INTERNATIONAL STANDARD

ISO/IEC 22123-1

First edition
2021-02

Information technology — Cloud computing —

Part 1:
Vocabulary

Technologies de l'information — Informatique en nuage —

Partie 1: Vocabulaire

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

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

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

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

Introduction

This document is the definitive reference for cloud computing, providing a consolidated cloud computing vocabulary consisting of terms, terminology and definitions.

Information technology — Cloud computing —

Part 1:
Vocabulary

1 Scope

This document provides terms and definitions for vocabulary used in the field of cloud computing.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

3.1 General

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.2 Terms related to cloud computing foundation

3.2.1
cloud computing
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

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.2.2
cloud service
one or more capabilities offered via *cloud computing* (3.2.1) invoked using a defined interface

3.3 Terms related to cloud deployment models

3.3.1
cloud deployment model
way in which *cloud computing* (3.2.1) can be organized based on the control and sharing of physical or virtual resources

Note 1 to entry: The *cloud deployment models* include *community cloud* (3.3.2), *hybrid cloud* (3.3.3), *private cloud* (3.3.4) and *public cloud* (3.3.5).

3.3.2
community cloud
cloud deployment model ([3.3.1](#)) where *cloud services* ([3.2.2](#)) exclusively support and are shared by a specific collection of *cloud service customers* ([3.4.2](#)) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

3.3.3
hybrid cloud
cloud deployment model ([3.3.1](#)) using at least two different *cloud deployment models* ([3.3.1](#))

3.3.4
private cloud
cloud deployment model ([3.3.1](#)) where *cloud services* ([3.2.2](#)) are used exclusively by a single *cloud service customer* ([3.4.2](#)) and resources are controlled by that *cloud service customer* ([3.4.2](#))

3.3.5
public cloud
cloud deployment model ([3.3.1](#)) where *cloud services* ([3.2.2](#)) are potentially available to any *cloud service customer* ([3.4.2](#)) and resources are controlled by the *cloud service provider* ([3.4.3](#))

3.4   Terms related to cloud computing roles and activities

3.4.1
party
natural person or legal person, whether or not incorporated, or a group of either that can assume one or more *roles* ([3.4.11](#))

3.4.2
cloud service customer
CSC
party ([3.4.1](#)) which is in a business relationship for the purpose of using *cloud services* ([3.2.2](#))

Note 1 to entry: A business relationship does not necessarily imply financial agreements.

3.4.3
cloud service provider
CSP
party ([3.4.1](#)) which makes *cloud services* ([3.2.2](#)) available

3.4.4
cloud service user
CSU
natural person, or entity acting on their behalf, associated with a *cloud service customer* ([3.4.2](#)) that uses *cloud services* ([3.2.2](#))

Note 1 to entry: Examples of such entities include *devices* ([3.14.4](#)) and applications.

3.4.5
cloud service partner
CSN
party ([3.4.1](#)) which is engaged in support of, or auxiliary to, *activities* ([3.4.8](#)) of either the *cloud service provider* ([3.4.3](#)) or the *cloud service customer* ([3.4.2](#)), or both

3.4.6
cloud auditor
cloud service partner ([3.4.5](#)) with the responsibility to conduct an *audit* ([3.14.10](#)) of the provision and use of *cloud services* ([3.2.2](#))

3.4.7
cloud service broker
cloud service partner (3.4.5) that negotiates relationships between *cloud service customers* (3.4.2) and *cloud service providers* (3.4.3)

3.4.8
activity
specified pursuit or set of tasks

3.4.9
peer cloud service provider
secondary cloud service provider
cloud service provider (3.4.3) who provides one or more *cloud services* (3.2.2) for use by one or more other *cloud service providers* (3.4.3) as part of their *cloud services* (3.2.2)

3.4.10
functional component
functional building block needed to engage in an *activity* (3.4.8), backed by an implementation

3.4.11
role
set of *activities* (3.4.8) that serves a common purpose

3.4.12
sub-role
subset of the *activities* (3.4.8) of a given *role* (3.4.11)

3.4.13
device platform cloud service
cloud service (3.2.2) offered by the *device platform provider* (3.14.13) to support the *device platform* (3.14.5)

Note 1 to entry: An *application marketplace* (3.14.6) can be an example of *device platform* (3.14.5) *cloud service* (3.2.2).

