
**Information technology — Cloud
computing —**

**Part 1:
Vocabulary**

*Technologies de l'information — Informatique en nuage —
Partie 1: Vocabulaire*



IECNORM.COM : Click to view the full PDF of ISO/IEC 22123-1:2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

ISO copyright office
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.....	iv
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
3.1 Terms related to cloud computing foundation.....	1
3.2 Terms related to cloud deployment models.....	2
3.3 Terms related to cloud computing roles and activities.....	3
3.4 Terms related to key cloud computing characteristics.....	4
3.5 Terms related to cloud capabilities types and cloud service categories.....	5
3.6 Terms related to interoperability.....	6
3.7 Terms related to cloud service agreements.....	7
3.8 Terms related to cloud portability.....	8
3.9 Terms related to cloud data.....	9
3.10 Terms related to security and privacy.....	12
3.11 Terms related to inter-cloud.....	12
3.12 Terms related to virtualization.....	12
3.13 Miscellaneous terms.....	13
3.14 Terms relating to multiplicity and organization of cloud services.....	15
Bibliography.....	16
Index.....	17

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).

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. 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 second edition of ISO/IEC 22123-1 cancels and replaces ISO/IEC 17788:2014 and ISO/IEC 22123-1:2021, which have been technically revised.

The main changes are as follows:

- the definition for hybrid cloud was changed;
- definitions for CSC role, CSP role, and CSN role were added;
- the definitions for CSC, CSP, and CSN were revised to leverage CSC role, CSP role, and CSN role, respectively;
- the ISO/IEC 27000 definitions for confidentiality, integrity, and information security were removed;
- the definition of inter-cloud computing was changed;
- terms relating to multi-cloud were added;
- peer cloud service and peer cloud service provider were replaced with secondary cloud service and secondary cloud service provider, respectively; and
- terms relating to multiplicity and organization of cloud services were added into a new subclause.

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 1: Vocabulary

1 Scope

This document defines terms used in the field of cloud computing.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 cloud computing foundation

3.1.1

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.

Note 2 to entry: Self-service provisioning refers to the provisioning of resources provided to *cloud services* (3.1.2) performed by *cloud service customers* (3.3.2) through automated means.

3.1.2

cloud service

one or more capabilities offered via *cloud computing* (3.1.1) invoked using a defined interface

3.1.3

cloud solution

cloud services (3.1.2) combined and controlled to meet *cloud service customer* (3.3.2) requirements

Note 1 to entry: A *cloud solution* can use any combination of *cloud deployment models* (3.2.1).

3.2 Terms related to cloud deployment models

3.2.1

cloud deployment model

way in which *cloud computing* (3.1.1) can be organized based on the control and sharing of physical or virtual resources

Note 1 to entry: Examples of *cloud deployment models* include *community cloud* (3.2.1), *hybrid cloud* (3.2.3), *private cloud* (3.2.4) and *public cloud* (3.2.5).

3.2.2

community cloud

cloud deployment model (3.2.1) where *cloud services* (3.1.2) exclusively support and are shared by a specific collection of *cloud service customers* (3.3.2) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

3.2.3

hybrid cloud

cloud deployment model (3.2.1) that uses a *private cloud* (3.2.4) and a *public cloud* (3.2.5)

3.2.4

private cloud

cloud deployment model (3.2.1) where *cloud services* (3.1.2) are used exclusively by a single *cloud service customer* (3.3.2) and resources are controlled by that *cloud service customer* (3.3.2)

3.2.5

public cloud

cloud deployment model (3.2.1) where *cloud services* (3.1.2) are potentially available to any *cloud service customer* (3.3.2) and resources are controlled by the *cloud service provider* (3.3.3)

3.2.6

multi-cloud

multicloud

cloud deployment model (3.2.1) in which a *cloud service customer* (3.3.2) uses *public cloud services* (3.1.2) provided by two or more *cloud service providers* (3.3.3)

Note 1 to entry: The *cloud service customer* (3.3.2) is responsible for integration and management of these *cloud services* (3.1.2) to form a *cloud solution* (3.1.3).

