NIST Special Publication 500-322

Evaluation of Cloud Computing Services Based on NIST SP 800-145

Eric Simmon

NIST Cloud Computing Cloud Services Working Group
NIST Cloud Computing Program
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500.322

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 500-322

Evaluation of Cloud Computing Services Based on NIST SP 800-145

Eric Simmon

NIST Cloud Computing Cloud Services Working Group
NIST Cloud Computing Program
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.500-322

February 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Special Publication 500-322
Natl. Inst. Stand. Technol. Spec. Publ. 500-322, 27 pages (February 2018)
CODEN: NSPUE2

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.500-322

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. This document reports on ITL's research, guidance, and outreach efforts in IT and its collaborative activities with industry, government, and academic organizations.

Abstract

This document provides clarification for qualifying a given computing capability as a cloud service by determining if it aligns with the NIST definition of cloud computing; and for categorizing a cloud service according to the most appropriate service model Software as a Service (SaaS), Platform as a Service, (PaaS), and Infrastructure as a Service (IaaS).

Keywords

Cloud Computing, Cloud Computing Definition, Cloud Services, Cloud Service Categorization, Cloud Service Evaluation, Cloud Service Models, Software as a Service, SaaS, Platform as a Service, PaaS, Infrastructure as a Service, IaaS

Acknowledgements

NIST thanks the many experts in industry and government who contributed their thoughts to the creation and review of this definition. NIST would like to acknowledgement the members of the NIST Cloud Computing Services Public Working Group listed below who worked many hours providing input for this document. A special appreciation to Cary Landis who was the industry chair of the group. We would also like to acknowledge Robert B. Bohn, NIST Cloud Computing Program Manager, for his editorial comments.

Cary Landis - *Industry Chair*		
Ali Khalvati *GSA*	**Lalit Bajaj** *GSA*	**Don Beaver** *GSA*
James Yaple	**Angela Rowe**	**James Mooney**
James Fowler	**Eugene Luster**	**Larry Lamers**
Keith Parker *ASI for GSA*	**Gary Rouse** *VMSI for GSA*	**Travis Ferguson**
Chris Ferris	**Kavya Pearlman**	

Table of Contents

List of Figures

1 Introduction

The National Institute of Standards and Technology (NIST), consistent with its mission[1], has a technology leadership role in support of the United States government efforts for the secure and effective adoption of the Cloud Computing model to reduce costs and improve services. NIST was charged with the mission of developing a cloud computing technology roadmap and to lead efforts in developing and prioritizing cloud computing standards. The NIST Cloud Computing Program (NCCP) created a series of public working groups on cloud computing to generate input for the SP 500-293 *NIST Cloud Computing Technology Roadmap, Volume I and II* [1]. SP 500-293, hereafter referred to as "the Roadmap," contains ten high-level priority requirements in security, interoperability, and portability for the government's adoption of cloud computing.

Requirement 4 of the Roadmap is for "Clearly and consistently categorized cloud services." This requirement is important to ensure that customers understand the characteristics of different types of cloud services and are able to objectively evaluate, compare, and select cloud services suitable to meet their business objectives.

In the absence of clarification, organizations are at risk of adopting "services" that do not provide characteristics of cloud computing. For example, some vendors reportedly decide to label their computing offerings as "cloud services," even if the offerings do not support the essential characteristics of a cloud service in the NIST definition.

Furthermore, the frequent and common usage of the informal "aaS" (as a Service) suffix in marketing, as in "EaaS" (Enterprise as a Service), "DaaS"(Desktop as a Service or Data as a Service), "STaaS" (Storage as a Service, and even "XaaS" (Everything as a Service) is confusing, and (unintentionally) obfuscating the architecturally well-founded distinction of Software as a Service (SaaS), Platform as a Service, (PaaS), and Infrastructure as a Service (IaaS). These "cloud service types" are generally coined by appending the suffix "aaS" after a type of computing capability or marketing term. This makes it difficult to determine whether something is a cloud service and has unintended consequence for organizations trying to satisfy their cloud-first objectives.

To demystify the ambiguity surrounding cloud services, the NIST Cloud Computing Services Public Working Group analyzed the NIST cloud computing definition and developed guidance on how to use it to evaluate cloud services.

This document clarifies the cloud computing service models as published in NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*. [2] The NIST Definition was intended for the stated purpose of "broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing."

The clarification supports the proper planning for cloud migration, deployment, and retirement of relevant legacy systems. The Government Accountability Office (GAO) recommended in [3] July 2012 that seven audited federal agencies should establish estimated costs, performance goals, and plans to retire associated legacy systems for each type of cloud-based service as well as the same for retiring legacy systems, as applicable, for planned additional cloud-based services.

[1] This effort is consistent with the NIST role per the National Technology Transfer and Advancement Act (NTTAA) of 1995, which became law in March 1996

As this document is meant to provide guidance in understanding the categorization, evaluation, comparison, and selection of cloud services, it does not provide a prescriptive set of guidelines for the selection process. Instead, it uses the principles set forth in the NIST cloud computing definition as a framework for understanding a customer's requirements in a cloud computing context and the capabilities offered by cloud service providers (CSP)s to enable easier decision making. The NIST cloud computing definition allows for flexibility in its interpretation and in many cases, the final decision relies on a mixture of objective and subjective perspectives.

