ISO/IEC JTC 1/SC 38

Distributed application platforms and services (DAPS)

Secretariat: ANSI

Document type: Request for comments

Title: Draft Study Group on Cloud Computing Report V.2

Status: **In accordance with Resolution** 6, Approval of Disposition of Comments on SC 38 N126, of the SC 38 Plenary Meeting in April 2011, the attached document is submitted for SC 38 review in conjunction with SC 38 N 281, Disposition of Comments Report on the Draft Study Group on Cloud Computing Report.

Please submit all comments to the SC 38 Secretary by 11 August 2011.

Following is the resolution:

- SGCC agreed to change the structure of SGCC Report based on editor's instructions contained in SC38 N0237, N0238, N0239 and N0240 and editors will produce draft SGCC Report V2 by 13 May 2011.
- The SC38 secretary will distribute the draft SGCC Report V2 and updated disposition of comments report to SC 38 National Bodies and Liaisons by 16 May 2011 for review and comment by 11 August 2011.
- SGCC agreed to move 7.1 through 7.21 of SC38 N0205, as modified by the 13 detailed changes proposed in N0213 to draft SGCC Report V2.

Date of document: 2011-05-16

Source: Project Editor (M. Carlson)

Expected action: COMM

Action due date: 2011-08-11

Email of secretary: mpeacock@ansi.org

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1sc38

(DRAFT) Study Group Report on Cloud Computing

16 May 2011

ISO/IEC JTC 1 SC 38 SGCC

Contents

Formatted: Font color: Red

Formatted: Left: 56.7 pt, Right: 56.7 pt, Top: 70.9 pt, Bottom: 70.9 pt, Width: 595.35 pt, Height: 842 pt

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Field Code Changed

Formatted: Font: Bold

Formatted: Font: Bold
Field Code Changed
Formatted: Font: Bold
Field Code Changed
Formatted: Font: Bold
Field Code Changed
Formatted: Font: Bold
Field Code Changed
Field Code Changed
Formatted: Font: Bold
Field Code Changed
Formatted: Font: Bold

Formatted: Indent: Left: 0 pt

1. Introduction and Purpose

With the significant advances in Information and Communications Technology (ICT) over the last half century, computing is evolving towards a model consisting of services that are commoditized and delivered in a standard manner. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Several computing paradigms have promised to deliver this computing vision, of which the latest one is known as Cloud Computing. The term “Cloud" denotes the services from which businesses and users are able to access applications from anywhere in the world on demand. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than to run on their individual computers. This concept is known as Cloud Computing, and it represents a paradigm shift that will be a refinement of the relationship between buyers and sellers of IT-related products and services.

This document intends to provide an overall review on the specified topics of Cloud Computing in terms of exploring standardization opportunities.~~,~~

Formatted: Font:

This document deals with:

- reviewing current concepts, characteristics, definitions, types and components used in Cloud Computing;
- a comparison of Cloud Computing to related technologies;
- analysing standardization activities for Cloud Computing in other standards organizations.~~; and,~~

2. Overview of Cloud Computing

Cloud Computing is 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. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

Formatted: Font: 12 pt, No underline, Font color: Auto

Formatted: Font: 12 pt

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’s provider.

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, laptops and PDAs).

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, network bandwidth and virtual machines.

Rapid elasticity.

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service.

Cloud systems automatically control and optimize resource use by leveraging a metering capability1 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.

Cloud Computing Service Models

Formatted: Font: 12 pt, No underline, Font color: Auto

Formatted: Font: 12 pt

Cloud Software as a Service (SaaS).

The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer 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.

Cloud Platform as a Service (PaaS).

The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer 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 application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS).

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

Cloud Computing Deployment Models

Formatted: Font: 12 pt, No underline, Font color: Auto

Formatted: Font: 12 pt

Private Cloud.

The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community Cloud.

The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud.

The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services.

Hybrid Cloud.

The Cloud infrastructure is a composition of two or more Clouds (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).

3. Cloud Computing Industry Initiatives

Cloud Computing touches many different areas – not all related to technology. Worldwide we see a number of national and international Cloud Computing initiatives: from industry consortia's as well as standardization organizations. Sometimes these initiatives are focusing on specific viewpoints of Cloud Computing, sometimes they may deal with Cloud architectures or use cases.

In this report we have been investigating several of these initiatives and table 1 shows a summary of current Cloud Computing industry initiatives by the time of this report.

