INTERNATIONAL STANDARD

ISO/IEC 17788

First edition
2014-10-15

Information technology — Cloud computing — Overview and vocabulary

Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 17788:2014(E)

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

Published in Switzerland

CONTENTS

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17788 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Distributed application platforms and services (DAPS)*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. Y.3500 (08/2014).

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Cloud computing – Overview and vocabulary

1 Scope

This Recommendation | International Standard provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards.

This Recommendation | International Standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

2 Normative references

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

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation | International Standard uses the following terms defined elsewhere.

The following terms are defined in ISO/IEC 27000:

3.1.1 **availability**: Property of being accessible and usable upon demand by an authorized entity.

3.1.2 **confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.1.3 **information security**: Preservation of **confidentiality** (3.1.2), **integrity** (3.1.4) and **availability** (3.1.1) of information.

NOTE – In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

3.1.4 **integrity**: Property of accuracy and completeness.

The following term is defined in Rec. ITU-T Y.101:

3.1.5 **interoperability**: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

The following term is defined in ISO/IEC 27729:

3.1.6 **party**: Natural person or legal person, whether or not incorporated, or a group of either.

The following term is defined in ISO/IEC 20000-1:

3.1.7 service level agreement (SLA): Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – 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 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation | International Standard

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

3.2.1 application capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can use the **cloud service provider's** (3.2.15) applications.

3.2.2 cloud application portability: Ability to migrate an application from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).

3.2.3 cloud auditor: **Cloud service partner** (3.2.14) with the responsibility to conduct an audit of the provision and use of **cloud services** (3.2.8).

3.2.4 cloud capabilities type: Classification of the functionality provided by a **cloud service** (3.2.8) to the **cloud service customer** (3.2.11), based on resources used.

NOTE – The **cloud capabilities types** are **application capabilities type** (3.2.1), **infrastructure capabilities type** (3.2.25) and **platform capabilities type** (3.2.31).

3.2.5 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 – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.2.6 cloud data portability: **Data portability** (3.2.21) from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).

3.2.7 cloud deployment model: Way in which **cloud computing** (3.2.5) can be organized based on the control and sharing of physical or virtual resources.

NOTE – The **cloud deployment models** include **community cloud** (3.2.19), **hybrid cloud** (3.2.23), **private cloud** (3.2.32) and **public cloud** (3.2.33).

3.2.8 cloud service: One or more capabilities offered via **cloud computing** (3.2.5) invoked using a defined interface.

3.2.9 cloud service broker: **Cloud service partner** (3.2.14) that negotiates relationships between **cloud service customers** (3.2.11) and **cloud service providers** (3.2.15).

3.2.10 cloud service category: Group of **cloud services** (3.2.8) that possess some common set of qualities.

NOTE – A **cloud service category** can include capabilities from one or more **cloud capabilities types** (3.2.4).

3.2.11 cloud service customer: **Party** (3.1.6) which is in a business relationship for the purpose of using **cloud services** (3.2.8).

NOTE – A business relationship does not necessarily imply financial agreements.

3.2.12 cloud service customer data: Class of data objects under the control, by legal or other reasons, of the **cloud service customer** (3.2.11) that were input to the **cloud service** (3.2.8), or resulted from exercising the capabilities of the **cloud service** (3.2.8) by or on behalf of the **cloud service customer** (3.2.11) via the published interface of the **cloud service** (3.2.8).

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the **cloud service** (3.2.8) contains or operates on data that is not **cloud service customer data**; this might be data made available by the **cloud service providers** (3.2.15), 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** (3.2.11) using the capabilities of the **cloud service** (3.2.8) on this data is likely to be **cloud service customer data** (3.2.12), following the general principles of copyright, unless there are specific provisions in the **cloud service** (3.2.8) agreement to the contrary.

3.2.13 cloud service derived data: Class of data objects under **cloud service provider** (3.2.15) control that are derived as a result of interaction with the **cloud service** (3.2.8) by the **cloud service customer** (3.2.11).

NOTE – **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** (3.2.8) has such configuration and customization capabilities.

3.2.14 cloud service partner: **Party** (3.1.6) which is engaged in support of, or auxiliary to, activities of either the **cloud service provider** (3.2.15) or the **cloud service customer** (3.2.11), or both.

3.2.15 cloud service provider: **Party** (3.1.6) which makes **cloud services** (3.2.8) available.

3.2.16 cloud service provider data: Class of data objects, specific to the operation of the **cloud service** (3.2.8), under the control of the **cloud service provider** (3.2.15).

