology — Cloud computing — Concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms related to security and privacy

3.1.1
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal. 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 establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.2 Terms relating to architecture

3.2.1
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

[SOURCE: ISO/IEC/IEEE 42010:2011, 3.2]

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 22123-2 and the following apply.

CCRA	cloud computing reference architecture
KPI	key performance indicator
MSA	master service agreement
OSS	operational support systems
QoS	quality of service
ToS	terms of service
VLAN	virtual local area network

5 Conventions

The following conventions apply:

1) Diagrams are used throughout this document to help illustrate the cloud computing reference architecture (CCRA). Figure 1 provides the conventions in the diagrams.

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

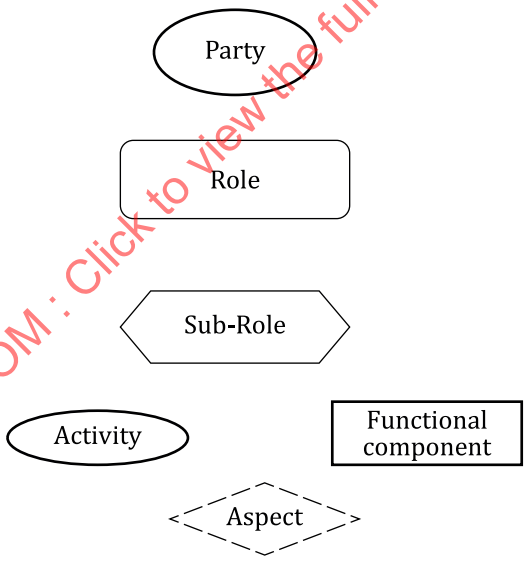

Figure 1 — Conventions for CCRA diagrams

2) This CCRA uses the term ICT (information and communication technology as defined in ISO/IEC/IEEE 24765:2017, 3.1853) and ICT systems. ICT is used to make it clear that the CCRA covers not only the compute and storage technologies associated with computer systems, but also the communications networks that link systems together.

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 ISO/IEC 22123-1).

The CCRA presented in this document 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 can put constraints on a specific system. The CCRA does not define prescriptive solutions and is not tied to any specific vendor products, services or reference implementation.

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 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 CCRA viewpoints

7.1 General

This document 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 document. The cloud computing paradigm is composed of key characteristics, cloud computing roles and activities, cloud capabilities types and cloud service categories, cloud deployment models, and cloud computing cross cutting aspects.

7.2 CCRA architectural views

Cloud computing systems can be described using a viewpoint approach.

Four distinct viewpoints are used in the CCRA (see Figure 2):

— user view;

— functional view;

— implementation view;

— deployment view.

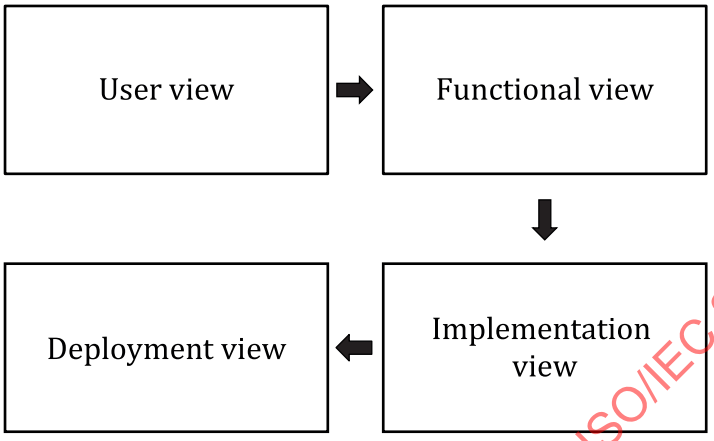

Figure 2 — Cloud computing architectural viewpoints

Table 1 provides a description of each of these views.

Table 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 document, the implementation and deployment views are related to technology and vendor specific cloud computing implementations and actual deployments and are therefore out of scope of this document.		

Figure 3 shows the transition from the user view to the functional view. Details are presented in 7.5.

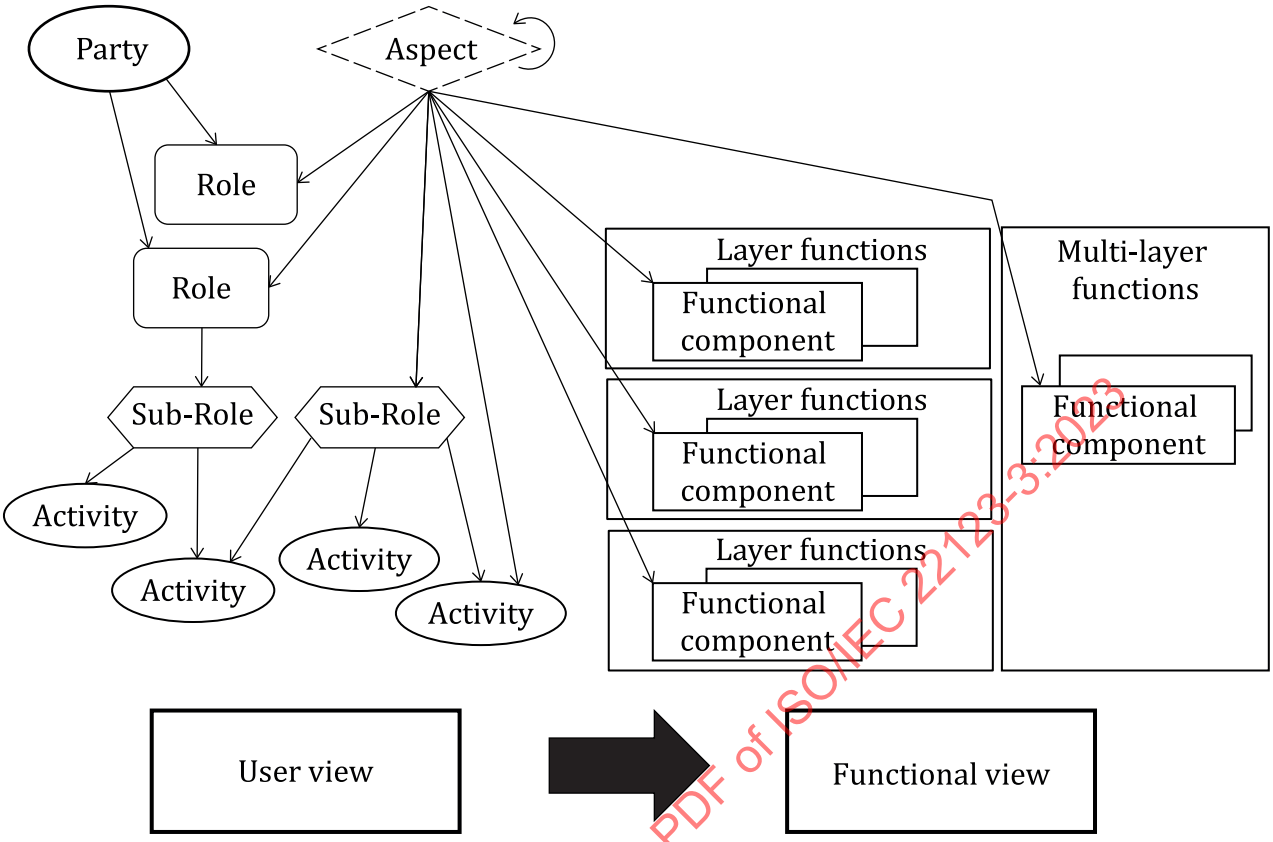

Figure 3 — Transition from user view to functional view

7.3 User view of cloud computing

7.3.1 General

The user view addresses the following cloud computing concepts:

— parties;

— roles and sub-roles;

— cloud computing activities;

— cloud services;

— cloud deployment models;

— cross-cutting aspects.

Figure 4 illustrates the relationships among parties, roles and sub-roles and their relationship to activities and cross-cutting aspects.