3.2.7

cloud service federation

two or more *cloud service providers* (3.3.3) bound together by an agreed set of policies, processes and trust in order to provide *cloud services* (3.1.2)

3.2.8

federated cloud

cloud deployment model (3.2.1) in which the *cloud services* (3.1.2) are provided by members of a *cloud service federation* (3.2.7)

3.2.9

hybrid multi-cloud

cloud deployment model (3.2.1) in which a *cloud service customer* (3.3.2) uses *cloud services* (3.1.2) from a *hybrid cloud* (3.2.3) and a *multi-cloud* (3.2.6)

3.2.10 inter-cloud intercloud

cloud deployment model (3.2.1) in which a *cloud service provider* (3.3.3) offers a *cloud service* (3.1.2) by using one or more *cloud services* (3.1.2) provided by other *cloud service providers* (3.3.3)

Note 1 to entry: The *primary cloud service provider* (3.11.2) provides the cloud service typically via intermediation, aggregation, or arbitrage of the cloud services provided by *secondary cloud service providers* (3.11.4).

3.3 Terms related to cloud computing roles and activities

3.3.1

party

natural person, legal person or a group of either, whether or not incorporated, that can assume one or more *roles* (3.3.10)

3.3.2

cloud service customer

CSC

party (3.3.1) that is acting in a *cloud service customer role* (3.3.14)

3.3.3

cloud service provider

CSP

party (3.3.1) that is acting in a *cloud service provider role* (3.3.15)

3.3.4

cloud service user

CSU

natural person, or entity acting on their behalf, associated with a *cloud service customer* (3.3.2) that uses *cloud services* (3.1.2)

Note 1 to entry: Examples of such entities include *devices* (3.13.4) and applications.

3.3.5

cloud service partner

CSN

party (3.3.1) that is acting in a *cloud service partner role* (3.3.16)

3.3.6

cloud auditor

cloud service partner (3.3.5) with the responsibility to conduct an *audit* (3.13.10) of the provision and use of *cloud services* (3.1.2)

3.3.7

cloud service broker

cloud service partner (3.3.5) that negotiates relationships between *cloud service customers* (3.3.2) and *cloud service providers* (3.3.3)

3.3.8

activity

specified pursuit or set of tasks

3.3.9

functional component

functional building block needed to engage in an *activity* (3.3.8), backed by an implementation

3.3.10

role

set of *activities* (3.3.8) that serves a common purpose

3.3.11

sub-role

subset of the *activities* (3.3.8) of a given *role* (3.3.10)

3.3.12

device platform cloud service

cloud service (3.1.2) offered by the *device platform provider* (3.13.13) to support the *device platform* (3.13.5)

Note 1 to entry: An *application marketplace* (3.13.6) can be an example of *device platform* (3.13.5) *cloud service* (3.1.2).

3.3.13

cloud service developer

cloud service partner (3.3.5) with the responsibility for designing, developing, testing and maintaining the implementation of a *cloud service* (3.1.2)

3.3.14

cloud service customer role

CSC role

set of *activities* (3.3.8) for the purpose of using *cloud services* (3.1.2)

3.3.15

cloud service provider role

CSP role

set of *activities* (3.3.8) that make *cloud services* (3.1.2) available

3.3.16

cloud service partner role

CSN role

set of *activities* (3.3.8) that support, or are auxiliary to, either the *cloud service provider role* (3.3.15) or the *cloud service customer role* (3.3.14), or both

3.4 Terms related to key cloud computing characteristics

3.4.1

measured service

metered delivery of *cloud services* (3.1.2) such that usage can be monitored, controlled, reported and billed

3.4.2

tenant

one or more *cloud service users* (3.3.4) sharing access to a set of physical and virtual resources

3.4.3

multi-tenancy

allocation of physical or virtual resources such that multiple *tenants* (3.4.2) and their computations and data are isolated from and inaccessible to one another

3.4.4

on-demand self-service

feature where a *cloud service customer* (3.3.2) can provision computing capabilities, as needed, automatically or with minimal interaction with the *cloud service provider* (3.3.3)

3.4.5

resource pooling

aggregation of a *cloud service provider's* (3.3.3) physical or virtual resources to serve one or more *cloud service customers* (3.3.2)

3.5 Terms related to cloud capabilities types and cloud service categories

3.5.1

cloud capabilities type

classification of the functionality provided by a *cloud service* (3.1.2) to the *cloud service customer* (3.3.2), based on resources used

Note 1 to entry: The *cloud capabilities types* are *application capabilities type* (3.5.2), *infrastructure capabilities type* (3.5.3) and *platform capabilities type* (3.5.4).