NOTE – **Cloud service provider data** includes but is not limited to resource configuration and utilization information, **cloud service** (3.2.8) specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.2.17 cloud service user: Natural person, or entity acting on their behalf, associated with a **cloud service customer** (3.2.11) that uses **cloud services** (3.2.8).

NOTE – Examples of such entities include devices and applications.

3.2.18 Communications as a Service (CaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is real time interaction and collaboration.

NOTE – **CaaS** can provide both **application capabilities type** (3.2.1) and **platform capabilities type** (3.2.31).

3.2.19 community cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) exclusively support and are shared by a specific collection of **cloud service customers** (3.2.11) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.2.20 Compute as a Service (CompaaS): **Cloud service category** (3.2.10) in which the capabilities provided to the **cloud service customer** (3.2.11) are the provision and use of processing resources needed to deploy and run software.

NOTE – To run some software, capabilities other than processing resources may be needed.

3.2.21 data portability: Ability to easily transfer data from one system to another without being required to re-enter data.

NOTE – 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".

3.2.22 Data Storage as a Service (DSaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is the provision and use of data storage and related capabilities.

NOTE – **DSaaS** can provide any of the three **cloud capabilities types** (3.2.4).

3.2.23 hybrid cloud: **Cloud deployment model** (3.2.7) using at least two different **cloud deployment models** (3.2.7).

3.2.24 Infrastructure as a Service (IaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is an **infrastructure capabilities type** (3.2.25).

NOTE – The **cloud service customer** (3.2.11) 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** (3.2.11) may also have limited ability to control certain networking components (e.g., host firewalls).

3.2.25 infrastructure capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can provision and use processing, storage or networking resources.

3.2.26 measured service: Metered delivery of **cloud services** (3.2.8) such that usage can be monitored, controlled, reported and billed.

3.2.27 multi-tenancy: Allocation of physical or virtual resources such that multiple **tenants** (3.2.37) and their computations and data are isolated from and inaccessible to one another.

3.2.28 Network as a Service (NaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is transport connectivity and related network capabilities.

NOTE – **NaaS** can provide any of the three **cloud capabilities types** (3.2.4).

3.2.29 on-demand self-service: Feature where a **cloud service customer** (3.2.11) can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider** (3.2.15).

3.2.30 Platform as a Service (PaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is a **platform capabilities type** (3.2.31).

3.2.31 platform capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) 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** (3.2.15).

3.2.32 private cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are used exclusively by a single **cloud service customer** (3.2.11) and resources are controlled by that **cloud service customer** (3.2.11).

3.2.33 public cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are potentially available to any **cloud service customer** (3.2.11) and resources are controlled by the **cloud service provider** (3.2.15).

3.2.34 resource pooling: Aggregation of a **cloud service provider's** (3.2.15) physical or virtual resources to serve one or more **cloud service customers** (3.2.11).

3.2.35 reversibility: Process for **cloud service customers** (3.2.11) to retrieve their **cloud service customer data** (3.2.12) and application artefacts and for the **cloud service provider** (3.2.15) to delete all **cloud service customer data** (3.2.12) as well as contractually specified **cloud service derived data** (3.2.13) after an agreed period.

3.2.36 Software as a Service (SaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is an **application capabilities type** (3.2.1).

3.2.37 tenant: One or more **cloud service users** (3.2.17) sharing access to a set of physical and virtual resources.

4 Abbreviations

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

CaaS	Communications as a Service
CompaaS	Compute as a Service
DSaaS	Data Storage as a Service
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
NaaS	Network as a Service
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SLA	Service Level Agreement

5 Conventions

References to terms defined in clause 3 are shown in bold.

6 Cloud computing overview

6.1 General

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. 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 that are briefly described in this clause 6.

6.2 Key characteristics

Cloud computing is an evolving paradigm. This clause 6.2 identifies and describes key characteristics of **cloud computing** and is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

Key characteristics of **cloud computing** are:

- ***Broad network access***: A feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that **cloud computing** offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops, and workstations;
- ***Measured service***: A feature where the metered delivery of **cloud services** is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered **cloud service**. The focus of this key characteristic is that the customer may only pay for the resources that they use. From the customers' perspective, **cloud computing** offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one;
- ***Multi-tenancy***: A feature where physical or virtual resources are allocated in such a way that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of **multi-tenancy**, the group of **cloud service users** that form a **tenant** will all belong to the same **cloud service customer** organization. There might be cases where the group of **cloud service users** involves users from multiple different **cloud service customers**, particularly in the case of **public cloud** and **community cloud** deployments. However, a given **cloud service customer** organization might have many different tenancies with a single **cloud service provider** representing different groups within the organization;
- ***On-demand self-service***: A feature where a **cloud service customer** can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider**. The focus of this key characteristic is that **cloud computing** offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead;
- ***Rapid elasticity and scalability***: A feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the **cloud service customer**, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the focus of this key characteristic is that **cloud computing** means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning;
- ***Resource pooling***: A feature where a **cloud service provider's** physical or virtual resources can be aggregated in order to serve one or more **cloud service customers**. The focus of this key characteristic is that **cloud service providers** can support **multi-tenancy** while at the same time using abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workload, such as maintenance requirements, to the provider. Even with this level of abstraction, it should be pointed out that users might still be able to specify location at a higher level of abstraction (e.g., country, state, or data centre).

6.3 Cloud computing roles and activities

Within the context of **cloud computing**, it is often necessary to differentiate requirements and issues for certain **parties**. These **parties** are entities that play roles (and sub-roles). Roles, in turn, are sets of activities and activities themselves are implemented by components. All **cloud computing** related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services. It is important to note that a **party** may play more than one role at any given point in time and may only engage in a specific subset of activities of that role.

The major roles of **cloud computing** are:

- ***Cloud service customer***: A **party** which is in a business relationship for the purpose of using **cloud services**. The business relationship is with a **cloud service provider** or a **cloud service partner**. Key activities for a **cloud service customer** include, but are not limited to, using **cloud services**, performing business administration, and administering use of **cloud services**;
- ***Cloud service partner***: A **party** which is engaged in support of, or auxiliary to, activities of either the **cloud service provider** or the **cloud service customer**, or both. A **cloud service partner's** activities vary depending on the type of partner and their relationship with the **cloud service provider** and the **cloud service customer**. Examples of **cloud service partners** include **cloud auditor** and **cloud service broker**;

– ***Cloud service provider***: A **party** which makes **cloud services** available. The **cloud service provider** focuses on activities necessary to provide a **cloud service** and activities necessary to ensure its delivery to the **cloud service customer** as well as **cloud service** maintenance. The **cloud service provider** includes an extensive set of activities (e.g., provide service, deploy and monitor service, manage business plan, provide audit data, etc.) as well as numerous sub-roles (e.g., business manager, service manager, network provider, security and risk manager, etc.).

6.4 Cloud capabilities types and cloud service categories

A **cloud capabilities type** is a classification of the functionality provided by a **cloud service** to the **cloud service customer**, based on the resources used. There are three different **cloud capabilities types**: **application capabilities type**, **infrastructure capabilities type**, and **platform capabilities type**, which are different because they follow the principle of separation of concerns, i.e. they have minimal functionality overlap between each other.

The **cloud capabilities types** are:

– ***Application capabilities type***: A **cloud capabilities type** in which the **cloud service customer** can use the **cloud service provider's** applications;

– ***Infrastructure capabilities type***: A **cloud capabilities type** in which the **cloud service customer** can provision and use processing, storage or networking resources;

– ***Platform capabilities type***: A **cloud capabilities type** in which the **cloud service customer** 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**.

There are only three **cloud capabilities types** defined in this Recommendation | International Standard. These **cloud capabilities types** should not be confused with other categorizations of **cloud services**.

A **cloud service category** is a group of **cloud services** that possess some common set of qualities. A **cloud service category** can include capabilities from one or more **cloud capabilities types**.

Representative **cloud service categories** are:

– ***Communications as a Service (CaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is real time interaction and collaboration;

– ***Compute as a Service (CompaaS)***: A **cloud service category** in which the capabilities provided to the **cloud service customer** are the provision and use of processing resources needed to deploy and run software;

– ***Data Storage as a Service (DSaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is the provision and use of data storage and related capabilities;

– ***Infrastructure as a Service (IaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is an **infrastructure capabilities type**;

– ***Network as a Service (NaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is transport connectivity and related network capabilities;

– ***Platform as a Service (PaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is a **platform capabilities type**;

– ***Software as a Service (SaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is an **application capabilities type**.

It is expected that there will be additional **cloud service categories** (see Annex A). This Recommendation | International Standard does not imply that any **cloud service category** is more important than any other.

6.5 Cloud deployment models

Cloud deployment models represent how **cloud computing** can be organized based on the control and sharing of physical or virtual resources.