3.4.14
cloud service developer
cloud service partner (3.4.5) with the responsibility for designing, developing, testing and maintaining the implementation of a *cloud service* (3.2.2)

3.5 Terms related to key cloud computing characteristics

3.5.1
measured service
metered delivery of *cloud services* (3.2.2) such that usage can be monitored, controlled, reported and billed

3.5.2
tenant
one or more *cloud service users* (3.4.4) sharing access to a set of physical and virtual resources

3.5.3
multi-tenancy
allocation of physical or virtual resources such that multiple *tenants* (3.5.2) and their computations and data are isolated from and inaccessible to one another

3.5.4
on-demand self-service
feature where a *cloud service customer* (3.4.2) can provision computing capabilities, as needed, automatically or with minimal interaction with the *cloud service provider* (3.4.3)

3.5.5
resource pooling
aggregation of a *cloud service provider's* ([3.4.3](#)) physical or virtual resources to serve one or more *cloud service customers* ([3.4.2](#))

3.6   Terms related to cloud capabilities types and cloud service categories

3.6.1
cloud capabilities type
classification of the functionality provided by a *cloud service* ([3.2.2](#)) to the *cloud service customer* ([3.4.2](#)), based on resources used

Note 1 to entry: The *cloud capabilities types* are *application capabilities type* ([3.6.2](#)), *infrastructure capabilities type* ([3.6.3](#)) and *platform capabilities type* ([3.6.4](#)).

3.6.2
application capabilities type
cloud capabilities type ([3.6.1](#)) in which the *cloud service customer* ([3.4.2](#)) can use the *cloud service provider's* ([3.4.3](#)) applications

3.6.3
infrastructure capabilities type
cloud capabilities type ([3.6.1](#)) in which the *cloud service customer* ([3.4.2](#)) can provision and use processing, storage or networking resources

3.6.4
platform capabilities type
cloud capabilities type ([3.6.1](#)) in which the *cloud service customer* ([3.4.2](#)) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the *cloud service provider* ([3.4.3](#))

3.6.5
cloud service category
group of *cloud services* ([3.2.2](#)) that possess some common set of qualities

Note 1 to entry: A *cloud service category* can include capabilities from one or more *cloud capabilities types* ([3.6.1](#)).

3.6.6
communications as a service
CaaS
cloud service category ([3.6.5](#)) in which the capability provided to the *cloud service customer* ([3.4.2](#)) is real time interaction and collaboration

Note 1 to entry: *CaaS* can provide both *application capabilities type* ([3.6.2](#)) and *platform capabilities type* ([3.6.4](#)).

3.6.7
compute as a service
CompaaS
cloud service category ([3.6.5](#)) in which the capabilities provided to the *cloud service customer* ([3.4.2](#)) are the provision and use of processing resources needed to deploy and run software

Note 1 to entry: To run some software, capabilities other than processing resources may be needed.

3.6.8
data storage as a service
DSaaS
cloud service category ([3.6.5](#)) in which the capability provided to the *cloud service customer* ([3.4.2](#)) is the provision and use of data storage and related capabilities

Note 1 to entry: *DSaaS* can provide any of the three *cloud capabilities types* ([3.6.1](#)).

3.6.9
infrastructure as a service
IaaS
cloud service category (3.6.5) in which the *cloud capabilities type* (3.6.1) provided to the *cloud service customer* (3.4.2) is an *infrastructure capabilities type* (3.6.3)

Note 1 to entry: The *cloud service customer* (3.4.2) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The *cloud service customer* (3.4.2) may also have limited ability to control certain networking components (e.g., host firewalls).

3.6.10
network as a service
NaaS
cloud service category (3.6.5) in which the capability provided to the *cloud service customer* (3.4.2) is transport connectivity and related network capabilities

Note 1 to entry: *NaaS* can provide any of the three *cloud capabilities types* (3.6.1).