3.5.2

application capabilities type

cloud capabilities type (3.5.1) in which the *cloud service customer* (3.3.2) can use the *cloud service provider's* (3.3.3) applications

3.5.3

infrastructure capabilities type

cloud capabilities type (3.5.1) in which the *cloud service customer* (3.3.2) can provision and use processing, storage or networking resources

3.5.4

platform capabilities type

cloud capabilities type (3.5.1) in which the *cloud service customer* (3.3.2) 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* (3.3.3)

3.5.5

cloud service category

group of *cloud services* (3.1.2) 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* (3.5.1).

3.5.6

communications as a service

CaaS

cloud service category (3.5.5) in which the capability provided to the *cloud service customer* (3.3.2) is real time interaction and collaboration

Note 1 to entry: CaaS can provide both *application capabilities type* (3.5.2) and *platform capabilities type* (3.5.4).

3.5.7

compute as a service

CompaaS

cloud service category (3.5.5) in which the capabilities provided to the *cloud service customer* (3.3.2) 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 are potentially needed.

3.5.8

data storage as a service

DSaaS

cloud service category (3.5.5) in which the capability provided to the *cloud service customer* (3.3.2) 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* (3.5.1).

3.5.9

infrastructure as a service

IaaS

cloud service category (3.5.5) in which the cloud capabilities type (3.5.1) provided to the cloud service customer (3.3.2) is an infrastructure capabilities type (3.5.3)

Note 1 to entry: The *cloud service customer (3.3.2)* 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 (3.3.2)* can also have limited ability to control certain networking components (e.g., host firewalls).

3.5.10

network as a service

NaaS

cloud service category (3.5.5) in which the capability provided to the cloud service customer (3.3.2) is transport connectivity and related network capabilities

Note 1 to entry: *Network as a service* can provide any of the three *cloud capabilities types (3.5.1)*.

3.5.11

platform as a service

PaaS

cloud service category (3.5.5) in which the cloud capabilities type (3.5.1) provided to the cloud service customer (3.3.2) is a platform capabilities type (3.5.4)

3.5.12

software as a service

SaaS

cloud service category (3.5.5) in which the cloud capabilities type (3.5.1) provided to the cloud service customer (3.3.2) is an application capabilities type (3.5.2)

3.6 Terms related to interoperability

3.6.1

interoperability

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

3.6.2

cloud interoperability

ability of a *cloud service customer's (3.3.2)* system to interact with a *cloud service (3.1.2)*, or the ability for one *cloud service (3.1.2)* to interact with other *cloud services (3.1.2)*, by exchanging information according to a prescribed method to obtain predictable results

3.6.3

transport interoperability

interoperability (3.6.1) where information exchange uses an established communication infrastructure between the participating systems

3.6.4

syntactic interoperability

interoperability (3.6.1) such that the formats of the exchanged information can be understood by the participating systems

3.6.5

semantic data interoperability

interoperability (3.6.1) so that the meaning of the data model within the context of a subject area is understood by the participating systems

3.6.6**behavioural interoperability**

interoperability (3.6.1) so that the actual result of the exchange achieves the expected outcome

3.6.7**policy interoperability**

interoperability (3.6.1) while complying with the legal, organizational, and policy frameworks applicable to the participating systems

3.7 Terms related to cloud service agreements**3.7.1****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.

3.7.2**cloud service product**

cloud service (3.1.2), allied to the set of business terms under which the *cloud service* (3.1.2) is offered

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

3.7.3**product catalogue**

listing of all the *cloud service products* (3.7.2) which *cloud service providers* (3.3.3) make available to *cloud service customers* (3.3.2)

3.7.4**service catalogue**

listing of all the *cloud services* (3.1.2) of a particular *cloud service provider* (3.3.3)

3.7.5**cloud service qualitative objective****cloud SQO**

commitment a *cloud service provider* (3.3.3) makes for a specific, qualitative characteristic of a *cloud service* (3.1.2), where the value follows the nominal scale or ordinal scale

Note 1 to entry: A *cloud service qualitative objective* can 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.