This document is intended for use by any stakeholder, including, but not limited to, buyers of IT and cloud services, IT managers, program managers, Federal Risk and Authorization Management Program (FedRAMP) stakeholders, systems integrators, resellers of cloud services, etc.

2 The NIST Definition of Cloud Computing

NIST SP 800-145 was published in the fall of 2010. Since that time, the cloud computing environment has experienced a growth in technical maturity, yet the NIST Definition has retained worldwide acceptance. This document provides an analysis of the NIST Definition of Cloud Computing based on today's perspective and provides a methodology for evaluating services, complementing the NIST definition.

NIST SP 800-145 provides a one sentence definition of cloud computing as *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* In addition, the NIST definition introduces the supporting concepts of three cloud service models, five essential characteristics, and four types of cloud deployments.

In total, the NIST Cloud Computing Definition is composed of 14 interrelated terms and their associated definitions:

Core definition of the cloud computing model (above)
Five essential characteristics
- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Three service models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Four deployment models
- Public
- Private
- Community
- Hybrid

NIST SP 800-145 also includes multiple clarifying statements that are integrated into the text of the various definitions. TheNIST Definition makes use of additional terms that are clarified below:

Application: Within the context of cloud computing, the term application may refer to either a cloud-enabled SaaS, web or mobile application or an application that exists on a virtual machine (e.g., Linux application). It is therefore preferable to clarify that type of application when using the term to avoid confusion.

as a Service (aaS): The term "as a [cloud] Service" is a suffix describing a computing capability that supports all five essential characteristics of cloud computing. The term "as a service (aaS)" implies that SaaS, PaaS, and IaaS are delivered by way of software.

Cloud Infrastructure: The collection of hardware and software that enables the five essential characteristics of cloud computing. The consumer of a cloud service does not manage or control the underlying cloud infrastructure. Cloud Infrastructure is represented in SP 500-292 *NIST Cloud Computing Reference Architecture* (CCRA) within the 'Resource Abstraction and Control' layer and Hardware layer.

Cloud Service: One or more capabilities offered via the cloud computing model.

Essential Characteristics: The five characteristics that must be available in a computing capability to be qualified as a "cloud service." They are listed here for clarity, but are discussed in greater detail in Section 3.

- on-demand self-service (see section 3.1)
- broad network access (see section 3.2)
- resource pooling (see section 3.3)
- rapid elasticity (see section 3.4)
- measured service (see section 3.5)

Multi-tenant: An architecture in which a single computing resource is shared but logically isolated to serve multiple consumers.

Service Model: The highest-level categorization of cloud services as based on the type of computing capability that is provided. Any given cloud service may be categorized as one of three service models, namely Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

This document uses an additional term "cloud service type" to describe informal terms often coined and used by industry by adding the suffix "aaS" after a computing capability, e.g., Email as a Service (EaaS). Example cloud service types are shown in Section 7 of this document.

3 Analysis of the Essential Characteristics of Cloud Computing

This section provides a detailed analysis of the five Essential Characteristics of Cloud Computing described in section 2. The approach was to decompose each characteristic to determine the primary criteria for determining if a computing capability is offered as a cloud service and the different options for determining whether the criteria is met.

To understand the essential characteristics, it is important to understand the meaning of the term "essential." In the context of SP 800-145 and this document, "essential" means each cloud service provider (CSP) must have the ability to provide each essential characteristic to the cloud service customer (CSC) for a given service. The CSC may or may not elect to implement or use each essential characteristic in a specific instance. In addition, the CSC must make a subjective judgement to determine

if their requirements are fulfilled and to decide if the CSP's offering can be considered a cloud service for their purposes.

The process of categorizing a computing capability is not always definitive. A CSC may want to interpret an essential characteristic in a specific way to support their requirements. Therefore, this document allows flexibility in determining that a computing capability qualifies as a cloud service by providing options for evaluating each essential characteristic.

The options are described as "Option A" or "Option B," where "Option A" is more objective, while "Option B" is more subjective and dependent on the specific requirements of the CSC. Option A is based on requirements that are common to all CSCs. Option B focuses on a user's perceived performance and provides for requirements that are specific to a single CSC or group of CSCs. If a CSC chooses to use Option B instead of Option A, they must evaluate whether "Option B" meets their requirements, and the results are not comparable between CSCs with different requirements. In cases where there is only one option, that option is labeled as "Option A."

Whether an entity can confirm a specific criterion is dependent on the criterion itself. Some criteria are externally visible (such as availability) and can be confirmed by the CSC or other third party entity, while other criteria (such as resource pooling) are internal to the cloud service and must be confirmed by the CSP.

3.1 On-demand self-service

"A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider." – NIST SP 800-145

Primary Criteria	The computing capability can be provisioned without human interaction with the service provider. **Option A)** Fully automated service provisioning (both the CSC interface and the internal cloud infrastructure). **Option B)** The CSC uses an automated interface to request and track the service, but the provider may use manual labor to provision the service internally.
Entity capable of confirming?	The CSC distinguish Option A from Option B because they can only see the provisioning interface, not the system behind the interface. Therefore, the CSP will confirm whether it is Option A or Option B.
Additional Clarification	• The term consumer and CSC are used synonymously. • Examples of "computing capabilities" include server time and network storage. • The term "Unilaterally" refers to the fact that the CSC initiates the service without human interaction with a human on the CSP side. The CSC organization may have a workflow process involving humans such as those for oversight and approval of expenditures, and the purchase can still be described as unilateral. • The term automatically refers to automated provisioning.