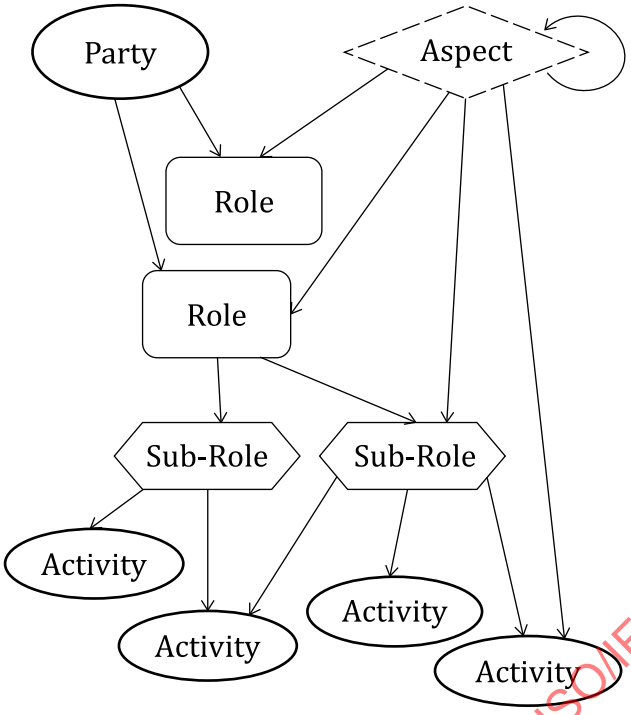

Figure 4 — User view entities

7.3.2 Cloud computing activities

ISO/IEC 22123-1 defines a cloud computing activity as a specified pursuit or set of tasks.

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

Activities in a cloud computing system are conducted using functional components (see 7.4.2).

Cloud computing activities are identified and described in more detail in 8.3.

7.3.3 Parties

ISO/IEC 22123-1 defines a party as a natural person or legal person, whether or not incorporated, or a group of either. Parties in a cloud computing system are its stakeholders. ISO/IEC 22123-2 identifies the following major parties of cloud computing:

— Cloud service customer (CSC)

— Cloud service partner (CSN)

— Cloud service provider (CSP)

ISO/IEC 22123-2 further describes that these parties are entities that play roles (and sub-roles). A party can play more than one role at any given point in time and can only engage in a specific subset of activities of that role.

7.3.4 Roles and sub-roles

ISO/IEC 22123-1 defines a role as a set of cloud computing activities that serves a common purpose.

ISO/IEC 22123-2 identifies the following as the major cloud computing roles:

— cloud service customer role (CSC role);

— cloud service provider role (CSP role);

— cloud service partner role (CSN role).

A sub-role is a sub-set 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 are provided in 8.1.

7.3.5 Cloud services

Cloud services are the essential elements of a cloud computing system. Cloud services are covered in ISO/IEC 22123-2.

Cloud services can be described in terms of the cloud capabilities types which they offer, based on the resources provided by the cloud service. The CCRA focuses on the following cloud capabilities types:

— application capabilities type;

— platform capabilities type;

— infrastructure capabilities type.

Cloud capabilities types are described in ISO/IEC 22123-2:2023, 5.3.

Cloud services are also grouped into categories, where each category is a group of cloud services that possess some common set of qualities. Representative cloud service categories include:

— infrastructure as a services (IaaS);

— platform as a service (PaaS);

— software as a service (SaaS);

— network as a service (NaaS).

The services in these categories can include capabilities from one or more of the cloud capabilities types above.

Other cloud service categories are described in ISO/IEC 22123-2:2023, 5.4 and Annex A.

7.3.6 Cloud deployment models

Cloud deployment models are defined in ISO/IEC 22123-1 and described in ISO/IEC 22123-2:2023, 5.5.

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

The CCRA focuses on the following cloud deployment models:

— public cloud;

— private cloud;

— community cloud;

— hybrid cloud.

NOTE Additional cloud deployment models include multi-cloud and federated cloud. See ISO/IEC 5140 for additional details.

7.3.7 Cloud computing 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.

Cross-cutting aspects of cloud computing described in ISO/IEC 22123-2:2023, Clause 7 include:

— auditability;

— availability;

— governance;

— interoperability;

— maintenance and versioning;

— performance;

— portability;

— protection of personally identifiable information;

— regulatory;

— resiliency;

— reversibility;

— security;

— service levels and service level agreements.

7.4 Functional view of cloud computing

7.4.1 General

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 among the functional components.

The functional view addresses the following cloud computing items:

— functional layers;

— functions;

— functional components;

— multi-layer functional components.

For the purposes of this document, the term “functional component” is used to represent a set of one or more functions.

Figure 5 illustrates the concepts of functions, layers and functional components.

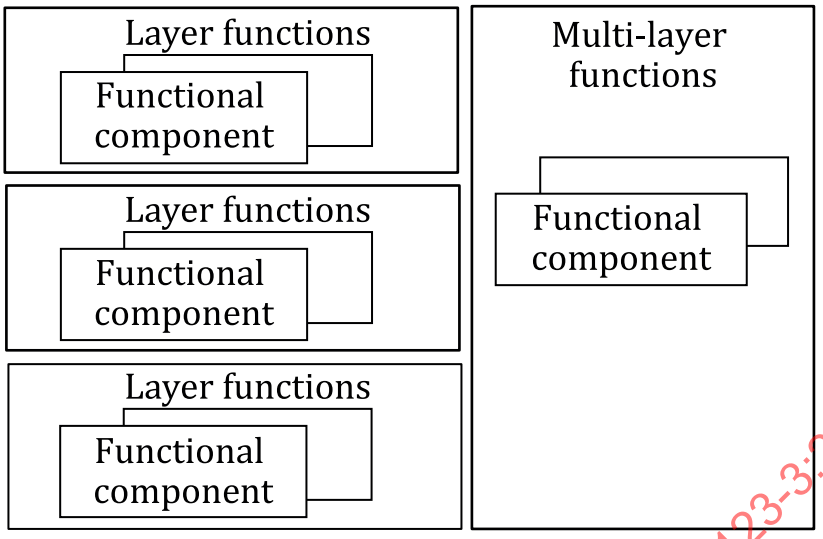

Figure 5 — Functional layering

The cloud computing functional architecture is described in subclause 9.1.

7.4.2 Functional components

ISO/IEC 22123-1 defines a functional component as 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 subclause 9.2.

7.4.3 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 CSCs and CSNs;

— 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.

Not all layers or functional components are necessarily instantiated in a specific cloud computing system.

7.4.4 Multi-layer functions

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

Multi-layer functional components can be classified on the basis of their purpose:

— development support;

— integration;

— security systems;

— operational support systems;

— business support systems.

Functional components of the multi-layer functions are described in clause 9.2.6.

7.5 Relationship between the user view and the functional view

Figure 6 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).

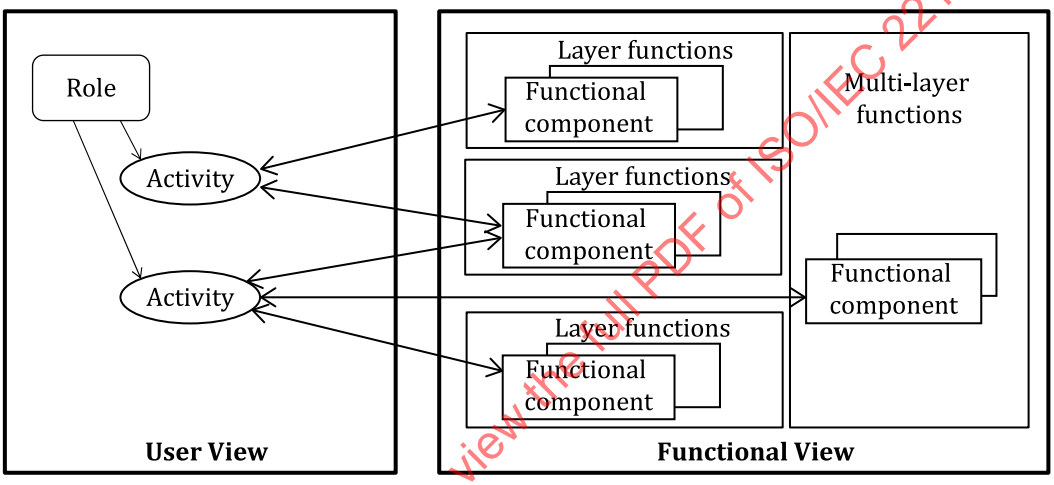

Figure 6 — From user view to functional view

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

7.6 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 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.