Table -1. Summary of Cloud Computing Initiatives

Formatted: Centered

Industry Initiative	Type of initiative
Open Grid Forum (OGF)	Industry consortium
Distributed Management Task Force (DMTF)	Industry consortium
Cloud Security Alliance (CSA)	Industry consortium
ETSI Technical Committee (TC) CLOUD	European standard organization
OASIS	Industry consortium
Object Management Group (OMG)	No activities
Storage Networking Industry Association (SNIA)	Industry consortium
ITU-T Focus Group on Cloud Computing	International standard organization
Cloud Computing Use Case Discussion Group	Ad Hoc
W3C	No entry
CCF (Cloud Computing Forum in Korea)	Korean industry consortium
KCSA (Korea Cloud Service Association)	Korean industry consortium
The Open Group	Industry consortium
Study Group on Smart Cloud (Japan)	Japanese industrial consortium
European Network and Information Security Agency (ENISA)	EU agency
ISO/IEC JTC 1/SC 7	International standard organization
ISO/IEC JTC 1/SC 27	International standard organization
Institute of Electrical and Electronic Engineers (IEEE)	International standard organization
CESI (China Electronics Standardization Institute)	Chinese standard organization
Cloud Industry Forum (CIF)	Industry consortium

4. Cloud Computing Standards Analysis

(TBD)

Formatted: No underline, Font color: Red

Formatted: Font: Font color: Red

5. SGCC Recommendations

Based on the Study Group's investigation of the current state of Cloud Computing (covered in the section "Overview of Cloud Computing"), and an analysis of current industry initiatives (covered in the section "Cloud Computing Industry Initiatives"), the Study Group makes the following recommendations:

The study group concludes that a series of work item deliverables, staged over time based on their dependencies will produce the optimal set of work products from a future working group.

The study group proposes a roadmap for SC 38 Cloud Computing work as follows:

1. Create a Cloud Computing Terminology Standard - a standard definition of Cloud Computing terminology that is normative on other standards in the Cloud Computing space.
    a. Revise these definitions as new terms come into common usage in the field of Cloud Computing
2. Define a methodology for identifying subsequent new work items proposals. One proposal for that methodolo~~lodo~~gy is described in the Annex 6. "Cloud Computing Use Cases and Scenarios".
3. Cloud Computing Standard(s) - define and approve international standard(s) that meets the requirements listed in the above (2).

Annex 1: General Technical Principles of Cloud Computing NWI

The attached Form 04 is a revised version of the draft proposal for a new work item contained in SC 38 N0199. The scope has been revised and the "Purpose and justification" section has been simplified to reflect this scope as per SC 38 N0219. Rather than provide a draft outline, this proposal calls for the use of SC 38 N0164 (the NIST definitions) as a base document.

NEW WORK ITEM PROPOSAL

Date of presentation	Reference number (to be given by the Secretariat)
Proposer	ISO/IEC / SC N
Secretariat	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee with a copy to the Central Secretariat and, in the case of a subcommittee, a copy to the secretariat of the parent technical committee. Proposals not within the scope of an existing committee shall be submitted to the secretariat of the ISO Technical Management Board.

The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, or organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

See overleaf for guidance on when to use this form.

IMPORTANT NOTE: Proposals without adequate justification risk rejection or referral to originator.

Guidelines for proposing and justifying a new work item are given overleaf.

Proposal (to be completed by the proposer)

Title of proposal (in the case of an amendment, revision or a new part of an existing document, show the reference number and current title)

English title `General Technical Principles of Cloud Computing`

French title
(if available)

Scope of proposed project

Concerns known patented items (see ISO/IEC Directives Part 1 for important guidance)

□ Yes ☒ No If "Yes", provide full information as annex

Envisaged publication type (indicate one of the following, if possible)

☒ International Standard □ Technical Specification □ Publicly Available Specification □ Technical Report

Purpose and justification (attach a separate page as annex, if necessary)

Target date for availability (date by which publication is considered to be necessary)

Proposed development track ☒ 1 (24 months) □ 2 (36 months - default) □ 3 (48 months)

Relevant documents to be considered

Relationship of project to activities of other international bodies

Liaison organizations

Need for coordination with:

□ IEC □ CEN □ Other (please specify)

Preparatory work (at a minimum an outline should be included with the proposal)

□ A draft is attached □ An outline is attached. It is possible to supply a draft by

The proposer or the proposer's organization is prepared to undertake the preparatory work required ☒ Yes □ No

Proposed Project Leader (name and address)

Name and signature of the Proposer
(include contact information)

Comments of the TC or SC Secretariat

Supplementary information relating to the proposal

☒ This proposal relates to a new ISO document;

□ This proposal relates to the amendment/revision of an existing ISO document;

□ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item;

□ This proposal relates to the re-establishment of a cancelled project as an active project.