	• The question arose as to whether a ticketing system supports the requirement for automated provisioning. The Cloud Services Working Group members suggest "yes," as long as the provisioning is fast enough to support CSC requirements as described in the Service-Level Agreement (SLA).
Benefits	• "As needed" access to computing capabilities.

3.2 Broad network access

"Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)." – NIST SP 800-145

Primary Criteria	The computing capability is available from a wide range of locations using standard protocols. **Option A)** Available over the Internet. **Option B)** Available over a network that is available from all access points the CSC requires.
Entity capable of confirming	The CSC or CSP can confirm Option A. The CSC will confirm Option B (this is based on the CSC's requirements for the cloud service).
Additional Clarification	• Examples of thin or thick client platforms are mobile phones, tablets, laptops, and workstations. • The phrase "thin or thick" is not included as primary criteria because it includes all clients. • The term "standard mechanisms" implies that the computing capability is available using standard protocols such as HTTP/HTTPS, REST, TCP/IP, UDP, and/or other Internet protocols. • The term "broad network" can apply equally to public, private, or hybrid clouds.
Benefits	• Anytime anyplace access to computing resources from any machine within policy and security constraints.

3.3 Resource Pooling

"The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or

knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth." – NIST SP 800-145

Primary Criteria	The computing infrastructure is shared among more than one CSC. **Option A)** Two or more CSCs can share the cloud service resources using a multi-tenant model.
Entity capable of confirming	This is dependent on the internal architecture of the cloud service – therefore the CSP will confirm.
Additional Clarification	• There is a sense of location independence in that the CSC generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). • Examples of "resources" include storage, processing, memory, and network bandwidth. • The term consumer and CSC are used synonymously. • The essential characteristic is met if the capability to serve multiple tenants exists, regardless of how many tenants are actually served. • According to the NIST Special Publication 500-293 – U.S. Government Cloud Computing Technology Roadmap Volume II, the Resource Abstraction and Control Layer of the Cloud Computing Reference Architecture "ties together the numerous underlying physical resources and their software abstractions to enable resource pooling." • Resource pooling is an inherent benefit of any service model (SaaS, PaaS, or IaaS) that is hosted on cloud infrastructure.
Benefits	• Lowers costs by sharing resources.

3.4 Rapid elasticity

"Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time." – NIST SP 800-145

Primary Criteria	The computing capabilities can be "rapidly" provisioned and released to scale. **Option A)** Resource allocation modification is automated and near-real-time. **Option B)** Not fully automated, but fast enough to support the requirements of the CSC.
Entity capable of confirming	The CSC or CSP can confirm Option A. The CSC will confirm Option B.
Additional Clarification	• To the CSC, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. • Rapid elasticity generally relates to horizontal scaling.
Benefits	• Ability to quickly grow and shrink computing capability – and associated costs – dynamically according to need.

3.5 Measured service

"Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service." – NIST SP 800-145

Primary Criteria	Cloud service characteristics including resource usage are measured with enough detail to support the requirements of the CSC. **Option A)** Cloud service characteristics are measured with enough detail to support the requirements of the CSC.
Entity capable of confirming	The CSC will confirm.
Additional Clarification	• The term consumer and CSC are used synonymously. • Typically "metering" is done on a pay-per-use or charge-per-use basis, though metering may be used for "showback," as well as chargeback. For example, in a private cloud, metering may be used to show organizational leadership which parts of the organization are consuming what portion of cloud resources.

	• Examples include tracking units of services consumed and associated costs, and tracking resource usage to the application level. • Resource usage can be monitored, controlled, and reported, providing transparency for both the CSP and CSC of the utilized service.

4 Analysis of Cloud Service Models

In SP 800-145, cloud services are computing capabilities that are provided by the CSP and exhibit the five essential characteristics of cloud computing. The NIST Cloud Computing Definition provides three possible cloud services categories (called service models): Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With respect to the NIST Cloud Computing Reference Architecture (CCRA), cloud services are made available in the Service layer, which is part of the Service Orchestration stack shown in Figure 1. [4]

The Service Models are depicted in the CCRA as "L shaped" horizontal and vertical bars, rather than as a simple "three-layer cake" stack. The reason is that, although cloud services can be dependent upon each other in the stack, it also may be possible for the services to be implemented independently and interact directly with the resource abstraction and control layer depending on the architecture of each layer (as shown in Figure 1).