The **cloud deployment models** include:

– ***Public cloud***: **Cloud deployment model** where **cloud services** are potentially available to any **cloud service customer** and resources are controlled by the **cloud service provider**. A **public cloud** may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the **cloud service provider**. Actual availability for specific **cloud service customers** may be subject to jurisdictional regulations. **Public clouds** have very

broad boundaries, where **cloud service customer** access to **public cloud** services has few, if any, restrictions;

– ***Private cloud***: **Cloud deployment model** where **cloud services** are used exclusively by a single **cloud service customer** and resources are controlled by that **cloud service customer**. A **private cloud** may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The **cloud service customer** may also authorize access to other **parties** for its benefit. **Private clouds** seek to set a narrowly controlled boundary around the **private cloud** based on limiting the customers to a single organization;

– ***Community cloud***: **Cloud deployment model** where **cloud services** exclusively support and are shared by a specific collection of **cloud service customers** who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A **community cloud** may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. **Community clouds** limit participation to a group of **cloud service customers** who have a shared set of concerns, in contrast to the openness of **public clouds**, while **community clouds** have broader participation than **private clouds**. These shared concerns include, but are not limited to, mission, **information security** requirements, policy, and compliance considerations;

– ***Hybrid cloud***: **Cloud deployment model** using at least two different **cloud deployment models**. The deployments involved remain unique entities but are bound together by appropriate technology that enables **interoperability**, **data portability** and application portability. A **hybrid cloud** may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. **Hybrid clouds** represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies. As such the boundaries set by a **hybrid cloud** reflect its two base deployments.

6.6 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. Such aspects may impact multiple roles, activities, and components, in such a way that it is not possible to clearly assign them to individual roles or components, and thus become shared issues across the roles, activities and components.

Key cross cutting aspects include:

– ***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;

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

– ***Governance***: The system by which the provision and use of **cloud services** are directed and controlled. Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with **SLAs** and other contractual elements of the **cloud service customer** to **cloud service provider** relationship. The term internal cloud governance is used for the application of design-time and run-time policies to ensure that **cloud computing** based solutions are designed and implemented, and **cloud computing** based services are delivered, according to specified expectations. The term external cloud governance is used for some form of agreement between the **cloud service customer** and the **cloud service provider** concerning the use of **cloud services** by the **cloud service customer**;

– ***Interoperability***: Ability of a **cloud service customer** to interact with a **cloud service** and exchange information according to a prescribed method and obtain predictable results;

– ***Maintenance and versioning***: Maintenance refers to changes to a **cloud service** or the resources it uses in order to fix faults or in order to upgrade or extend capabilities for business reasons. Versioning implies the appropriate labelling of a service so that it is clear to the **cloud service customer** that a particular version is in use;

– ***Performance***: A set of behaviours relating to the operation of a **cloud service**, and having metrics defined in a **SLA**;

– ***Portability***: Ability of **cloud service customers** to move their data or their applications between multiple **cloud service providers** at low cost and with minimal disruption. The amount of cost and disruption that is acceptable may vary based upon the type of **cloud service** that is being used;

– ***Protection of PII***: Protect the assured, proper, and consistent collection, processing, communication, use and disposal of Personally Identifiable Information (PII) in relation to **cloud services**;

- ***Regulatory***: There are a number of different regulations that may influence the use and delivery of **cloud services**. Statutory, regulatory, and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both **cloud service customers** and **cloud service providers**. Compliance with such requirements is often related to governance and risk management activities;
- ***Resiliency***: Ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation;
- ***Reversibility***: A process for the **cloud service customer** to retrieve their **cloud service customer data** and application artefacts and for the **cloud service provider** to delete all **cloud service customer data** as well as contractually specified **cloud service derived data** after an agreed period;
- ***Security***: Ranges from physical security to application security, and includes requirements such as authentication, authorization, **availability**, **confidentiality**, identity management, **integrity**, non-repudiation, audit, security monitoring, incident response, and security policy management;
- ***Service levels and service level agreement***: The **cloud computing service level agreement** (cloud **SLA**) is a **service level agreement** between a **cloud service provider** and a **cloud service customer** based on a taxonomy of **cloud computing** specific terms to set the quality of the **cloud services** delivered. It characterizes quality of the cloud services delivered in terms of: 1) a set of measurable properties specific to **cloud computing** (business and technical) and 2) a given set of **cloud computing roles** (**cloud service customer** and **cloud service provider** and related **sub-roles**).

Many of these cross cutting aspects, when combined with the key characteristics of **cloud computing**, represent good reasons for using **cloud computing**. However, cross cutting aspects like security, protection of PII, and governance have been identified as major concerns and in some cases an impediment to the adoption of **cloud computing**.