3.7.6**cloud service level agreement****cloud SLA**

part of the *cloud service agreement* (3.7.8) that includes *cloud service level objectives* (3.7.7) and *cloud service qualitative objectives* (3.7.5) for the covered *cloud service(s)* (3.1.2)

Note 1 to entry: A *cloud service level agreement* is a *service level agreement* (3.7.1) used in the context of *cloud computing* (3.1.1).

3.7.7

cloud service level objective

cloud SLO

commitment a *cloud service provider* (3.3.3) makes for a specific, quantitative characteristic of a *cloud service* (3.1.2), where the value follows the interval scale or ratio scale

Note 1 to entry: A *cloud service level objective* commitment can be expressed as a range.

3.7.8

cloud service agreement

documented agreement between the *cloud service provider* (3.3.3) and *cloud service customer* (3.3.2) that governs the covered *cloud service(s)* (3.1.2)

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

3.7.9

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.

3.7.10

failure notification policy

policy specifying the processes by which the *cloud service customer* (3.3.2) and *cloud service partner* (3.3.5) can notify the *cloud service provider* (3.3.3) of a service outage and by which the *cloud service provider* (3.3.3) can notify the *cloud service customer* (3.3.2) and *cloud service partner* (3.3.5) that a service outage has occurred

Note 1 to entry: The policy can 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.

3.7.11

remedy

compensation available to the *cloud service customer* (3.3.2) in the event the *cloud service provider* (3.3.3) fails to meet a specified *cloud service level objective* (3.7.7)

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.

3.8 Terms related to cloud portability

3.8.1

cloud application portability

ability to migrate an application from one *cloud service* (3.1.2) to another *cloud service* (3.1.2)

3.8.2

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 can 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 can 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 cannot be described as "easy."

3.8.3**cloud data portability**

data portability (3.8.2) from one *cloud service* (3.1.2) to another *cloud service* (3.1.2)

3.8.4**data syntactic portability**

data portability (3.8.2) using data formats that can be decoded on the target

3.8.5**data semantic portability**

data portability (3.8.2) such that the meaning of the data model is understood within the context of a subject area by the target

3.8.6**data policy portability**

data portability (3.8.2) while complying with the legal, organizational and policy frameworks applicable to both the source and target

3.8.7**application portability**

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

3.8.8**application syntactic portability**

application portability (3.8.7) where the format of the application artefacts can be decoded on the target

3.8.9**application instruction portability**

application portability (3.8.7) so that the application's instruction set executes on the target

3.8.10**application metadata portability**

application portability (3.8.7) so that the application's metadata is retained and understood on the target

3.8.11**application behaviour portability**

application portability (3.8.7) so that execution on the target produces equivalent results to those produced on the source

3.8.12**application policy portability**

application portability (3.8.7) while complying with the legal, organizational and policy frameworks applicable to the source and target

3.9 Terms related to cloud data**3.9.1****cloud service customer data**

class of data objects under the control, by legal or other reasons, of the *cloud service customer* (3.3.2) that were input to the *cloud service* (3.1.2), or resulted from exercising the capabilities of the *cloud service* (3.1.2) by or on behalf of the *cloud service customer* (3.3.2) via the published interface of the *cloud service* (3.1.2)

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

Note 2 to entry: It can be that the *cloud service* (3.1.2) contains or operates on data that is not *cloud service customer data*; this can be data made available by the *cloud service providers* (3.3.3), or obtained from another source, or it can be publicly available data. However, any output data produced by the actions of the *cloud service customer* (3.3.2) using the capabilities of the *cloud service* (3.1.2) 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* (3.7.8) to the contrary.