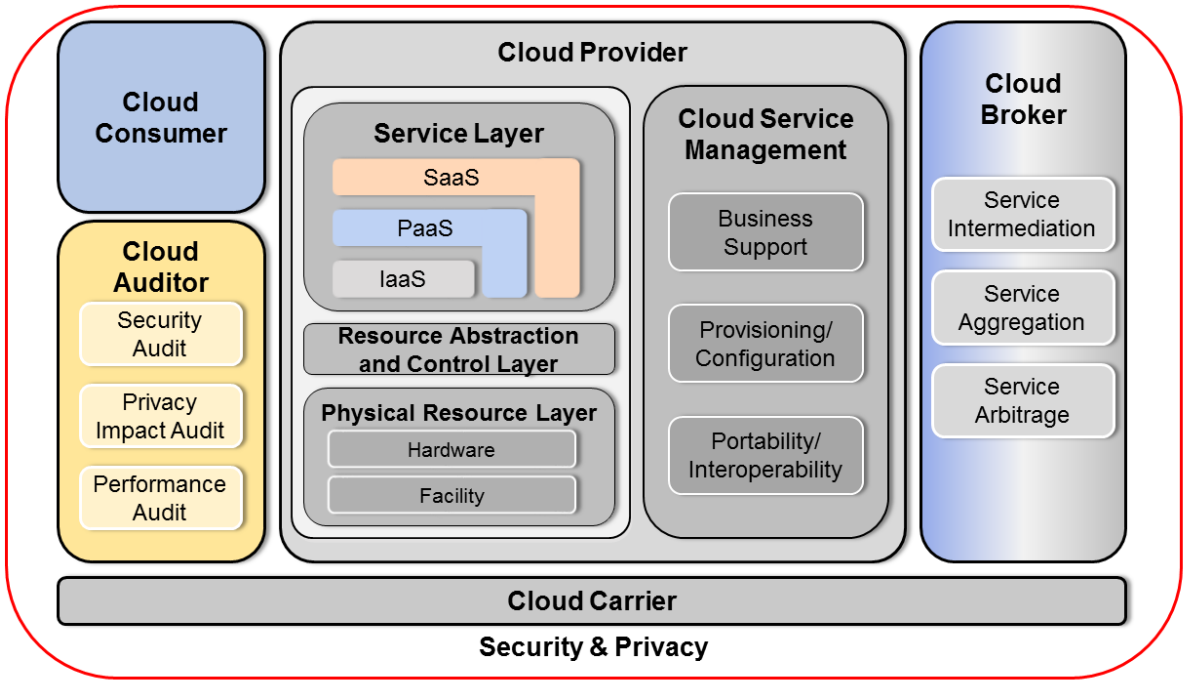

Figure 1 - Cloud Computing Reference Architecture

SaaS, PaaS, and IaaS are best distinguished by two factors: the computing capability that is provisioned (provided as a Service) and the primary CSCs (end user, developer/deployer, or IT operations). The term "platform" in the PaaS context refers to a development platform and/or deployment platform for cloud-enabled applications. The term "platform" is broadly used in the computing industry. It therefore helps to understand the context of the term with regards to Platform as a Service.

This section supports the categorization of a given cloud service as a software, platform, or infrastructure service. The guidance for categorizing cloud services supports Requirement #4 of the U.S. Government Cloud Computing Technology Roadmap Volume I [1], which calls for "*clear and consistently categorized cloud services.*"

4.1 Software as a Service (SaaS)

The capability provided to the CSC is to use the CSP's applications running on a cloud infrastructure.[2] The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The CSC does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Primary Criteria	The service that is provisioned is a software application, described as computer programs designed to permit the user to perform a group of coordinated functions, tasks, or activities. [5]
Entity capable of confirming	The CSC or CSP will confirm.
Additional Clarification	• The primary CSCs are end users of software applications [3]. • The term "applications" in the SaaS context refers to cloud-enabled applications (e.g., web or mobile) by nature of supporting essential characteristic #2 – broad network access. This differs from desktop applications that may be installed on a virtual machine. • SaaS applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or application programming interface (API). [2] • SaaS applications may be extensible by way of an API. • A web application is not necessarily considered SaaS, unless the application itself qualifies as a cloud service. • The SaaS provider is typically responsible for all aspects of making the software service available, including the availability of any PaaS and IaaS dependencies that may exist. The NIST Reference Architecture for Cloud Computing clarifies that the SaaS provider is responsible for deploying, configuring, maintaining, and updating the operation of the software

[2] See definition of Cloud Infrastructure on page 9.

	applications on a cloud infrastructure. The term "provider" refers to the entity responsible for making the service available and may therefore be different than the SaaS application developer. • Many modern SaaS applications are extensible. Extensibility alone does not denote that a software service is PaaS.
Common categories	• Custom (For example, custom applications built or deployed using PaaS) • Off the shelf (For example, cloud-based email applications)

4.2 Platform as a Service (PaaS)

The capability provided to the CSC is to deploy onto the cloud infrastructure CSC-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. [2] The CSC does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Primary Criteria	The service that is provisioned is a software development and/or deployment platform, described as the capability to [develop and/or] deploy applications [2] without the complexities of managing underlying infrastructure services. [6]
Entity capable of confirming	The CSC or CSP can confirm.
Additional Clarification	• The primary CSCs are application developers who design and implement application software, and application deployers who publish applications into the cloud. [4] • The term "platform" in the PaaS context refers to a development and/or deployment platform for cloud-enabled applications. • The term "applications" in the PaaS context refers to cloud-enabled applications (e.g., web or mobile) by nature of supporting essential characteristic #2 – broad network access. This differs from VM/desktop applications that may be installed on a virtual machine. • PaaS is distinguished from an extensible SaaS or web application by its primary CSCs: developers and deployers versus end users. • The applications can be CSC-created or acquired. • The applications can be created using programming languages, libraries, services, and tools supported by the provider. This does not necessarily preclude the use of compatible

	programming languages, libraries, services, and tools from other sources. • A PaaS provider may be responsible for making the platform service available, including any IaaS dependencies. These typical terms may be negotiated as a shared responsibility model.
Common Categories	• Application development platforms • Application deployment platforms • Integration platforms