Clause 8.2 provides additional information on cross-cutting aspects.

7.7 Implementation view of cloud computing

While details of the user view and functional view are addressed within this document, the implementation view is out of the scope of this document.

7.8 Deployment view of cloud computing

While details of the user view and functional view are addressed within this document, the deployment view is out of the scope of this document.

8 User view

8.1 Cloud computing roles and sub-roles

8.1.1 General

It is often necessary to differentiate requirements and issues for the following major cloud computing parties: CSC, CSP, and CSN.

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.

In addition to the CSC role, CSP role, and CSN role (see 7.3.4), ISO/IEC 22123-2 identifies a set of sub-roles for each and uses a naming convention in which the name of a sub-role has the prefix of "CSC:" for CSC sub-roles, "CSN:" for CSN sub-roles, or "CSP:" for CSP sub-roles and then the sub-role name. Table 2 shows the prefix for each of the three cloud computing roles.

Table 2 — Cloud computing sub-roles

Role	Sub-role prefix	Example
CSC role	"CSC:"	CSC:cloud service administrator
CSP role	"CSP:"	CSP:network provider
CSN role	"CSN:"	CSN:cloud auditor

Roles and sub-roles are sets of activities (see 8.2).

Figure 7 shows the roles of cloud computing, with their associated sub-roles.

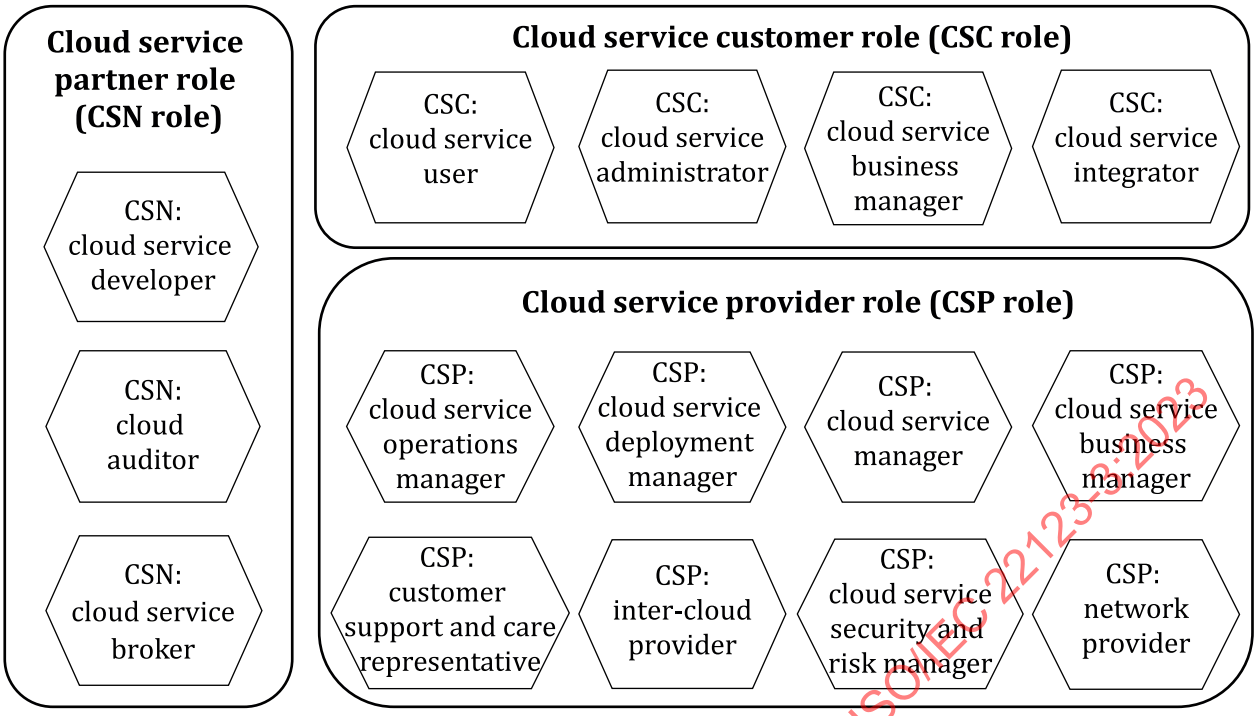

Figure 7 — Roles and sub-roles

Additional information is provided on the CSC role in 8.1.2, the CSP role in 8.1.3, and the CSN role in 8.1.4.

8.1.2 Cloud service customer role

8.1.2.1 General

ISO/IEC 22123-1 defines a CSC as a party that is acting in the cloud service customer role (CSC role). The CSC is in a business relationship with a CSP or a CSN for the purpose of using cloud services. The CSC role can include ensuring the smooth operation of the cloud services, acquisition and use of cloud services, and integration of cloud services with a CSC's existing ICT systems.

Figure 8 shows the common sub-roles for the CSC role as well as the associated activities; the activities listed are not exhaustive.

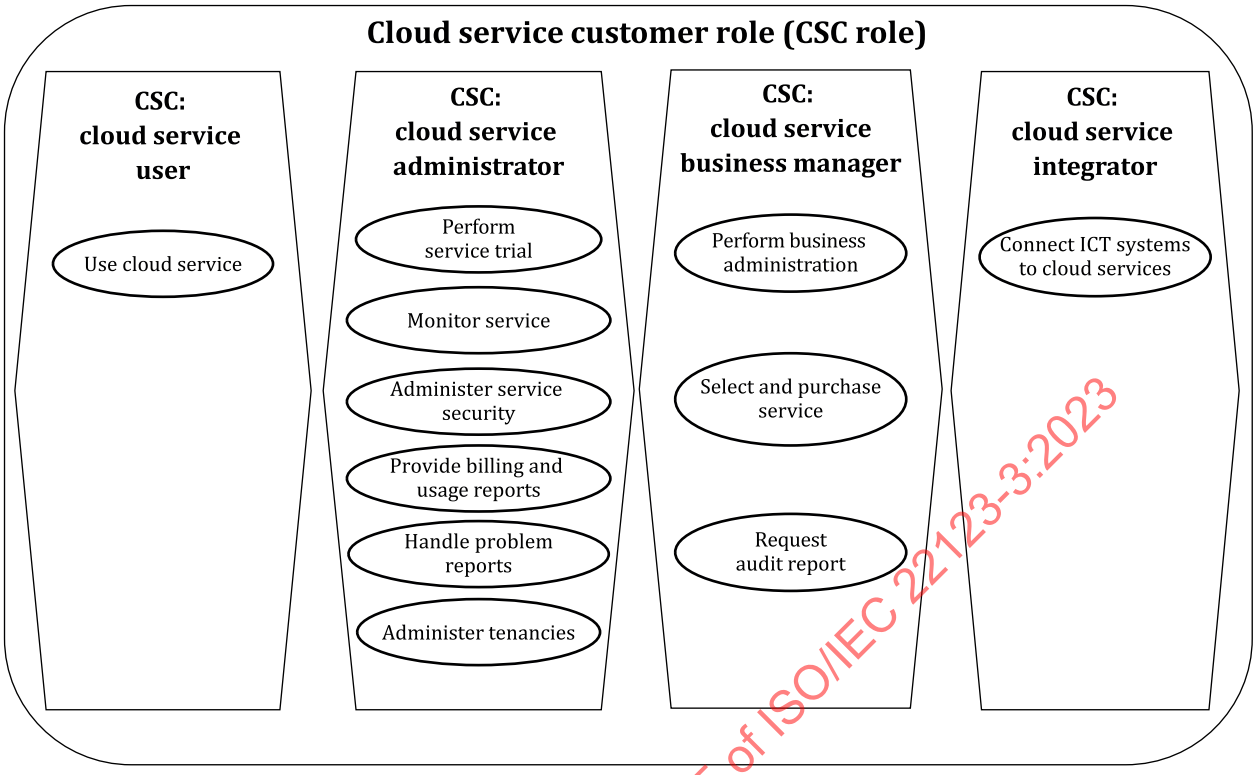

Figure 8 — Sub-roles and activities for the CSC role

8.1.2.2 CSC:cloud service user

The CSC:cloud service user is a sub-role of the CSC role which is associated with a CSC that uses cloud services.