3.6.11
platform as a service
PaaS
cloud service category (3.6.5) in which the *cloud capabilities type* (3.6.1) provided to the *cloud service customer* (3.4.2) is a *platform capabilities type* (3.6.4)

3.6.12
software as a service
SaaS
cloud service category (3.6.5) in which the *cloud capabilities type* (3.6.1) provided to the *cloud service customer* (3.4.2) is an *application capabilities type* (3.6.2)

3.7   Terms related to interoperability

3.7.1
interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

3.7.2
cloud interoperability
ability of a *CSC's* (3.4.2) system to interact with a *cloud service* (3.2.2), or the ability for one *cloud service* (3.2.2) to interact with other *cloud services* (3.2.2), by exchanging information according to a prescribed method to obtain predictable results

Note 1 to entry: *cloud service* (3.2.2) to *cloud service* (3.2.2) interactions occur through a *CSP* (3.4.3): inter-cloud provider relationship

3.7.3
transport interoperability
interoperability (3.7.1) where information exchange uses an established communication infrastructure between the participating systems

3.7.4
syntactic interoperability
interoperability (3.7.1) such that the formats of the exchanged information can be understood by the participating systems

3.7.5
semantic data interoperability
interoperability (3.7.1) so that the meaning of the data model within the context of a subject area is understood by the participating systems

5

3.7.6
behavioural interoperability
interoperability (3.7.1) so that the actual result of the exchange achieves the expected outcome

3.7.7
policy interoperability
interoperability (3.7.1) while complying with the legal, organizational, and policy frameworks applicable to the participating systems

3.8 Terms related to cloud service agreements

3.8.1
service level agreement
SLA
documented agreement between the service provider and customer that identifies services and service targets

Note 1 to entry: A *service level agreement* can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

Note 2 to entry: A *service level agreement* can be included in a contract or another type of documented agreement.

3.8.2
cloud service product
cloud service (3.2.2), allied to the set of business terms under which the *cloud service* (3.2.2) is offered

Note 1 to entry: Business terms can include pricing, rating, and service levels.

3.8.3
product catalogue
listing of all the *cloud service products* (3.8.2) which *cloud service providers* (3.4.3) make available to *cloud service customers* (3.4.2)

3.8.4
service catalogue
listing of all the *cloud services* (3.2.2) of a particular *cloud service provider* (3.4.3)

3.8.5
cloud service qualitative objective
SQO
commitment a *cloud service provider* (3.4.3) makes for a specific, qualitative characteristic of a *cloud service* (3.2.2), where the value follows the nominal scale or ordinal scale

Note 1 to entry: A *cloud service qualitative objective* may be expressed as an enumerated list.

Note 2 to entry: Qualitative characteristics typically require human interpretation.

Note 3 to entry: The ordinal scale allows for existence/nonexistence.

3.8.6
cloud service level agreement
cloud SLA
part of the *cloud service agreement* (3.8.8) that includes *cloud service level objectives* (3.8.7) and *cloud service qualitative objectives* (3.8.5) for the covered *cloud service(s)* (3.2.2)

3.8.7
cloud service level objective
SLO
commitment a *cloud service provider* (3.4.3) makes for a specific, quantitative characteristic of a *cloud service* (3.2.2), where the value follows the interval scale or ratio scale

Note 1 to entry: An SLO commitment may be expressed as a range.

3.8.8
cloud service agreement
documented agreement between the *cloud service provider* (3.4.3) and *cloud service customer* (3.4.2) that governs the covered *cloud service(s)* (3.2.2)

Note 1 to entry: A *cloud service agreement* can consist of one or more parts recorded in one or more documents.

3.8.9
metric
standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement

Note 1 to entry: A metric implements a particular abstract metric concept.

Note 2 to entry: A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific goal.

3.8.10
failure notification policy
policy specifying the processes by which the *cloud service customer* (3.4.2) and *cloud service partner* (3.4.5) can notify the *cloud service provider* (3.4.3) of a service outage and by which the *cloud service provider* (3.4.3) can notify the *cloud service customer* (3.4.2) and *cloud service partner* (3.4.5) that a service outage has occurred

Note 1 to entry: The policy may also include the process for providing updates on service outages, who receives notifications and updates, the maximum time between the detection of a service outage and the issuance of a notice of service outage, the maximum time interval between service outage updates and how service outage updates are described.