4.3 Infrastructure as a Service (IaaS)

The capability provided to the CSC to provision processing, storage, networks, and other fundamental computing resources where the CSC can deploy and run arbitrary software, which can include operating systems and applications. The CSC does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Primary Criteria	The service that is provisioned is infrastructure.
Entity capable of confirming	The CSC or CSP can confirm.
Additional Clarification	• The primary CSCs are an IT Operations role creating, installing, monitoring, and managing services and applications deployed in an IaaS cloud. [4] • The infrastructure service is typically software-defined. • Infrastructure as a Service is distinctly different from cloud infrastructure (see definition) and also different from the underlying physical infrastructure. • The terms “software” and “application” in the IaaS context refers to VM/desktop software and applications, rather than referring to cloud-enabled SaaS or web applications. • The infrastructure service may optionally include a pre-installed operating system and other support VM/desktop software and applications, such as a webserver. • The term “arbitrary software” in this context means that the CSC can deploy and run many types of VM/desktop software.
Common Categories	• Computing resources • Network resources • Storage resources

5 Analysis of Cloud Deployment Models

Definition of the Cloud Deployment Models

In SP 800-145, cloud deployment models describe how the cloud is operated and who has access to the cloud service resources. The four deployment models are defined in SP 800-145 as follows:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple CSCs (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of CSCs from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It 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.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It 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 provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Details of the Cloud Deployment Models

The following detailed discussion of cloud deployment models is from the NIST Cloud Computing Standards Roadmap.

Private Cloud. A private cloud gives a single CSC's organization the exclusive access to and usage of the cloud service and related infrastructure and computational resources. It may be managed either by the CSC organization or by a third party, and may be hosted on the organization's premises (i.e., on-site private clouds) or outsourced to a hosting company (i.e., outsourced private clouds). Figure 2 and Figure 3 present an on-site private cloud and an outsourced private cloud, respectively.

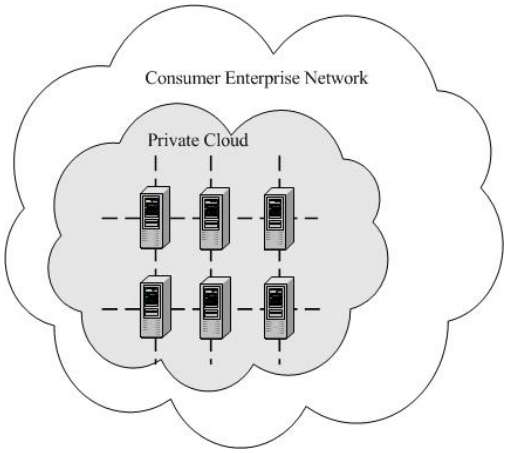

Figure 2: On-site Private Cloud

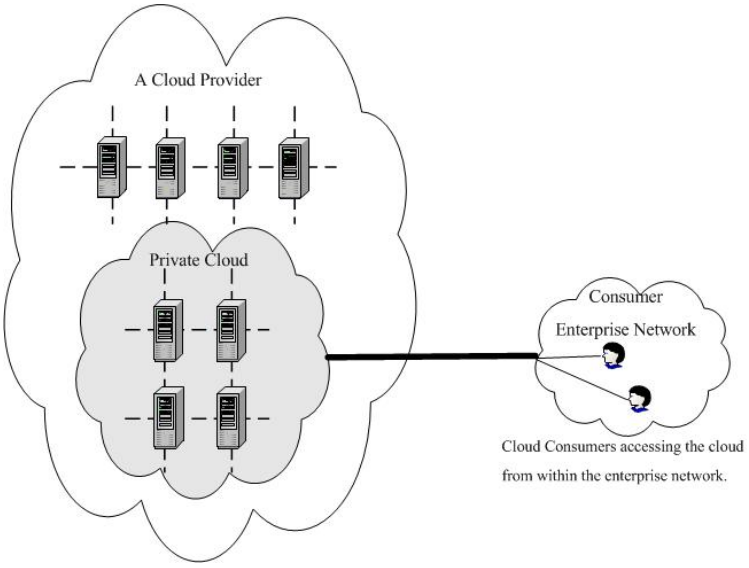

Figure 3: Outsourced Private Cloud

Community Cloud - A community cloud serves a group of CSCs that have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organization (e.g., a private cloud). Similar to private clouds, a community cloud may be managed by the organizations or by a third party and may be implemented on the CSC's premise (i.e., *on-site community cloud*) or outsourced to a hosting company (i.e., *outsourced community cloud*). Figure 4 depicts an on-site community cloud comprised of a number of participant organizations. A CSC can access the local cloud resources, and also the resources of other participating organizations through the connections between the associated organizations. Figure 5 shows an outsourced community cloud, where the server side is outsourced to a hosting company. In this case, an outsourced community cloud builds its infrastructure off premise, and serves a set of organizations that request and consume cloud services.