The CSC:cloud service user's cloud computing activities include: use cloud service (8.2.2.1).

8.1.2.3 CSC:cloud service administrator

The CSC:cloud service administrator is a sub-role of the CSC role which has a main goal of ensuring the effective 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 CSC and one or more CSPs.

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

— perform service trial (8.2.2.2);

— monitor service (8.2.2.3);

— administer service security (8.2.2.4);

— handle problem reports (8.2.2.5);

— provide billing and usage reports (8.2.2.6);

— administer tenancies (8.2.2.7).

8.1.2.4 CSC:cloud service business manager

The CSC:cloud service business manager is a sub-role of the CSC role which aims to meet the business goals of the CSC through the acquisition and use of cloud services in a cost efficient way. The CSC:cloud service business manager is concerned with financial and legal aspects of the use of cloud services. This includes approval to operate as well as on-going ownership of, and accountability for, meeting business goals.

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

— perform business administration (8.2.2.8);

— select and purchase cloud service (8.2.2.9);

— request audit report (8.2.2.10).

8.1.2.5 CSC:cloud service integrator

The CSC:cloud service integrator is a sub-role of the CSC role that supports integration of cloud services with a CSC's ICT systems, including applications, functions and data.

The CSC:cloud service integrator's cloud computing activities include: connect ICT systems to cloud services (8.2.2.11).

8.1.3 Cloud service provider role

8.1.3.1 General

ISO/IEC 22123-1 defines a CSP as a party that is acting in the cloud service provider role (CSP role). The CSP is in a business relationship with a CSC or a CSN for the purpose of providing cloud services.

The CSP role is a set of activities that make cloud services available. The CSP role focuses on activities necessary to provide a cloud service and activities necessary to ensure its delivery to the CSC as well as cloud service maintenance. The CSP role includes an extensive set of activities including. providing services, deploying and monitoring services, managing business plans, providing audit data, etc. Specific descriptions of sub-roles for CSP role and associated activities are described in 8.1.3.2 through 8.1.3.9.

Figure 9 shows the common sub-roles for the CSP role as well as the associated activities; the activities listed are not exhaustive.

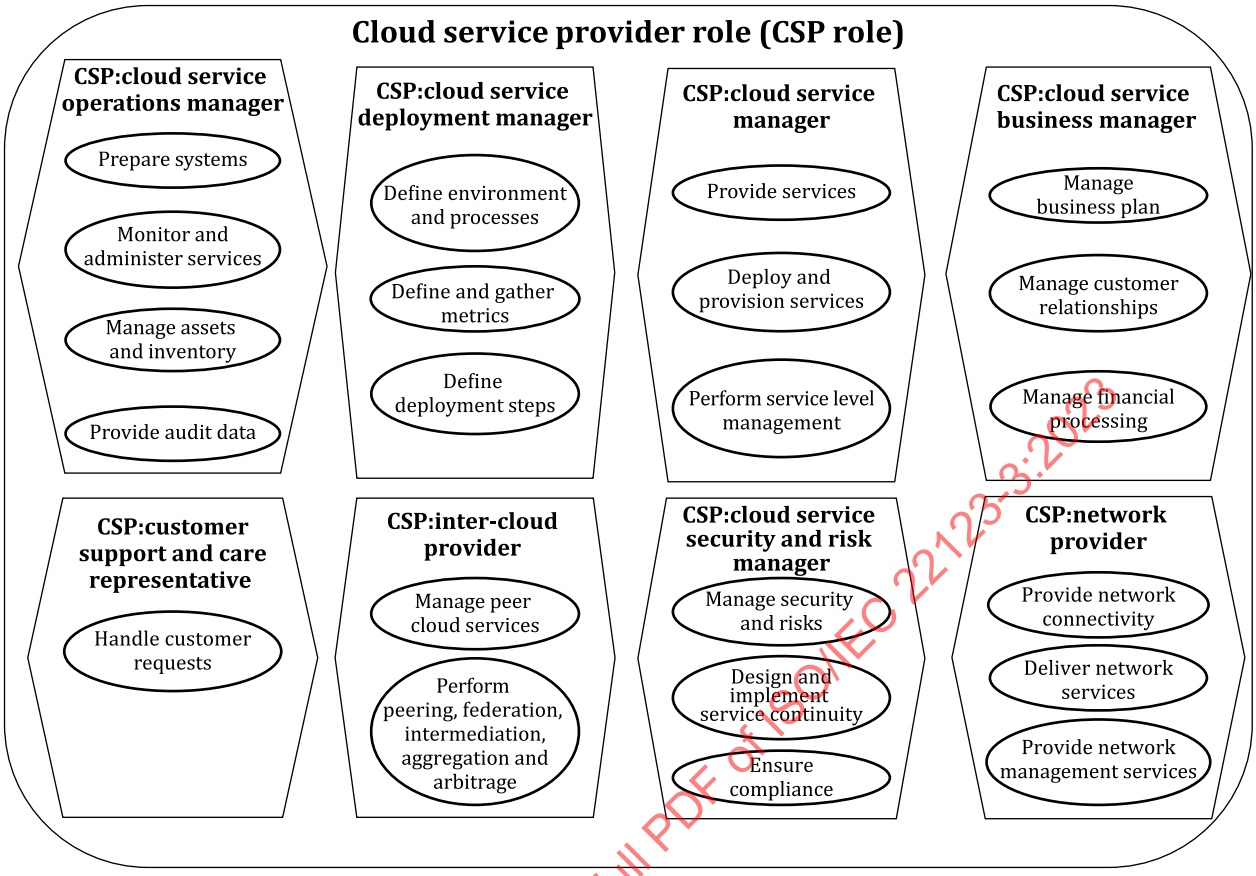

Figure 9 — Sub-roles and activities for the CSP role

8.1.3.2 CSP:cloud service operations manager

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

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

— prepare systems (8.2.3.1);

— monitor and administer services (8.2.3.2);

— manage assets and inventory (8.2.3.3);

— provide audit data (8.2.3.4).

8.1.3.3 CSP:cloud service deployment manager

The CSP:cloud service deployment manager is a sub-role of the CSP role 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 (8.2.3.5);

— define and gather metrics (8.2.3.6);

— define deployment steps (8.2.3.7).

8.1.3.4 CSP:cloud service manager

The CSP:cloud service manager is a sub-role of the CSP role which has responsibility for ensuring that the CSP's services are available for use by CSCs, 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 CSP's business support system and operational support system, as well as the operation of the other functionalities offered to the CSCs and CSNs for management, administration and other cloud computing activities.

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

— provide services (8.2.3.8);

— deploy and provision services (8.2.3.9);

— perform service level management (8.2.3.10).

8.1.3.5 CSP:cloud service business manager

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

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

— manage business plan to provide cloud services (8.2.3.11);

— manage customer relationships (8.2.3.12);

— manage financial processing (8.2.3.13).

8.1.3.6 CSP:customer support and care representative

The CSP:customer support and care representative is a sub-role of the CSP role that is the main interface for the CSC with the CSP 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 provided to the CSC.

The CSP:customer support and care representative's cloud computing activities include: handle customer requests (8.2.3.14).

8.1.3.7 CSP:primary inter-cloud provider

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

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

— manage cloud services from secondary inter-cloud providers (8.2.3.15);

— perform intermediation, aggregation and arbitrage (8.2.3.16).

8.1.3.8 CSP:cloud service security and risk manager

The CSP:cloud service security and risk manager is a sub-role of the CSP role which has the responsibility of ensuring that the CSP 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 CSC and the CSP are aligned and meet security requirements stated in the SLA.