3.8.11
remedy
compensation available to the *cloud service customer* (3.4.2) in the event the *cloud service provider* (3.4.3) fails to meet a specified *cloud service level objective* (3.8.7)

Note 1 to entry: This definition of the term in English is based on the "legal reparation" meaning defined in The Shorter Oxford English Dictionary.

3.9   Terms related to portability

3.9.1
cloud application portability
ability to migrate an application from one *cloud service* (3.2.2) to another *cloud service* (3.2.2)

3.9.2
data portability
ability to easily transfer data from one system to another without being required to re-enter data

Note 1 to entry: It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy."

3.9.3
cloud data portability
data portability (3.9.2) from one *cloud service* (3.2.2) to another *cloud service* (3.2.2)

3.9.4
data syntactic portability
data portability (3.9.2) using data formats that can be decoded on the target

3.9.5
data semantic portability
data portability (3.9.2) such that the meaning of the data model is understood within the context of a subject area by the target

3.9.6
data policy portability
data portability (3.9.2) while complying with the legal, organizational and policy frameworks applicable to both the source and target

3.9.7
application portability
ability to migrate an application from a source system to a target system

3.9.8
application syntactic portability
application portability (3.9.7) where the format of the application artefacts can be decoded on the target

3.9.9
application instruction portability
application portability (3.9.7) so that the application's instruction set executes on the target

3.9.10
application metadata portability
application portability (3.9.7) so that the application's metadata is retained and understood on the target

3.9.11
application behaviour portability
application portability (3.9.7) so that execution on the target produces equivalent results to those produced on the source

3.9.12
application policy portability
application portability (3.9.7) while complying with the legal, organizational and policy frameworks applicable to the source and target

3.10 Terms related to cloud data

3.10.1
cloud service customer data
class of data objects under the control, by legal or other reasons, of the *cloud service customer* (3.4.2) that were input to the *cloud service* (3.2.2), or resulted from exercising the capabilities of the *cloud service* (3.2.2) by or on behalf of the *cloud service customer* (3.4.2) via the published interface of the *cloud service* (3.2.2)

Note 1 to entry: An example of legal controls is copyright.

Note 2 to entry: It may be that the *cloud service* (3.2.2) contains or operates on data that is not *cloud service customer data*; this might be data made available by the *cloud service providers* (3.4.3), or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the *cloud service customer* (3.4.2) using the capabilities of the *cloud service* (3.2.2) on this data is likely to be *cloud service customer data*, following the general principles of copyright, unless there are specific provisions in the *cloud service agreement* (3.8.8) to the contrary.

3.10.2
cloud service derived data
class of data objects under *cloud service provider* ([3.4.3](#)) control that are derived as a result of interaction with the *cloud service* ([3.2.2](#)) by the *cloud service customer* ([3.4.2](#))

Note 1 to entry: *Cloud service derived data* includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the *cloud service* ([3.2.2](#)) has such configuration and customization capabilities.

3.10.3
cloud service provider data
class of data objects, specific to the operation of the *cloud service* ([3.2.2](#)), under the control of the *cloud service provider* ([3.4.3](#))

Note 1 to entry: *Cloud service provider data* includes but is not limited to resource configuration and utilization information, *cloud service* ([3.2.2](#)) specific *virtual machine* ([3.13.2](#)), storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.10.4
account data
class of data specific to each *CSC* ([3.4.2](#)) that is required to administer the *cloud service* ([3.2.2](#))

Note 1 to entry: Account data is typically generated when a *cloud service* ([3.2.2](#)) is purchased and is under the control of the *CSP* ([3.4.3](#)).

Note 2 to entry: Account data consists of data elements provided by *CSC* ([3.4.2](#)), such as; name, address, telephone, etc.

3.10.5
end user identifiable information
EUII
derived data associated with a *CSC* ([3.4.2](#)) that is captured or generated from the use of the *cloud service* ([3.2.2](#)) by that *CSC* ([3.4.2](#))

3.10.6
mixed dataset
set of data objects that contain both *PII* ([3.11.4](#)) and *non-personal data* ([3.10.11](#))

3.10.7
individual data
class of data objects under the control, by legal or other reasons, of a natural person

Note 1 to entry: *Individual data* can be a *mixed dataset* ([3.10.6](#)).