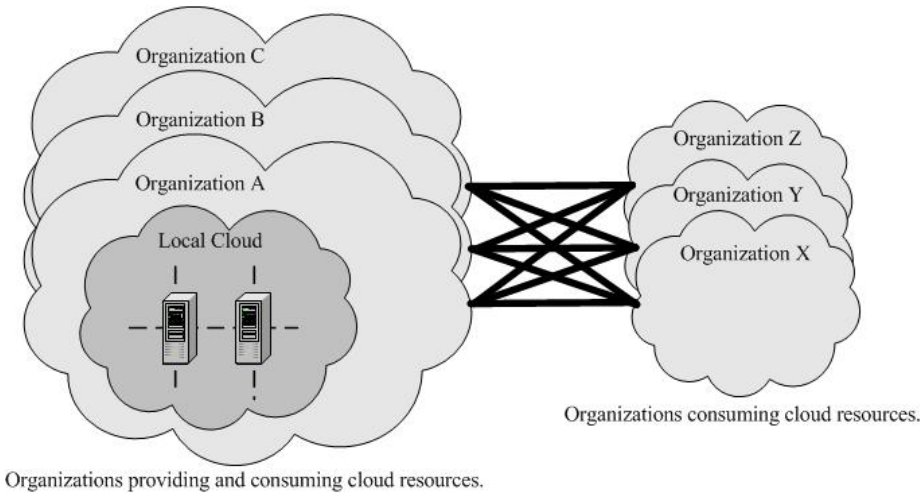

Figure 4: On-site Community Cloud

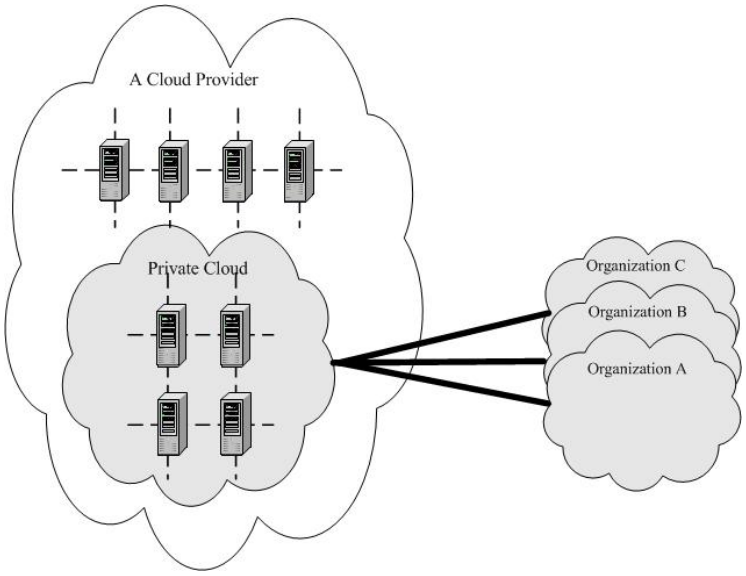

Figure 5: Outsourced Community Cloud

Public Cloud - A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization providing cloud services, and serves a diverse pool of clients. Figure 6 presents a simple view of a public cloud and its customers.

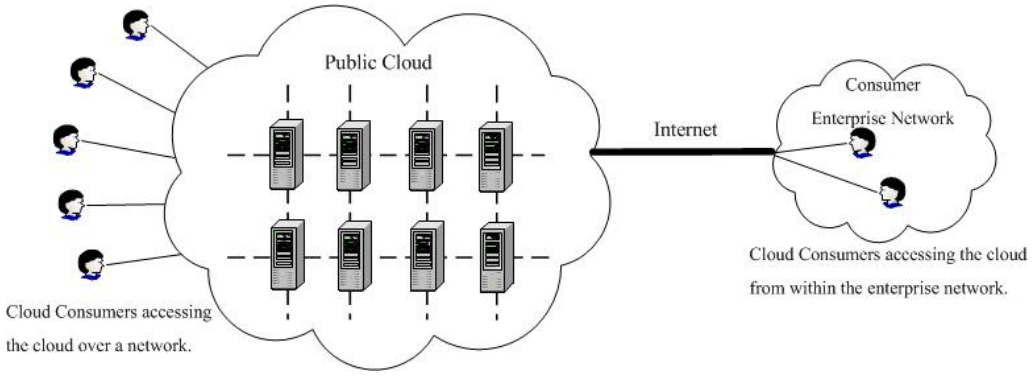

Figure 6: Public Cloud

Hybrid Cloud. A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability. Figure 7 presents a simple view of a hybrid cloud that could be built with a set of clouds in the five deployment model variants.