Other:

Voting information

The ballot associated with this proposal comprises a vote on:

☒ Adoption of the proposal as a new project

□ Adoption of the associated draft as a committee draft (CD)

□ Adoption of the associated draft for submission for the enquiry vote (DIS or equivalent)

Other:

Annex(es) are included with this proposal (give details)

□

Date of circulation	Closing date for voting	Signature of the TC or SC Secretary

Use this form to propose:

a) a new ISO document (including a new part to an existing document), or the amendment/revision of an existing ISO document;
b) the establishment as an active project of a preliminary work item, or the re-establishment of a cancelled project;
c) the change in the type of an existing document, e.g. conversion of a Technical Specification into an International Standard.
This form is not intended for use to propose an action following a systematic review - use ISO Form 21 for that purpose.
Proposals for correction (i.e. proposals for a Technical Corrigendum) should be submitted in writing directly to the secretariat concerned.

Guidelines on the completion of a proposal for a new work item

(see also the ISO/IEC Directives Part 1)

a) Title: Indicate the subject of the proposed new work item.

b) Scope: Give a clear indication of the coverage of the proposed new work item. Indicate, for example, if this is a proposal for a new document, or a proposed change (amendment/revision). It is often helpful to indicate what is not covered (exclusions).

c) Envisaged publication type: Details of the types of ISO deliverable available are given in the ISO/IEC Directives, Part 1 and/or the associated ISO Supplement.

d) Purpose and justification: Give details based on a critical study of the following elements wherever practicable. *Wherever possible reference should be made to information contained in the related TC Business Plan.*

1) The specific aims and reason for the standardization activity, with particular emphasis on the aspects of standardization to be covered, the problems it is expected to solve or the difficulties it is intended to overcome.

2) The main interests that might benefit from or be affected by the activity, such as industry, consumers, trade, governments, distributors.

3) Feasibility of the activity: Are there factors that could hinder the successful establishment or global application of the standard?

4) Timeliness of the standard to be produced: Is the technology reasonably stabilized? If not, how much time is likely to be available before advances in technology may render the proposed standard outdated? Is the proposed standard required as a basis for the future development of the technology in question?

5) Urgency of the activity, considering the needs of other fields or organizations. Indicate target date and, when a series of standards is proposed, suggest priorities.

6) The benefits to be gained by the implementation of the proposed standard; alternatively, the loss or disadvantage(s) if no standard is established within a reasonable time. Data such as product volume or value of trade should be included and quantified.

7) If the standardization activity is, or is likely to be, the subject of regulations or to require the harmonization of existing regulations, this should be indicated.

If a series of new work items is proposed having a common purpose and justification, a common proposal may be drafted including all elements to be clarified and enumerating the titles and scopes of each individual item.

e) Relevant documents and their effects on global relevancy: List any known relevant documents (such as standards and regulations), regardless of their source. When the proposer considers that an existing well-established document may be acceptable as a standard (with or without amendment), indicate this with appropriate justification and attach a copy to the proposal.

f) Cooperation and liaison: List relevant organizations or bodies with which cooperation and liaison should exist.

General Technical Principles of Cloud Computing

Overview

Cloud Computing represents a significant evolution in the practices of buying, selling, developing, delivering, and using software and IT services. The Cloud Computing paradigm arose from the confluence of several, related technical and economic trends including grid computing, virtualization, service oriented architectures, enterprise computing, and the use of the World Wide Web as an application development and delivery platform.

This diversity of origins combined with the inherently multi-faceted nature of Cloud Computing has led to a plethora of overlapping and, in some cases, contradictory terms, definitions, descriptions, and acronyms. The lack of a common set of terms and definitions acts as an impediment to any efforts to standardize Cloud Computing, forcing each specification to provide its own definitions and obscuring attempts to compare or relate specifications.

What is required is a common definition of Cloud Computing along with a nomenclature that identifies the various kinds of Clouds, their constituent components, the actors involved, etc. This common framework should, to the extent possible, be based upon those terms and definitions that have already found widespread acceptance within the industry.

The purpose of this publication is create a standard which provides common terms and definitions for the field of Cloud Computing. These terms and definitions shall include the general concepts and characteristics of Cloud Computing, the types of Cloud Computing, the components of Cloud Computing, and Cloud Computing roles and actors.

Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO and IEC Standards

Standards Developing Organizations (SDO)

1. The NIST Definition of Cloud Computing, See http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Terms, Definitions, Notations, and Conventions

[Editor's Note] Terms, Definitions, Notations, and Conventions to explain the texts in the following section will be described.

Definition of Cloud Computing

Cloud Computing

Cloud Computing is 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. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics, Service Models, and Deployment Models of Cloud Computing

Essential Characteristics

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's provider.

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, laptops, and PDAs).

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, network bandwidth, and virtual machines.

Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

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.

Service Models

Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer 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.

Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer 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 application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS)

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

Deployment Models

Private Cloud

The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community Cloud

The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud

The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services.

Hybrid Cloud

The Cloud infrastructure is a composition of two or more Clouds (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).

Components of Cloud Computing

Cloud Computing roles and actors

Annex 2: Repository of Industry Standards for Cloud Computing

Standardization Areas and Issues - JTC 1 Perspective

Many Cloud Computing standardization efforts exist today. The section *Mapping Between SCs and Cloud Computing* shows such work in existing SC in JTC1. The section *Cloud Computing Initiatives* also shows work in other international standards bodies, international industry consortia, or even interests groups of individuals.

To foster collaboration among national bodies, JTC1 needs to identify new work items in Cloud Computing space because Cloud delivered services tend to easily cross country borders. In particular, it is required to consider the standards for adoption of Cloud Computing in various public sectors such as e-Government. It is also needed to consider the collaboration and liaisons with other relevant SDOs

In order to identify new work items for Cloud Computing in JTC 1, the following issues should be investigated as the first priority:

1. **General & Fundamentals:** There are lots of Cloud Computing technologies and solutions even if some of them do not tend to real Cloud Computing philosophy. These include: what are the general and common requirements for future Cloud Computing environment? How to deploy the Cloud service with relevant scenarios; and so on. (See N126 6.9 1. Primary Standards)

Editors Note: (N171/FI03) The candidate work items for standardization on the Cloud Computing should explicitly address collaboration between different Cloud systems. Without addressing inter-Cloud collaboration in the standardization efforts, it becomes a threat that future Cloud systems become yet another stove pipes. A Cloud ecosystem should be seen as a system of systems comprising one or more autonomic Cloud systems, instead of concentrating on individual Clouds and considering inter-Cloud collaboration as a special case that can be tackled with simple data integration. Such inter-Cloud perspective is now lacking in the list of candidate work items.

– Explicitly address inter-Cloud collaboration in the “General & Fundamentals” issues of candidate standardization work items.

– Describe Cloud ecosystems from the perspective of system-of-systems consisting one or more autonomously administered Cloud systems

– Add a usage scenario involving inter-Cloud usage.

2. **Data/Service Lock-in** : Software stacks have improved interoperability among platforms, but the APIs for Cloud Computing itself are still essentially proprietary, or at least have not been the subject of active standardization. (See N126 6.9 2. Interoperation-related Standards)
3. **Quality of Service (QoS)**: QoS will be an oft-employed term in Cloud Computing. Given that enterprises as well as private consumers demand a guaranteed quality of service, high levels of reliability and continued availability from their computing infrastructure, what level of service should users demand and expect from Cloud Computing vendors? How do we set service level agreements (SLAs) for Cloud Computing applications? Equally importantly, what are the parameters that determine the quality of one vendor with respect to another? It is worth bearing in mind that corporate users might reluctantly accept IT downtimes when it takes place within the organization, but the expectations can be radically higher when the computing service is outsourced to an external provider, so the service providers will have to play a role in educating their customers in developing rational expectations about downtimes. (See N126 6.9 5. Service level agreement standards)
4. **Security**: With a lot of responsibilities transferring to the Cloud Computing vendor, the organization will need to discuss several issues with the Cloud-computing vendor, including privileged user access (the personnel in the vendor organizations who will have specialized access to data, and the hiring and management of such administrators), regulatory compliance (enforced through external audits), end user control over data location, data segregation (to make sure that encryption is available at all stages and that these encryption schemes were designed and tested by experienced professionals), data recovery and disaster management (including “intelligent” Clouds that can automatically

relocate computing resources), investigative support for inappropriate or illegal activity, and long-term organizational viability. (See N126 6.9 3. Security and audit-related standards)

5. **Data Confidentiality and Auditability**: Current Cloud offerings are essentially public (rather than private) networks, exposing the system to more attacks. There are also requirements for auditability and confidentiality for data in Cloud. Although, there are no fundamental obstacles to making a Cloud-computing environment as secure as the vast majority of in-house, that many of the obstacles can be overcome immediately with well understood technologies such as encrypted storage, Virtual Local Area Networks, and network middleboxes (e.g. firewalls, packet filters). (See N126 6.9 3. Security and audit-related standards)

6. **Data ownership**: Data ownership is an interesting issue. Will the concept itself become outdated, just like data ownership "within a department" has become an outdated concepts in an enterprise after the introduction of centralized database management systems? However, data authentication will become very important: business processes and technologies will need to be developed to ensure end users that when they access data on the Cloud, its integrity has not been compromised. (See N126 6.9 3. Security and audit-related standards)