3.9.2

cloud service derived data

class of data objects under *cloud service provider* (3.3.3) control that are derived as a result of interaction with the *cloud service* (3.1.2) by the *cloud service customer* (3.3.2)

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* (3.1.2) has such configuration and customization capabilities.

3.9.3

cloud service provider data

class of data objects, specific to the operation of the *cloud service* (3.1.2), under the control of the *cloud service provider* (3.3.3)

Note 1 to entry: *Cloud service provider data* includes but is not limited to resource configuration and utilization information, *cloud service* (3.1.2) specific *virtual machine* (3.12.2), storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.9.4

account data

class of data specific to each *cloud service customer* (3.3.2) that is required to administer the *cloud service* (3.1.2)

Note 1 to entry: Account data is typically generated when a *cloud service* (3.1.2) is purchased and is under the control of the *cloud service provider* (3.3.3).

Note 2 to entry: Account data consists of data elements provided by *cloud service customer* (3.3.2), such as; name, address, telephone, etc.

3.9.5

end user identifiable information

EUII

derived data associated with a *cloud service customer* (3.3.2) that is captured or generated from the use of the *cloud service* (3.1.2) by that *cloud service customer* (3.3.2)

3.9.6

mixed dataset

set of data objects that contain both *personally identifiable information* (3.10.1) and *non-personal data* (3.9.11)

3.9.7

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* (3.9.6).

Note 2 to entry: Customer content data is *individual data* when the *cloud service customer* (3.3.2) is a natural person.

3.9.8**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 *cloud service customer* (3.3.2) is an organization and thus not a natural person.

Note 3 to entry: *Cloud service provider data* (3.9.3) is always *organizational data* by nature.

Note 4 to entry: *Organizational data* can be a *mixed dataset* (3.9.6).

3.9.9**organizational protected data****OPD**

organizational data (3.9.8) 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* (3.9.8) can contain *organizational protected data* and *personally identifiable information* (3.10.1).

3.9.10**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 are encouraged to make themselves aware of the specific legal situation applicable to them.

3.9.11**non-personal data**

class of data objects that does not contain *personally identifiable information* (3.10.1)

Note 1 to entry: Data objects that were originally *personally identifiable information* (3.10.1) and were later made anonymous are *non-personal data*

3.9.12**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* (3.13.4), or a software application.

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

3.9.13**transparency**

open, comprehensive and understandable presentation of information

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

3.10 Terms related to security and privacy

3.10.1

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, to identify that natural person.

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

3.10.2

secure multi-tenancy

type of *multi-tenancy* (3.5.3) 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.

3.11 Terms related to inter-cloud

3.11.1

inter-cloud computing

paradigm for enabling the interworking between a *primary cloud service provider* (3.11.2) and one or more *secondary cloud service providers* (3.11.4)

3.11.2

primary cloud service provider

in *inter-cloud computing* (3.11.1), a *cloud service provider* (3.3.3) which is making use of *cloud services* (3.1.2) of *secondary cloud service providers* (3.11.4) as part of its own *cloud services* (3.1.2)

3.11.3

secondary cloud service

cloud service (3.1.2) of one *cloud service provider* (3.3.3) which is used as part of a *cloud service* (3.1.2) of one or more other *cloud service providers* (3.3.3)

3.11.4

secondary cloud service provider

cloud service provider (3.3.3) who provides one or more *cloud services* (3.1.2) for use by one or more other *cloud service providers* (3.3.3) as part of their *cloud services* (3.1.2)

3.12 Terms related to virtualization

3.12.1

virtual

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

3.12.2

virtual machine

VM

isolated execution environment for running software that uses virtualized physical resources

Note 1 to entry: Virtualized physical resources can include processor, memory, storage, I/O devices and network connections.

3.12.3**hypervisor****virtual machine monitor**

software that virtualizes physical resources and allows for running *virtual machines* ([3.12.2](#))

3.12.4**container**

isolated execution environment for running software that uses a virtualized operating system kernel

3.12.5**container image**

package of software that can run within a *container* ([3.12.4](#))

Note 1 to entry: Typically, it includes dependencies except for the operating system kernel.