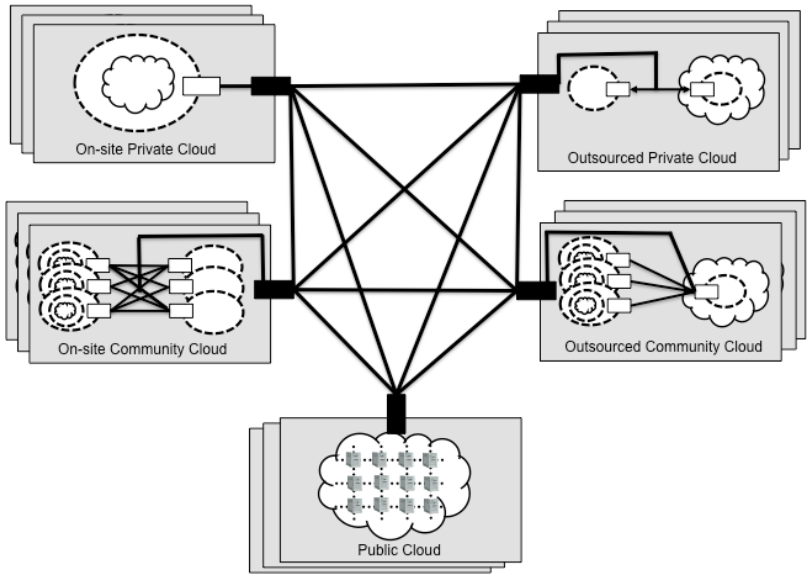

Figure 7: Hybrid Cloud

5.1 Private Cloud Computing Service Deployment

Primary Criteria	Only one organization can use the cloud service and the underlying resources.
Entity capable of confirming	The CSP must confirm.
Additional Clarification	**Organization in private cloud context –** In a private cloud context, the model, definition, and associated risks to an organization remain intact, as the cloud resources are provisioned for exclusive use by a single organization comprising multiple business units. In a private cloud model, the organization gets affected in the following ways: • Organization's cloud resources may be owned, managed, and operated by organization, a third party or a combination. • Private cloud may be on premises or off premises and provides much greater control over data, underlying systems, and applications. • Private cloud model provides an organization greater control over security, assurance over data location, and removal of multiple jurisdiction legal and compliance requirements.
Common categories	*on-site private cloud, outsourced private cloud*

5.2 Community Cloud Service Deployment

Primary Criteria	A specific community of CSCs from organizations that have shared concerns have exclusive use of the cloud service and the underlying resources.
Entity capable of confirming	The community of cloud CSCs forming the group of organizations verifies the scope of the group of organizations, while the CSP must confirm that the service and underlying infrastructure are exclusive to the group.
Additional Clarification	**Organization in community cloud context -** In a community cloud context, the model, definition, and associated risks to an organization are shared by other organizations, as the cloud resources are provisioned for exclusive use by a specific community of CSCs from organizations that have shared objectives and requirements. In a community cloud model, the organization gets affected in the following ways: • Organization's cloud resources may be operated by one or more of the organizations in the community or a third party. • Community clouds generally get the cost benefits of a public cloud while providing heightened privacy, security, and regulatory compliance. • Each organization may have individual organizational concerns that are not shared by the group (but they must be able to coexist within the environment).

	A cloud service auditor can conduct independent assessment of cloud services to confirm the scope of the group and confirm that the service and underlying infrastructure are exclusive to the group.
Common categories	*on-site community cloud, outsourced community cloud*

5.3 Public Cloud Service Deployment

Primary Criteria	Unrelated CSCs use the shared cloud service and the underlying resources.
Entity capable of confirming	The CSC will confirm.
Additional Clarification	While the CSP may limit access to a service, the CSC has no control over the set of users accessing the service.
Common categories	*Unrestricted commercial cloud*

5.4 Hybrid Cloud Service Deployment

Criteria	At least two or more distinct cloud infrastructures are connected together to facilitate hosted data and application portability. AND The cloud service infrastructure for each set of CSCs is virtually separated from the other sets of CSCs.
Entity capable of confirming	The CSP will confirm.
Additional Clarification	Deployment Choice. Hybrid Cloud provides for innovative business solutions by combining different cloud services.
Common categories	*Hybrid storage-processing cloud*

6 Worksheets

6.1 Cloud Service Worksheet

The following worksheet may be used with Section 3 to determine whether a service is a cloud service.

Is it a Cloud Service?
On-Demand Self-Service
Can the computing capability be provisioned without human interaction with the CSP? ____ YES ____ NO ____ Option A) Fully automated service provisioning ____ Option B) The CSC uses an automated interface to request and track the service, but the CSP may use manual labor to provision the service.
Broad Network Access
Is the computing capability available from a wide range of locations using standard protocols? ____ YES ____ NO ____ Option A) Available over the Internet using internet protocols ____ Option B) Available over a network that is available from all access points the CSC requires
Resource Pooling
Can two or more CSCs use a single cloud service where the resources are shared based on a multi-tenant model? ____ YES ____ NO
Can the resources be assigned and reassigned according to CSC demand? ____ YES ___ NO
Rapid Elasticity
Can the computing capabilities be “rapidly” provisioned and released to scale? ____ YES ____ NO ____ Option A) Resource allocation modification is automated and near-real-time (e.g. within five minutes). ____ Option B) Not fully automated, but fast enough to support the requirements of the CSC.
Measured Service
Cloud services characteristics including resource usage are measured with enough detail to support the requirements of the CSC. ____ YES ____ NO ____ Option A) Cloud services characteristics are measured with enough detail to support the requirements of the CSC.