7. **Data privacy**: If confidential data is to be maintained on the Cloud, users need to be aware as to how it might be shared. Can a court subpoena a consumer's financial data that is maintained by a financial aggregator? Can the government do so under any circumstance? What will be the liabilities of the provider if data security is breached? If a consumer (or for that matter, a business) closes her account with the provider, till what time would her data be still maintained on the provider's servers, and at what point of time will the provider guarantee that the data has been completely purged from its servers? Privacy and security would be some of the main reasons why many enterprises might opt for what are being called "private Clouds", whereby users within the organization share resources of a computing infrastructure that is maintained and is under the control of the organization. (See N126 6.9 3. Security and audit-related standards)

Editors Note: (N149/DE034) Data privacy is certainly an important legal issue. For instance, in Germany, legal implications and uncertainties with regard to the protection of private data is one of the main obstacles in introducing Cloud Computing.

Make the link between the two issues more explicit

8. **Software Licensing**: Current software licenses commonly restrict the computers on which the software can run. Users pay for the software and then pay an annual maintenance fee. In the Cloud Computing, it is required new licensing mechanism for the Cloud service and applications.

Editors Note: (N188/GB022) Modify this lead in text for the following change to the table: Relabel ' Software Licensing' as 'Software Licensing and Software Asset Management'

Change bullet points to:

- Identification of software deployed to

provide Cloud services

- Specification of entitlements for

deploying/using Cloud services

- Metering of usage of Cloud resources

including in particular of licensing entitlements

- Discovery of relevant information about software deployments, entitlements, and usage regardless of the type of (virtualized) environment and bringing it together appropriately to enable effective management

- Life cycle management processes for information describing software deployed, entitlements held and allocated, and usage of entitlements.

9. **Legal issues**: If consumers and organizations are to depend on Cloud Computing providers for all their computing needs, a host of new legal issues will have to be tackled. Contracts will need to specify the required standards for vendor availability. Standards need to be developed so that consumers and organizations are not overly dependent on their current set of vendors. Providers will need to specify how they define concurrent use and therefore licensing. The old models of licensing based on CPUs or instances or named users simply do not work in the on-demand, elastic world of Cloud Computing and virtualization. Rigid software licensing models need to be changed just as the static network and application network infrastructure will get modified. The models need to evolve into something more fluid and flexible, and applicable to the new world of on-demand computing. One piece of good news for software providers will be that piracy will cease to be much of an issue, since it will be relatively simple to ensure that only paying customers can access the service.

10. **Inter-Cloud Interoperability**: The Inter-Cloud is an interconnected global "Cloud of Clouds" and an extension of the Internet "network of networks" on which is based. For the Inter-Cloud, ensuring interoperability among Clouds is essential to the proliferation and adoption of Cloud Computing among developers and enterprise, and new protocols and formats for Cloud Computing for inter-Cloud shall be considered. (See N126 6.9 2. Interoperation-related Standards)

Editors Note: (N171/FI04) Issues in inter-Cloud collaboration surpass those of technical connectivity and data-integration issues. Inter- Cloud interoperability can not be reduced to individual technical connectivity issues related only to data, infrastructure and platform application programming interfaces. Such technological interoperability issues are somewhat addressed in the list of candidate work items, but issues related to semantic or pragmatic interoperability in inter-Cloud collaborations are not addressed. These issues include conflicts between business rules and policies of autonomous Cloud providers during service migrations, or semantic misinterpretations between service functionality or associated information, for example.

– Inter-Cloud interoperability must not be rejected as a individual issue in the list of candidate work items

– Address inter-Cloud interoperability already at the level of reference models and reference architectures for Cloud Computing

– Work on the inter-Cloud interoperability standardization should cooperate with and partly coordinate efforts in standardization related to “Generals & Fundamentals” (especially reference models and architectures work), as well as standardization work related to more technological issues, such as in data, infrastructure and platform APIs.

11. **Device Independence**: The number of different kinds of device such as phones, smart phones, personal digital assistants, interactive television systems, voice response systems, kiosks that can be accessed in the Cloud Computing, and in a viewpoint of standardization, methods by which the characteristics of the device are made available for use in the processing associated with device independence and methods to assist authors in creating sites and applications that can support device independence in ways that allow it to be widely employed is required. (See N126 6.9 2. Interoperation-related Standards)

Editors Note: (N146/US026) There are 12 items in the table, but only 11 in the prose – is Virtualization missing from the prose?

Remove the last table entry on Virtualization.