Note 2 to entry: Customer content data is *individual data* when the *CSC* ([3.4.2](#)) is a natural person.

3.10.8
organizational data
class of data objects under the control, by legal, contractual or other reasons, of an organization

Note 1 to entry: An organization can be a for-profit company, a non-profit organization, a public or government agency, a non-governmental organization or an international organization, and can be small, medium or large.

Note 2 to entry: Customer content data is *organizational data* when the *CSC* ([3.4.2](#)) is an organization and thus not a natural person.

Note 3 to entry: *Cloud service provider data* ([3.10.3](#)) is always *organizational data* by nature.

Note 4 to entry: *Organizational data* can be a *mixed dataset* ([3.10.6](#)).

3.10.9
organizational protected data
OPD

organizational data ([3.10.8](#)) whose protection is required based on the policies established by governance of data process

Note 1 to entry: Organizations have policies that govern the data under their control. ISO/IEC 38505-1 identifies and examines higher level governance concerns regarding the use of data which is relevant from the perspective of governance of data.

Note 2 to entry: *Organizational data* ([3.10.8](#)) can contain *OPD* and *PII* ([3.11.4](#)).

3.10.10
public domain data

class of data objects over which nobody holds or can hold copyright or other intellectual property rights

Note 1 to entry: Data can be in the public domain in some jurisdictions, while not in others.

Note 2 to entry: The concept of public domain, and the difference between this and "publicly available" is both subtle and varies between jurisdictions. Readers should make themselves aware of the specific legal situation as it may apply to them.

3.10.11
non-personal data

class of data objects that does not contain *PII* ([3.11.4](#))

Note 1 to entry: data objects that were originally *PII* ([3.11.4](#)) and were later made anonymous are *non-personal data*

3.10.12
data principal

entity to which data relates

Note 1 to entry: The term "data principal" is broader than "PII principal" (or "data subject" as used elsewhere), and is able to denote any entity such as a person, an organization, a *device* ([3.14.4](#)), or a software application.

[SOURCE: ISO/IEC 20889:2018, 3.4]

3.10.13
transparency

open, comprehensive and understandable presentation of information

[SOURCE: ISO 21931-2:2019, 3.33]

3.11 Terms related to security and privacy

3.11.1
confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.11.2
integrity

property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.11.3
information security
preservation of *confidentiality* ([3.11.1](#)), *integrity* ([3.11.2](#)) and *availability* ([3.14.7](#)) of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.11.4
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: 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* ([3.4.1](#)), to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.11.5
secure multi-tenancy
type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance

Note 1 to entry: Secure multi-tenancy exists when the risk profile of an individual *tenant* ([3.5.2](#)) is no greater than it would be in a dedicated, single-tenant environment.

Note 2 to entry: In very secure environments even the identity of the *tenants* ([3.5.2](#)) is kept secret.

[SOURCE: ISO/IEC 27040:2015, 3.39]

3.12 Terms related to inter-cloud

3.12.1
inter-cloud computing
paradigm for enabling the interworking between two or more *cloud service providers* ([3.4.3](#)).

[SOURCE: Recommendation ITU-T Y.3511, 3.2.1]

3.12.2
primary cloud service provider
In *inter-cloud computing* ([3.12.1](#)), a *cloud service provider* ([3.4.3](#)) which is making use of *cloud services* ([3.2.2](#)) of *peer cloud service providers* ([3.4.9](#)) (i.e., *secondary cloud service providers* ([3.4.9](#))) as part of its own *cloud services* ([3.2.2](#))

[SOURCE: Recommendation ITU-T Y.3511, 3.2.2]

3.12.3
peer cloud service
cloud service ([3.2.2](#)) of one *cloud service provider* ([3.4.3](#)) which is used as part of a *cloud service* ([3.2.2](#)) of one or more other *cloud service providers* ([3.4.3](#))

3.13 Terms related to virtualization

3.13.1
virtual
not physically existing as such but made by software to appear to do so