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

— manage security and risks (8.2.3.17);

— design and implement service continuity (8.2.3.18);

— address regulatory compliance obligations (8.2.3.19).

8.1.3.9 CSP:network provider

The CSP:network provider is a sub-role of the CSP role which is to provide network connectivity and network services for the CSC, CSN and CSP. The CSP:network provider can provide network connectivity between systems within the CSP's data centre, or provide network connectivity between the CSP's systems and systems outside the provider's data centre, for example, CSC systems or systems belonging to other CSPs.

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

— provide network connectivity (8.2.3.20);

— deliver network services (8.2.3.21);

— provide network management services (8.2.3.22).

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

8.1.4 Cloud service partner role

8.1.4.1 General

ISO/IEC 22123-1 defines a CSN as a party that is acting in the cloud service partner role (CSN role).

The CSN role is a set of activities that support, or are auxiliary to, either the CSP role or the CSC role, or both. Activities of a CSN role vary depending on the type of partner and their relationship with the CSP role and the CSC role (see ISO/IEC TR 23187). Specific descriptions of sub-roles for the CSN role and associated activities are described in 8.1.4.2 through 8.1.4.4.

Figure 10 shows the common sub-roles for the CSN role as well as the associated activities; the activities listed are not exhaustive.

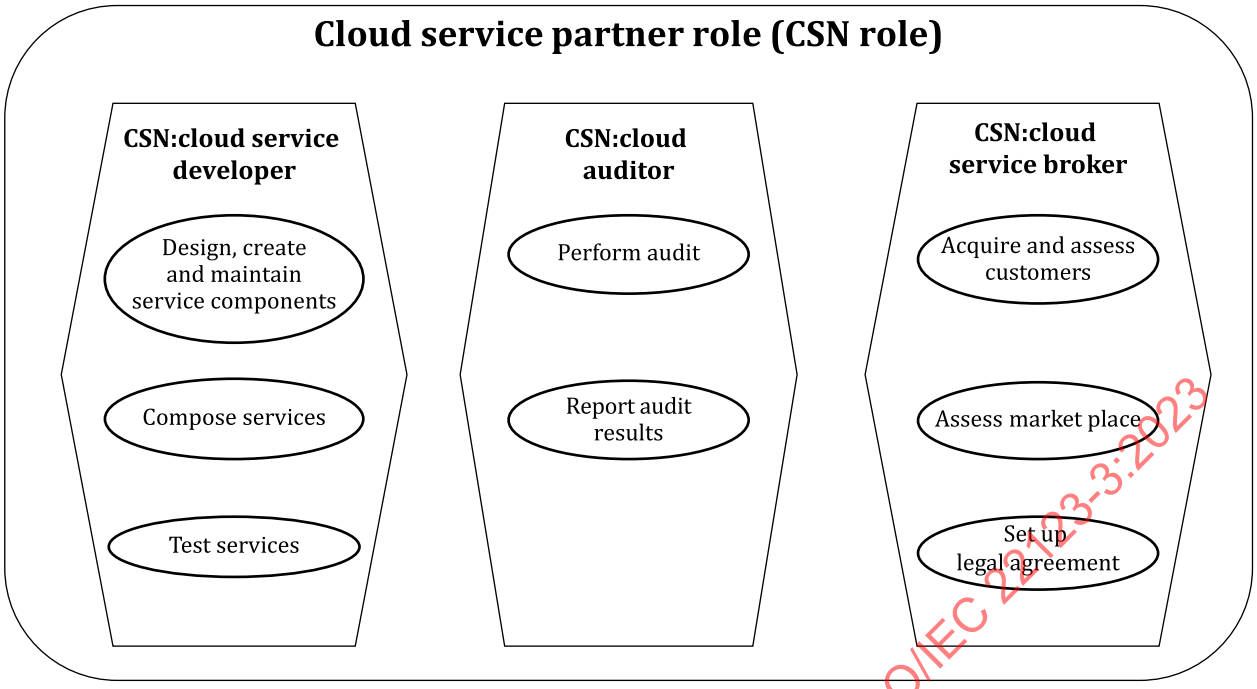

Figure 10 — Sub-roles and activities for the CSN role

8.1.4.2 CSN:cloud service developer

The CSN:cloud service developer is a sub-role of the CSN role 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 CSN:cloud service developer's cloud computing activities include:

— design, create and maintain service components (8.2.4.1);

— compose services (8.2.4.2);

— test services (8.2.4.3).

NOTE 1 CSN:cloud service integrator and CSN:cloud service component developer describe sub-roles of CSN:cloud service developer, where CSN:cloud service integrator deals with the composition of a service from other services, and where CSN: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 secondary cloud service providers.

8.1.4.3 CSN:cloud auditor

The CSN:cloud auditor is a sub-role of the CSN role with the responsibility to conduct 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 CSN:cloud auditor's cloud computing activities include:

— perform audit (8.2.4.4);

— report audit results (8.2.4.5).

The CSN:cloud auditor's cloud computing activities are security audit, privacy impact audit and performance audit. For all of these cloud computing activities, the CSN:cloud auditor can obtain audit evidence from the CSP. The form of the audit evidence can vary depending on the type of audit and the standard(s) that apply to the audit (see ISO/IEC TR 3445 for details on cloud audit). The evidence can take the form of procedural documents, or the form of log records. In any case, the CSP can have a means by which the CSN:cloud auditor can obtain the required evidence.

8.1.4.4 CSN:cloud service broker

The CSN:cloud service broker is a sub-role of the CSN role that negotiates relationships between CSCs and CSPs. The cloud service broker is not itself a CSP and should not be confused with the role of CSP: primary inter-cloud provider (see clause 8.1.3.7). The CSN:cloud service broker role can be combined with or operate independently of the role of CSP:primary inter-cloud provider.

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

— acquire and assess customers (8.2.4.6);

— assess marketplace (8.2.4.7);

— set up legal agreement (8.2.4.8).

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

In either case, the CSN:cloud service broker only acts during the contracting phase of the service, between the CSC and CSP. The CSN:cloud service broker is not involved during the consumption of the service. In such cases, the activities involve CSP role activities.

8.2 Cloud computing activities

8.2.1 General

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.

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 cloud services and are associated with the CSC role (8.2.2);

— activities that provide cloud services and are associated with the CSPC role (8.2.3);

— activities that support cloud services and are associated with the CSN role (8.2.4).

8.2.2 Activities associated with the CSC role

8.2.2.1 Use cloud service

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

The use cloud service activity typically involves:

— the provision of user credentials to enable the CSP to authenticate the user and grant access to the cloud service;

— 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 CSP in order to ensure that the cloud service is fit for the CSC's business needs. The cloud services are used on a trial basis, with mutual agreement and understanding between the CSP and CSC.

The perform service trial activity involves:

— The provision of the user credentials to enable the CSP to authenticate the user and grant access to the "trial" cloud service;

— The invocation of the "trial" cloud service, which can be tested by the CSC 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 CSC and CSP. This activity utilizes intrinsic monitoring functions of the cloud services. This activity involves:

— keeping track of usage (measured) of each cloud service, and by which users. This provides 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 of 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;

— evaluate and monitor data transfer in compliance to regulatory and other legal requirements.

8.2.2.4 Administer service security

The administer service security activity involves:

— ensuring appropriate security for CSC 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 CSC data both at rest and also in motion;

— defining the handling of any personally identifiable information (PII) in the CSC data.

8.2.2.5 Handle problem 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 Provide billing and usage reports

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

— assessing of the impact of each problem;

— troubleshooting to determine the cause(s) of the problem;

— opening a problem report(s) with the CSP 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 CSC with the CSP. 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 the accounting and financial management. This activity includes:

— adjusting business plan to accommodate use of cloud services;

— tracking the use of the services and dealing with accounting and financial management;

— handling billing/invoices received from the CSP for the use made of cloud services;

— ensuring that billing matches the actual usage of cloud services made by the CSC;

— making payments to the CSP;

— 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) CSPs to determine if the service offered meets the business and technical requirements of the CSC. 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 CSP permits variable terms for the service);

— accepting the contract for the cloud service and performing registration with the CSP.