The following are some candidates for work items on the Cloud Computing under the above contexts:

Table Annex 2-1 - Candidate work items for standardization on the Cloud Computing

Issues	Candidate work items to be standardized
① **General & Fundamentals**	• General requirements for Cloud Computing • Definition and Terminology for Cloud Computing • Reference model and Taxonomies for Cloud Computing • Reference architecture for Cloud Computing • Deployment model and Service scenarios for Cloud Computing
② **Data/Service Lock-in**	• Common Interface(API) for Cloud service • Metadata & Storage formats for Cloud service • Resource description & specification
③ **Quality of Service**	• Requirements for Service Level Architecture (SLA) • Framework for Cloud Computing SLA • SLA Quality Parameter for Cloud Computing • Monitoring interfaces and data formats for SLA validation
④ **Security**	• Framework for Trust & Secure Cloud Computing • Secure Cloud architecture and protocols • Identity & Access management • Application Security • Monitoring interfaces and data formats for security event and incident management
⑤ **Data Confidentiality and**	• Secure Data format for Cloud Computing

Auditability	• Audit and compliance for Cloud Computing
⑥ **Data ownership**	• Data authentication
⑦ **Data privacy**	• Cloud Data Protection & Encryption • Legal issues of data privacy
⑧ **Software Licensing and Software Asset Management**	• Identification of software deployed to • provide Cloud services • Specification of entitlements for deploying/using Cloud services • Metering of usage of Cloud resources including in particular of licensing entitlements • Discovery of relevant information about software deployments, entitlements, and usage regardless of the type of (virtualized) environment and bringing it together appropriately to enable effective management • Life cycle management processes for information describing software deployed, entitlements held and allocated, and usage of entitlements.
⑨ **Legal**	• Legal recommendation for distributed Cloud service
⑩ **Inter-Cloud Interoperability**	• Protocol and API for inter-Cloud service • Data format for inter-Cloud service • Universal Format for Cloud VM(Virtual Machine)
⑪ **Device Independence**	• Pass/SaaS API for various types of Cloud clients
⑫ **Virtualization**	• Resource virtualization for resources (storage, network, desktop, etc.)

Editors Note on rows 5-7: (N171/FI07) Data confidentiality, auditability, ownership and privacy are strongly inter-connected issues. However, safe Cloud Computing environment cannot be established by only addressing these topics concentrating on the usage of data alone. Processes, meta-information and participation in service collaborations are also kinds of knowledge that are vulnerable for exploitation. Knowledge mining based on composition of knowledge from several sources is also a security threat in Cloud ecosystems. Trustworthiness of a service provider as a privacy protecting entity should also be addressed, as well as detection of privacy breaches.

– Join “Security”, “Data confidentiality and Auditability”, “Data ownership” and “Data privacy” issues to a single coherent package.

– In addition to simple data-related safety issues, address also other kinds of knowledge, such as involved with the processes and several kinds of meta-information required for establishing service collaborations in Cloud ecosystems.

– Address knowledge-related security and privacy issues that are more specific for Cloud ecosystems.

Editors Note on row 10, 3: (N171/FI05,FI06) Inter-Cloud interoperability cannot be guaranteed with a selection of individual, technology-centric solutions. Instead, inter-Cloud interoperability should be addressed already at the fundamental level of Cloud Computing.

– Consider inter-Cloud interoperability as a multi-faceted issue surpassing those of technological connectivity

Management of inter-Cloud interoperability should be addressed at a technology-independent manner and fulfil the requirements stemming from inter-Cloud collaborations.

Cloud standardization should address non-functional features more widely. In the current version the non- functional features that are addressed include mostly technical service quality factors. In addition to these also management of non-functional features that are more related to the business domain of the Cloud Computing environment should be addressed. Such domain-specific, business-driven non-functional features can introduce for example use of notaries and associated business protocols between a service provider and consumer.

– Candidate work items on the issue of "Quality of Service" in Cloud Computing standardization should address non-functional features also at the business level of Cloud Computing. Currently, the work items seem to address only quite technical SLA-related issues.

– Guidelines for managing and introducing non-functional features in Cloud Computing environments should be provided in a platform-independent manner.

Editors Note on row 11: (N171/FI09) Platform independency should not be addressed at technological level alone in form of application- programming interfaces. Instead, connectivity and interoperation with the IaaS and PaaS level abstract platforms should be established in the standardization in a technology independent manner. For this purpose, IaaS and PaaS should be formalized as abstract platforms, possibly comprising different conformance levels (see our comment on 9.1, Issue "General & Fundamentals"). Connectivity with these abstract platforms should be defined as platform-dependent bindings, service conversations, and communication protocols to reach the same platform abstraction between different end-user devices.

– Instead of technology-driven API approach, use a more generic abstract platform approach for delivering device-independence.