3.13 Miscellaneous terms**3.13.1****architecture**

fundamental concepts or properties of an entity in its environment and governing principles for the realization and evolution of this entity and its related life cycle processes

[SOURCE: ISO/IEC/IEEE 42010:2022, 3.2]

3.13.2**accessibility**

usability of a product, service, environment or facility by people within the widest range of capabilities

Note 1 to entry: The concept of accessibility addresses the full range of user capabilities and is not limited to users who are formally recognized as having disability.

Note 2 to entry: The usability-oriented concept of accessibility aims to achieve levels of effectiveness, efficiency and satisfaction that are as high as possible considering the specified context of use, while paying attention to the full range of capabilities within the user population.

Note 3 to entry: It is important in the context of ISO/IEC 19086 to distinguish between the specialized meaning of “accessibility” as defined here and the term “accessible” which is used with its dictionary meaning of “able to be reached or entered”.

3.13.3**application cloud service**

cloud service ([3.1.2](#)) that supports applications running on a given *device* ([3.13.4](#)), where the *cloud service* ([3.1.2](#)) is provided by a *party* ([3.3.1](#)) other than the *device platform provider* ([3.13.13](#))

3.13.4**device**

physical entity that communicates directly or indirectly with one or more *cloud services* ([3.1.2](#))

Note 1 to entry: This definition relates to *devices* that use a *cloud service* ([3.1.2](#)), not a general definition for all types of *devices*.

3.13.5**device platform**

operating system and related feature set that provide the core capabilities for a *device* ([3.13.4](#))

Note 1 to entry: An *application marketplace* ([3.13.6](#)) is specific to a *device platform*.

3.13.6

application marketplace

set of *cloud services* (3.1.2) providing a digital marketplace intended to offer applications and other digital content for a particular *device platform* (3.13.5) allowing users to browse and download applications and other content

Note 1 to entry: An *application marketplace* can be offered to the public, or to private groups such as a corporate environment.

Note 2 to entry: A *device* (3.13.4) can use more than one *application marketplace*.

3.13.7

availability

ability to be in a state to perform as required

Note 1 to entry: *Availability* depends upon the combined characteristics of the reliability, recoverability, and maintainability of the item, and the maintenance support performance.

3.13.8

reversibility

process for *cloud service customers* (3.3.2) to retrieve their *cloud service customer data* (3.9.1) and application artefacts and for the *cloud service provider* (3.3.3) to delete all *cloud service customer data* (3.9.1) as well as contractually specified *cloud service derived data* (3.9.2) after an agreed period

3.13.9

resilience

ability of a *cloud service* (3.1.2) to recover operational condition quickly after a fault occurs

3.13.10

audit

systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself.

Note 2 to entry: External audits include those generally called second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing organizations, such as those providing certification/registration of conformity or governmental agencies.

[SOURCE: ISO 19011:2018, 3.1]

3.13.11

auditability

capability of collecting and making available necessary evidential information related to the operation and use of a *cloud service* (3.1.2), for the purpose of conducting an *audit* (3.13.10)

3.13.12

cloud native application

application that is explicitly designed to run within and to take advantage of the capabilities and environment of *cloud services* (3.1.2)

3.13.13

device platform provider

device platform cloud service provider

cloud service provider (3.3.3) that provides *cloud services* (3.1.2) necessary to support a *device platform* (3.13.5) including managing needed digital identities

Note 1 to entry: The *cloud service provider* (3.3.3) that offers the *application marketplace* (3.13.6) is typically the same as the *device platform provider*, but it is not required to be.

3.14 Terms relating to multiplicity and organization of cloud services

3.14.1

affinity

resource affinity

placement of two or more resources close to each other

Note 1 to entry: Closeness relates to factors such as speed of access or high bandwidth of access between the resources.

3.14.2

geo-dispersion

resource geo-dispersion

placement of two or more resources so that they are geographically separated from each other

Note 1 to entry: Separation relates to factors such as external physical events not applying to all of the separated resources.

3.14.3

availability domain or zone

logically and physically isolated location within a *cloud region* ([3.14.4](#))

3.14.4

cloud region

region

geographical area containing a set of physical resources used by cloud services that are independent and isolated from the physical resources contained in other geographical areas