8.2.2.10 Request audit report

The request audit report activity involves the CSC requesting the report of an audit of the cloud service, typically conforming to a particular audit standard or scheme. The CSC can request the report from a cloud auditor, or possibly from the CSP, although it is expected that the audit report is prepared by an entity independent of the CSP 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 CSP'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 of business data between CSC's existing ICT systems and cloud services;

— invoking cloud service operations from existing ICT components and applications, with supply of input data and 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 use of management interfaces for cloud services;

— integrating logging and security incident management between cloud services and CSC monitoring and management infrastructure.

8.2.3 Activities associated with the CSP role

8.2.3.1 Prepare systems

This 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 increase in use of existing services;

— modifying or expanding the resources in the data centre to meet the needs of new deployments.

8.2.3.2 Monitor and administer services

This activity focuses on monitoring and administering services and the associated infrastructure which includes user and system privileges. This activity involves:

— monitoring the services and infrastructure of the CSP;

— 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 CSCs 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 virtualization environment;

— monitoring the behaviour of the ICT environment of the CSP 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.

8.2.3.3 Manage assets and inventory

This 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 no longer required. This can include appropriate secure disposal of any assets that can hold data.

8.2.3.4 Provide audit data

This 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 can depend on the auditing scheme or standard that is being used. This activity involves:

— creating and sending appropriate audit information from logs;

— redacting information from any log records or other data that can contain sensitive information or PII.

8.2.3.5 Define environment and processes

This activity focusses 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 conforms to appropriate standards relating to security and business;

— defining the processes to follow when the service is running, including plans for fixes, upgrades and migration.

8.2.3.6 Define and gather metrics

This 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.

8.2.3.7 Define deployment steps

This activity focuses on defining the steps for 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 CSCs.

8.2.3.8 Provide services

This activity involves all steps required to deliver a cloud service to its CSCs. The provide services activity includes accepting and processing service invocations from the user with associated authentication and authorization of the user identity. 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 service fault handling process;

— managing the business support system and the operational support system;

— maintaining 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 CSP's data centre;

— installing and configuring 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.

8.2.3.9 Deploy and provision services

This activity involves getting a service implementation running, making it available at a network endpoint accessible to the CSC:cloud service users and 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.

8.2.3.10 Perform service level management

This 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.

8.2.3.11 Manage business plan

This activity involves:

— defining service offering, describing the technical aspects of the offering (functional interfaces, SLAs, etc.) and business aspects of the offering;

NOTE When establishing the service offering, the CSP takes into account aspects related to the interaction with secondary 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 CSP;

— preparing a business plan and adjusting the business plan to provide cloud services.

8.2.3.12 Manage customer relationships

This activity involves the management of the business relationship of the CSP with the CSC 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).

8.2.3.13 Manage financial processing

This activity involves:

— handling of 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 CSC;

— handling the receipt of payments from the CSC and their accounting.

8.2.3.14 Handle customer requests

This activity involves: handling of support requests, reports, and incidents from CSCs, however received. Customers can be provided with a variety of means to communicate, from forums through email, customer support desk system or web portals to real-time communication with provider support personnel.

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

8.2.3.15 Manage cloud services from secondary inter-cloud providers

This activity focuses on managing the usage of cloud services of a secondary inter-cloud service provider. This activity involves:

— selecting and using one or more services of a secondary inter-cloud service provider;

— monitoring and managing the secondary inter-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 secondary inter-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 secondary inter-cloud service provider, and by which users; including assurance that the use is appropriate and within the business plan;

— monitoring the integration of the cloud services of a secondary inter-cloud service provider with service implementations to ensure that business goals are being met;

— ensuring security and privacy protection obligations are met;

— coordinating identity and security credentials between the CSC and all the secondary inter-cloud service providers.

8.2.3.16 Perform intermediation, aggregation and arbitrage

This activity involves the use of secondary inter-cloud service provider's cloud services in particular ways:

— intermediation involves a CSP offering a cloud service which is based on conditioning or enhancing the cloud service of a secondary inter-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 CSP offering a cloud service which is based on the composition of a set of services provided by secondary inter-cloud service providers;

— arbitrage involves a CSP offering a cloud service which is based on selecting one service offering from a group offered by secondary inter-cloud service providers.

8.2.3.17 Manage security and risks

This 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;

— assessing information security risks relating to the cloud service and the approach to those risks that meets the business goals of the CSP. 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 CSC via the service agreement, in order to address the cost requirements of some part of the marketplace;

— making design decisions and selecting the associated information security controls required to address risks associated with the service provision and design decisions. 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 security of cloud services of secondary 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 CSP staff based on the particular CSCs tenants they provide service to.

8.2.3.18 Design and implement service continuity

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

8.2.3.19 Ensure compliance

This activity involves implementing regulatory compliance and standards conformance, including:

- ensuring that the implementation of the cloud service and its supporting infrastructure meets the requirements of any standards that need to be supported;
- ensuring that the implementation of the cloud service and its supporting infrastructure (including data handling) meets any regulatory obligations that can exist for the service or for the data that is stored or processed by the service.

8.2.3.20 Provide network connectivity

This activity involves the setting up of requested network connections and related capabilities, including (amongst others) connections between the CSC and the CSP's system and between one CSP's system and another CSP'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.

8.2.3.21 Deliver network services

This activity involves the provision of network related services such as firewalls or load balancing.

8.2.3.22 Provide network management services

This activity focuses on managing the network infrastructure used to carry cloud services. This activity provides methods, tools and procedures allowing 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 is replaced or upgraded with new functions;
- configuring resources in the network to support a cloud service.

8.2.4 Activities associated with the CSN role

8.2.4.1 Design, create and maintain service components

This 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.

8.2.4.2 Compose services

This 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, etc.);

— designing an interface to the CSC representing the composed services from across multiple CSP offerings;

— performing composition which can involve intermediation, aggregation or arbitrage of the existing services.

8.2.4.3 Test services

This 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 secondary cloud service provider;

— testing which should include checking that the connections to the CSP'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 CSP's data centre.

8.2.4.4 Perform audit

This 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;

— 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 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 CSP which includes security controls, privacy impact, performance, and other cloud service related cloud computing activities identified by the audit requestor. The request can come from the CSP itself, where the CSP wants proof of the quality of its cloud services which can then be presented to potential CSCs.

8.2.4.5 Report audit results

This activity involves providing a documented report of the results of performing an audit, for example on a given cloud service or on a CSP or on a CSC'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 can be given to the CSP, or possibly on request to a CSC, depending on the business situation or the legal context.

8.2.4.6 Acquire and assess customers

This activity includes the tasks required to market and sell cloud services up to the point where a CSC 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 customer;

— assessing the customer's needs and requirements for cloud services.

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

8.2.4.7 Assess marketplace

This 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 CSPs, obtaining both technical and business information;

— subscribing to and receiving notifications of changes to the content of CSPs' product catalogues;

— matching the product offerings to the customer's needs and requirements, including technical, business and regulatory aspects.

8.2.4.8 Set up legal agreement

This activity concerns the service agreement between the CSC and the chosen CSP(s). This involves negotiating the service agreement between the CSC and the chosen CSP(s), aiming to meet the customer's needs.

8.3 Cross-cutting aspects

8.3.1 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.

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

For the CCRA, the cross-cutting aspects shall be as described in ISO/IEC 22123-2:2023, Clause 7. The following clauses further elaborate on critical cross-cutting aspects.

8.3.2 Auditability

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 CSCs, CSPs and CSNs. 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 CSCs, the CSPs and the CSNs.

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.

8.3.3 Governance

The individual governance practices used by CSCs and CSPs 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 CSC to CSP relationship.

8.3.4 Interoperability

Interoperability in the context of cloud computing includes the ability of a CSC 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 CSC should be able to use widely available ICT facilities in-house when interacting with the 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 an CSP:primary inter-cloud provider relationship, or where a CSC 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 CSC with the cloud service management facilities of the CSP. Ideally, the CSC should have a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more CSPs 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.