6.2 Cloud Service Model Worksheet

The following worksheet may be used along with Section 4 to determine whether a service is a cloud service.

Is the cloud serice SaaS, PaaS or IaaS?
Software as a Service (SaaS)
Is the cloud service a Software Application? ____ YES ____ NO
Is the service Platform as a Service (PaaS)?
Is the cloud service a Software Development and/or Deployment Platform? ____ YES ____ NO
Is the service Infrastructure as a Service? (IaaS)?
Is the cloud service IT Infrastructure? ____ YES ____ NO

6.3 Cloud Deployment Model Worksheet

The following worksheet may be used along with Section 5 to determine whether a service is a cloud service.

Is the cloud service private, community, public, or hybrid?
Private Deployment
Is the cloud service infrastructure, including hardware resources, used only by a single CSC? ____ YES ____ NO
Community Deployment
Is the cloud service infrastructure including hardware resources used by a specific, known set of CSCs, but not available to any CSC? ____ YES ____ NO
Public Deployment
Is the cloud service infrastructure available for use by any CSCs? ____ YES ____ NO

7 Example Cloud Service Marketing Terms

Cloud service marketing terms are informal terms often coined and used by industry by adding the suffix "aaS" after a computing capability (e.g., Email as a Service). Cloud service marketing terms do not replace the three service models (SaaS, PaaS, and IaaS), which serve as the high-level categorization of cloud services, but rather serve to informally facilitate communication relating to specialized services. At this time NIST does not take a position on defining any given cloud service types. A cloud service type may optionally be informally used to subcategorize the cloud services models; however, the usage is inconsistent depending on the source of the term.

The following is a list of examples identified from various sources, including Internet searches, solicitations, and marketing collaterals. This is not a complete list of all cloud service marketing terms, and the list is not validated or filtered in any way.

Address Verification as a Service	Encryption as a Service	Mobility Backend as a Service
Anything as a Service	Enterprise Resource	Monitoring as a Service
API as a service (APIaaS)	Management as a Service	Network Access Control as a
Application Delivery as a Service	Ethernet as a Service	Service
Application Platform as a	Everything as a Service	Network as a Service
Service	Firewall as a Service	Operations as a Service
Architecture as a Service	Framework as a Service	Optimization as a Service
Authentication as a Service	Globalization as a Service	Payment as a Service
Backend as a Service	Hadoop as a Service	Quality as a Service
Backup as a Service	Hardware as a Service	Query as a Service
Big Data as a Service	High Performance Computing as	Recovery as a Service
Broker as a Service	a Service	Remote Backup as a Service
Business as a Service	Identity as a Service	Risk Assessment as a Service
Business Process as a Service	Infrastructure PaaS	Robot as a Service
Cloud Load Balancers as a	Insight as a Service	Security as a service
Service	Integrated Development	Service Desk as a Service
Cloud Search as a Service	Environment as a Service	Solutions as a Service
Collaboration-as-a-Service	Integration as a Service	Storage as a Service
Commerce as a Service	Integration Platform as a	Telepresence as a Service
Communication as a Service	Service	Test environment as a Service
Computing as a Service	Integration Platform as a	Testing as a Service
Contact Center as a Service	Service	Transport as a Service
Conversations as a Service	IT as a Service	Unified Communications as a
Data as a service	Java Platform as a Service	Service
Database as a service	Knowledge as a Service	User Interface as a Service
Desktop as a Service	Light as a Service	Video Conferencing as a Service
Development as a Service	Logon as a Service	Video Surveillance as a Service
DevTest as a Service	Management as a Service	Voice as a Service
Disaster Recovery as a Service	Mashups as a Service	Website as a Service
Drupal as a Service	Message Queuing as a Service	
Email as a Service	Metal as a Service	
	Mobility as a Service	

8 References

1. Badger, L., D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, M. Iorga, J. Mao, J. Messina, K. Mills, E. Simmon, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, *US Government Cloud Computing Technology Roadmap - Volumes I and II, NIST SP 500-293.* 2014, NIST. p. 40 (Vol I), 98 (Vol II) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf.

2. Mell, P. and T. Grance, *The NIST Definition of Cloud Computing*, *NIST SP 800-145*. 2011, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology: Gaithersburg, MD. p. 7 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

3. GAO, *INFORMATION TECHNOLOGY REFORM Progress Made but Future Cloud Computing Efforts Should be Better Planned*, *GAO-12-756*. 2012, U.S. Government Accountability Office. p. 43 http://www.gao.gov/assets/600/592249.pdf.

4. Liu, F., J. Tong, J., R. Bohn, J. Messina, L. Badger, and D. Leaf, *NIST Cloud Computing Reference Architecture*, *NIST SP 500-292*. 2011, NIST. p. 35 http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505.

5. *Definition of: application program*. PC Mag https://www.pcmag.com/encyclopedia/term/37919/application-program.

6. Labourey, S., *PaaS Primer: What is platform as a service and why does it matter?*, B. Butler, Editor. 2013 https://www.networkworld.com/article/2163430/cloud-computing/paas-primer--what-is-platform-as-a-service-and-why-does-it-matter-.html.