Mapping b~~B~~etween SCs and Cloud Computing

SC No.	Subcommittee Title	Relationship to Cloud Computing
SC 02	Coded character sets	(TBD)
SC 06	Telecommunications and information exchange between systems	▪ Inter-Cloud communication & protocol issues ▪ Cloud Service architecture issues
SC 07	Software and systems engineering	▪ Software architecture for Cloud Computing (Platform, Middleware) issue ▪ Development environments (platform, language, etc.) issue for Cloud service ▪ Software asset management (SAM)

		· Software identification tagging · Software entitlement tagging · Management of tagging · SAM processes
SC 17	Cards and personal identification	(TBD)
SC 22	Programming languages, their environments and system software interfaces	▪ Development environments (platform, language, etc.) issue for Cloud service
SC 23	Digitally Recorded Media for Information Interchange and Storage	(TBD)
SC 24	Computer graphics, image processing and environmental data representation	(TBD)
SC 25	Interconnection of information technology equipment	▪ Common information and data storage device issue
SC 27	IT Security techniques	▪ Cloud security issue (Privacy, Security, Authentication, etc.) ▪ Relevant documents include: ■ ISO CD29100 (Privacy Framework) ■ ISO CD29101 (Privacy Reference Architecture) ■ ISO 24760 (Framework for Identity Management) ■ ISO 2nd WD 29146 (framework for Access Management) ■ ISO CD 29115 (Entity Authentication Assurance Framework)
SC 28	Office equipment	(TBD)
SC 29	Coding of audio, picture, multimedia and hypermedia information	▪ Media-level Cloud service issue (e.g., Media Cloud)
SC 31	Automatic identification and data capture techniques	(TBD)
SC 32	Data management and interchange	▪ Common Cloud data format and Cloud service interchange issue
SC 34	Document description and processing languages	(TBD)
SC 35	User interfaces	(TBD)
SC 36	Information technology for learning, education and training	(TBD)
SC 37	Biometrics	Verification of users' identity – user verification by biometric identifiers – personal recognition issues (e.g., architectures, protocols, remote user

		identification/verification).

ISO/IEC Management standards:

There are a number of management-oriented standards which should be relevant for any organization providing or using Cloud Computing services, but which are not focused solely on Cloud Computing. Some of these are formal Management System Standards such as ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1.

Others include ISO/IEC 19770-1 on Software Asset Management Processes, and ISO 31000 on RiskManagement.

Editors Note: (N188/GB004) Add coverage to the report of related standards which have more management orientation, such as ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO/IEC 19770-1, etc.

Note: If the report is restructured to give greater prominence to management requirements, then this type of standard would be discussed before technical standards, rather than after them.

Cloud Computing Initiatives

Open Grid Forum (OGF)

- Type: *Industry Consortium*
- Scope: The Open Cloud Computing Interface comprises a set of open community-lead specifications delivered through the Open Grid Forum. OCCI is a Protocol and API for all kinds of Management tasks. OCCI was originally initiated to create a remote management API for IaaS model based Services, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling and monitoring. It has since evolved into a flexible API with a strong focus on **integration**, **portability**, **interoperability** and **innovation** while still offering a high degree of extensibility.

Spec.	Type	Timeline	Scope	Issue related	Comments
OCCI Core	Consortium	December 2010	OCCI Core describes the formal definition of the OCCI Core Model	1. Data/Service Lock-in 2. Inter-Cloud Interoperability 3. Patterns for interoperation and interconnection of Clouds	
OCCI Infrastructure	Consortium	December 2010	OCCI Infrastructure contains the definition of the OCCI Infrastructure extension for the IaaS domain. The document defines additional resource types, their attributes and the actions that can be taken on each resource type.	4. Data/Service Lock-in 5. Inter-Cloud Interoperability 6. Patterns for interoperation and interconnection of Clouds	
OCCI HTTP Rendering	Consortium	January 2011	OCCI HTTP Rendering defines how to interact with the OCCI Core Model using the RESTful OCCI API. The document defines how the OCCI Core Model can be communicated and thus serialized using the HTTP protocol.	7. Data/Service Lock-in 8. Inter-Cloud Interoperability 9. Patterns for interoperation and interconnection of Clouds	

The Cloud Computing Interoperability Forum (CCIF)

1. Type: *industrial consortium*
2. Scope: CCIF is an open, vendor neutral, open community of technology advocates, and consumers dedicated to driving the rapid adoption of global Cloud Computing services. CCIF shall accomplish this by working through the use open forums (physical and virtual) focused on building community consensus, exploring emerging trends, and advocating best practices / reference architectures for the purposes of standardized Cloud Computing.