8.3.5 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 CSP and maintenance performed by the CSC. In the case of a SaaS service, it is likely that virtually all maintenance actions are to be performed by the provider. In the case of IaaS and PaaS services, the application components belong to the CSC and the CSC 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 can 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 CSP 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.

8.3.6 Performance

Performance includes a set of non-functional facets, relating to the operation of a cloud service. The following can also apply:

— availability of the service;

— response time to complete service requests;

— data centre network IP address pool and/or virtual local area network (VLAN) range capacity.

Where the service involves running an application (IaaS, PaaS) then the same facets of performance apply to the behaviour of the application running in the CSP'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.

8.3.7 Portability

Portability is significant in cloud computing since prospective CSCs are interested in avoiding lock-in when they choose to use cloud services. CSCs need to know that they can move CSC data or their applications between multiple CSPs 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 CSC organization is considering moving from one IaaS CSP to another, the CSC 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 a SaaS environment, when a CSC organization wants to move a SaaS application to a different CSP (i.e. switch SaaS service providers), the CSC needs to

be able to take their data with them, but the rest of the switching cost can include exporting, mapping and importing the data into the new CSP's SaaS application, and that cost is a function of how well the data models and formats of the two SaaS CSPs line up. Ideally, SaaS CSPs should adopt standard data interchange format(s) relevant to their application domain. Changing between SaaS applications can also involve the CSC 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.

CSC data is a class of data objects under the control of the CSC. Cloud data portability allows the CSCs the ability to copy CSC data into or out of a cloud service by network access or 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 CSP to another CSP, or the migration of application components (PaaS service) from one CSP 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).

8.3.8 Protection of Personally Identifiable Information

Protection of PII is described in ISO/IEC 22123-2, 7.9.

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

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 CSCs using cloud services and for the CSPs.

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 CSCs and CSPs. Compliance with such requirements is often related to governance and risk management activities.

8.3.9 Reversibility

The principle of the "right to be forgotten" can also apply, in that the CSC has a right to expect that once they indicate to the CSP their intention to cease use of the service(s), there is an orderly process for the CSC to retrieve cloud service customer data and their application artefacts and that the CSP deletes all copies and does not retain any materials belonging to the CSC after an agreed period.

8.3.10 Security

8.3.10.1 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 CSPs, but also affects CSCs and CSNs.

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 CSPs' 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 CSC to the CSP (e.g. 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 CSCs, which affect both CSCs and CSPs. These threats are more fully described in other specifications, such as ISO/IEC 27018.

8.3.10.2 Distribution of security responsibilities

A CSP and a CSC 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, CSPs and CSCs collaboratively design, build, deploy, and operate cloud computing systems.

The split of control means that both roles now share the responsibilities in 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 CSPs and CSCs. 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 CSP meanwhile application user account management for the application deployed on that IaaS service is typically the responsibility of the CSC who deploys the application using the IaaS service. By contrast, for a SaaS application service, the account management controls for all types of users are in the hands of the CSP (although the CSC can provide capabilities such as third party authentication).

8.3.10.3 Cloud service category perspectives

A cloud service category defined in ISO/IEC 22123-1 is a group of cloud services that possess some common set of qualities. Cloud service categories present CSCs 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 VMs that are executed on hypervisors on the hosts, therefore, hypervisor security for achieving VM isolation has been studied extensively for IaaS CSPs that use virtualization technologies.

8.3.10.4 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 CSC organization, whereas a public cloud can 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 service can or cannot need additional boundary controllers at the cloud service boundary when the private cloud service is hosted on site within the CSC 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.

8.3.10.5 Data protection strategy and responsibility

Protection of data assumes a new dimension in cloud computing. An organization can opt to store its data in cloud service but then the data protection responsibility and accountability needs to be agreed upon clearly. The first step that the CSC 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).

Encryption is a potential technique to use but then key management has to be given consideration where the CSC or any third party manages the keys. If the keys are managed by the CSP then they are responsible for logical and physical control of the keys as well as the data.

8.3.11 Service levels and service level agreements

Service levels and service level agreements are described in ISO/IEC 22123-2, 7.14.

The cloud computing service level agreement (cloud SLA) is a service level agreement between a CSP and a CSC based on a taxonomy of cloud computing specific terms to set the quality of the cloud services delivered. It characterizes 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 (CSC and CSP and related sub-roles).

For instance, CSCs 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 SLA. A CSP can also list within the cloud SLA a set of promises explicitly not made to CSCs, i.e. limitations and obligations that CSCs 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 can 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 is to be handled in relation to the cloud services.

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

9.1.1 General

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 8.2 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.

9.1.2 Layering framework

9.1.2.1 General

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 11.

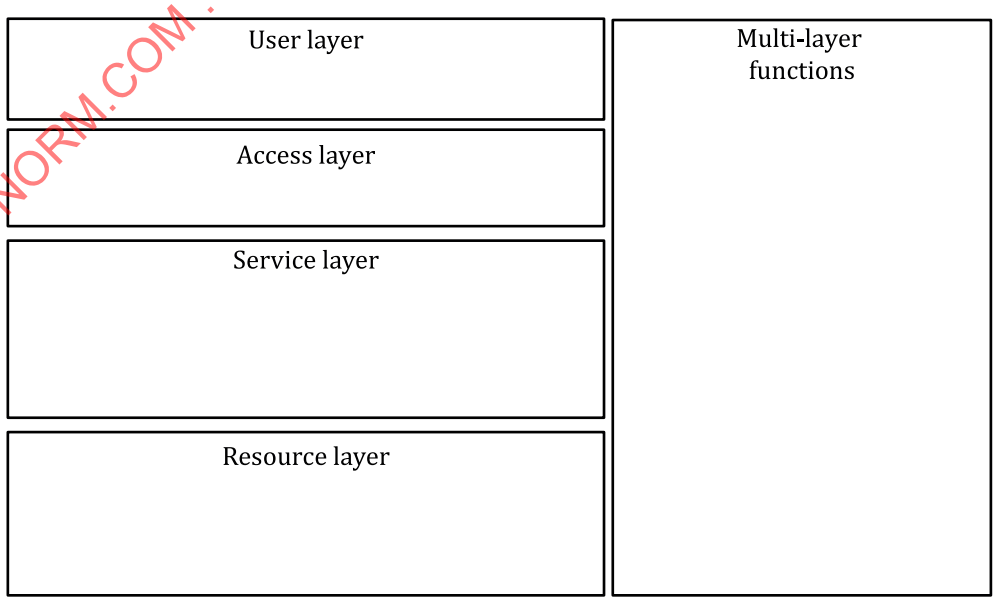

Figure 11 — Cloud computing layering framework

Each of the layers in the framework is described in the following sub-clauses.

9.1.2.2 User layer

The user layer is the user interface, through which a CSC role interacts with a CSP role and with cloud services, perform customer related administrative activities, and monitors cloud services.

NOTE The user layer represents all of the functions required for the interface between a CSU (a CSC:cloud service user) and any available cloud service.

9.1.2.3 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 CSP) 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 CSC or CSP's cloud service consumption requests to access CSPs' services and resources.

9.1.2.4 Service layer

The service layer contains the implementation of the services provided by a CSP. 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.

9.1.2.5 Resource layer

The resource layer includes equipment typically used in a data centre such as servers, network switches and routers, storage devices, and also the corresponding non-cloud-specific software such as host operating systems, hypervisors, device drivers and generic systems management software.

The resource layer also includes the cloud transport network functionality which is required to provide underlying connectivity between the CSP and the CSC(s), as well as within the CSP and among peer CSPs.

For a CSP to provide services consistent with the cloud SLA, the CSP can require dedicated and/or secure connections between CSUs and the CSP.

9.1.2.6 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 required functionality);

— development support capabilities (involving the creation, testing and lifecycle management of services and service components).

9.2 Functional components

9.2.1 General

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 12 presents a high level overview of the CCRA functional components organized by means of the layering framework.

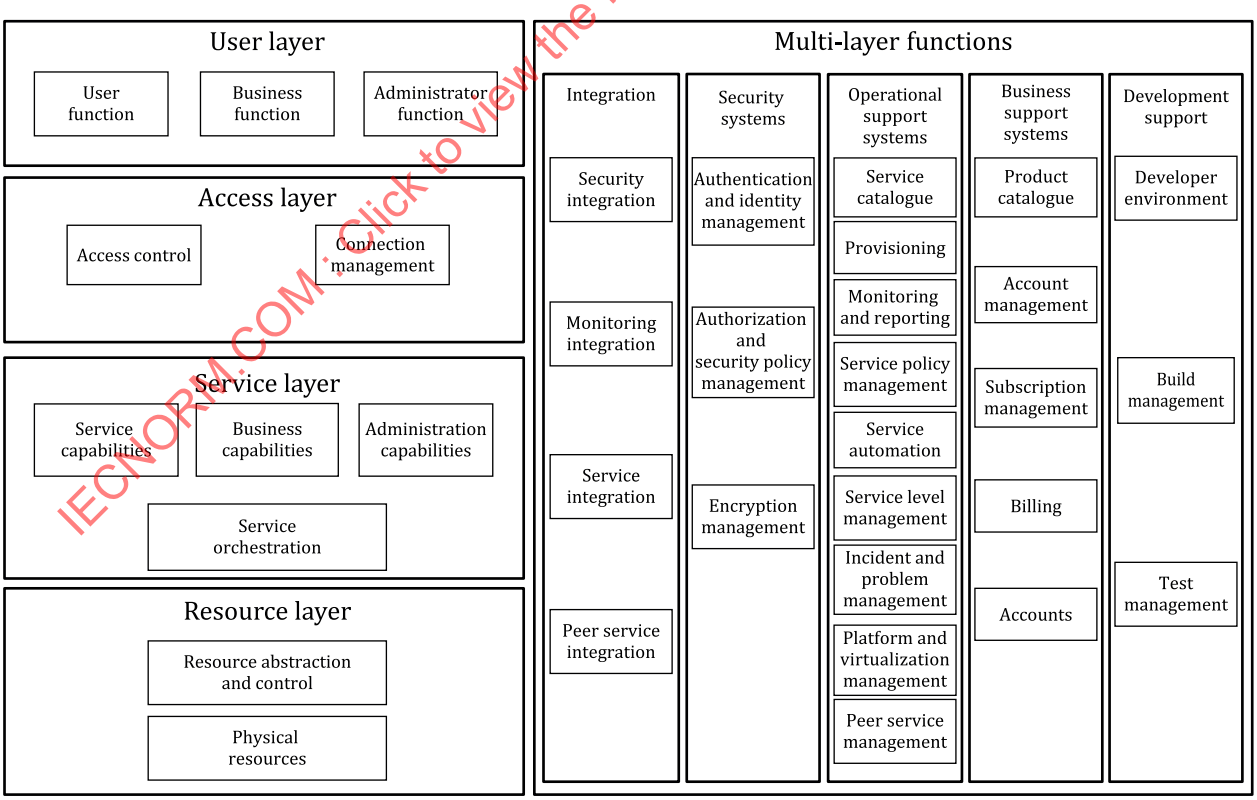

Figure 12 — Functional components of the CCRA

9.2.2 User layer functional components

9.2.2.1 General

The user layer functional components include:

— user function;

— business function;

— administration 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.

9.2.2.2 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 can be as simple as a browser running on a user device. However, in other cases, it can involve a sophisticated enterprise system running business processes, applications, middleware and associated infrastructure.

9.2.2.3 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.

9.2.2.4 Administration function

The administration 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.

9.2.3 Access layer functional components

9.2.3.1 General

The access layer functional components include:

— access control:

  — service access;

  — business access;

  — administration access;

  — development access.

— connection management.

9.2.3.2 Access control

Access control limits users to the use of particular services. Principally, access control involves 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.

9.2.3.3 Service access

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

9.2.3.4 Business access

The business access functional component provides access to business capabilities offered by the CSP, as implemented by the business support systems.

9.2.3.5 Administration access

The administration access functional component provides access to administration capabilities offered by the CSP, as implemented by the operational support systems.

9.2.3.6 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.

9.2.3.7 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.

9.2.4 Service layer functional components

9.2.4.1 General

The service layer **functional components** include:

— service capabilities;

— business capabilities;

— administration capabilities;

— service orchestration.

9.2.4.2 Service capabilities

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

9.2.4.3 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.

9.2.4.4 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.

9.2.4.5 Service orchestration

The service orchestration functional component provides coordination, aggregation and composition of multiple service components in order to deliver the cloud service. Service orchestration also specifies the required cloud resources and the dependencies between the resources.

9.2.5 Resource layer functional components

9.2.5.1 General

The resource layer **functional components** include:

— resource abstraction and control;

— physical resources.

9.2.5.2 Resource abstraction and control

The resource abstraction and control functional component is used by CSPs 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. Service orchestration also specifies the required cloud resources and the dependencies between the resources.

The resource abstraction and control functional component enables a CSP 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 9.2.6.3). 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 can 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 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.

9.2.5.3 Physical resources

The physical resources functional component represents the elements needed by the CSP 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. Typically, the operational support systems functional component itself runs on some part of the physical resources.

9.2.6 Multi-layer functions

9.2.6.1 Integration functional components

9.2.6.1.1 General

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.

9.2.6.1.2 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.

9.2.6.1.3 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.

9.2.6.1.4 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.

9.2.6.1.5 Peer service integration

The peer service integration functional component is used to connect to services of peer CSPs in a controlled fashion, with appropriate security and with appropriate accounting for the usage, linking back to the identity of the CSC. 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.

9.2.6.2 Security systems functional components

9.2.6.2.1 General

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

9.2.6.2.2 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 and unified authentication.

9.2.6.2.3 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.

9.2.6.2.4 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.

9.2.6.3 Operational support systems functional components

9.2.6.3.1 General

The operational support systems functional components encompass the set of operational related management capabilities 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.

9.2.6.3.2 Service catalogue

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

9.2.6.3.3 Provisioning

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

Provisioning also includes managing cloud resource requirements and allocating quotas.

9.2.6.3.4 Monitoring and reporting

The monitoring and reporting functional component provides capabilities for:

— monitoring the cloud computing activities of other functional components throughout the CSP'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 operational support systems (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 CSP'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 some task), or 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.

9.2.6.3.5 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 CSCs.

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.

9.2.6.3.6 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 CSC can be capable of being automated and need not require any intervention by the CSP.

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

9.2.6.3.7 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.

9.2.6.3.8 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 CSP's systems, or they can be detected and reported by CSCs.

9.2.6.3.9 Platform and virtualization management

The platform and virtualization management functional component provides the capabilities for managing the underlying resources of the CSP (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, licenses, energy use).

9.2.6.3.10 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 CSPs, 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 CSPs.

9.2.6.4 Business support systems components

9.2.6.4.1 General

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;

— metering and billing;

— accounts.

9.2.6.4.2 Product catalogue

The product catalogue functional component provides capabilities for CSCs 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 CSP. It can also serve as a service entry for cloud products for customers to create resources.

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.

9.2.6.4.3 Account management

The account management functional component provides capabilities for managing CSC 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.

9.2.6.4.4 Subscription management

The subscription management functional component handles subscriptions from CSCs 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.

9.2.6.4.5 Metering and billing

The metering and billing functional component has capabilities for:

— the metering and rating of the use of cloud services by CSCs - where metering is the measurement of the consumption of cloud services by each CSC 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 CSCs. Invoice data is also lodged with the accounts functional component and the account management functional component;

— metering management provides cloud resource order information and consumption details of CSCs. Order information records the order information about the CSC's creation, allocation and destruction of resources. The consumption details record the CSC's resource consumption information in each metering cycle;

— cost accounting and apportionment of cloud products and cloud services cost element arrangement, cost unit price calculation and cost apportionment.

9.2.6.4.6 Accounts

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

9.2.6.5 Development support functional components

9.2.6.5.1 General

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;