Spec.	Type	Timeline	Scope	Issue related	Comments
Unified Cloud Interface (UCI)	*Project*	*Not Clear*	Unified Cloud Computing is an attempt to create an open and standardized Cloud interface	Issue listed in Appendix 6 of N126 and future update:	*Not clear of market acceptance*

			for the unification of various Cloud API's. A singular programmatic point of contact that can encompass the entire infrastructure stack as well as emerging Cloud centric technologies all through a unified interface.	3. General & Fundamentals 4. Data/Service Lock-in 5. Quality of Service 6. Security 7. Data Confidentiality and 8. Auditability 9. Data ownership 10. Data privacy 11. Software Licensing 12. Legal 13. Inter-Cloud Interoperability 14. Device Independence 15. Virtualization 16. Pricing/chargeback 17. Cloud management 18. Patterns for interoperation and interconnection of Clouds 19. Platform APIs 20. Infrastructure APIs 21. Data APIs 22. Environment 23. Management 24. Identity…	
UCI_Requirements	Use Cases	Not Mature	Specifies the implementation of semantic process that can broker access and represent multiple Cloud providers that are Cloud-platform or Cloud-infrastructure designs. The concept is to provide a single interface that can be used to retrieve a unified representation of all multi-Cloud resources and to control these resources as needed.	25. inter-Cloud Interoperability	*Not clear of market acceptance*
UCI_Architecture	Technical	Not Mature	This document is intended to give an overview of the proposed UCI architecture.	26. inter-Cloud Interoperability 27. Platform APIs 28. Infrastructure APIs 29. Data APIs 30.	*Not clear of market acceptance*

Distributed Management Task Force (DMTF)

- Type: *Industry Consortium*
- Scope: Using the recommendations developed by DMTF's Open Cloud Standards Incubator, the Cloud management workgroup (CMWG) is focused on standardizing interactions between Cloud environments by developing specifications that deliver architectural semantics and implementation details to achieve interoperable Cloud management between service providers and their consumers and developers.

Spec.	Type	Timeline	Scope	Issue related	Comments
OVF	National Body Standard INCITS 469-2010	August 2010	The *Open Virtualization Format (OVF) Specification* describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.	31. Data/Service Lock-in 32. Inter-Cloud Interoperability 33. Virtualization 34. Patterns for interoperation and interconnection of Clouds	Enables portable movement of IaaS workloads from Cloud to Cloud
Interoperable Clouds	Consortium	November 2009	Describes the work being done in the DMTF Open Cloud Standards Incubator, including use cases and reference architecture as they relate to the interfaces between a Cloud service provider and a Cloud service consumer.	35. Data/Service Lock-in 36. Inter-Cloud Interoperability 37. Patterns for interoperation and interconnection of Clouds	Whitepaper
Architecture for Managing Clouds	Consortium	June 2010	This white paper is one of two Describes the reference architecture as it relates to the interfaces between a Cloud service provider and a Cloud service consumer. The goal of the Incubator is to define a set of architectural semantics that unify the interoperable management of enterprise and Cloud Computing.	38. Data/Service Lock-in 39. Inter-Cloud Interoperability 40. Patterns for interoperation and interconnection of Clouds	Whitepaper
Use Cases and Interactions for Managing Clouds	Consortium	June 2010	This document is one of two documents that together describe how standardized interfaces and data formats can be used to manage Clouds. This document focuses on use cases, interactions, and data formats.	41. Data/Service Lock-in 42. Inter-Cloud Interoperability 43. Patterns for interoperation and interconnection of Clouds	Whitepaper

Cloud Security Alliance (CSA)

- Type: *Industrial Consortium*
- Scope: To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

http://www.cloudsecurityalliance.org/

Spec.	Type	Timeline	Scope	Issue related	Comments
Security Guidance for Critical Areas of Focus in Cloud Computing	Technical Specification	December 2009	Foundational best practices for securing Cloud Computing	Cloud Security	
Cloud Controls Matrix (CCM)	Technical Specification	December 2010	Security controls framework for Cloud provider and Cloud consumers	Cloud Security	
Top Threats to Cloud Computing	Assessment Specification	March 2010	Threat research	Cloud Security	

ETSI Technical Committee (TC) CLOUD

- Type: *Local (Europe) standard organization*
- Scope: The goal of TC CLOUD is to address issues associated with the convergence between IT (Information Technology) and Telecommunications. The focus is on scenarios where connectivity goes beyond the local network.

The following table doesn't take into account the ETSI work on Grid computing.

Spec.	Type	Timeline	Scope	Issue related	Comments
ETSI TR 102 997 V1.1.1: Initial analysis of standardization requirements for Cloud services	Technical report	April 2010	The present document describes standardization requirements for Cloud services.	None	It is based on the outcome of a 2 days workshop. It is a list of standardization requirements for Cloud services. It could be consider in the SG analysis.
DTR/CLOUD-0010: Use Cases for Cloud Service Scenarios	Technical report	It has just stated	This document will collect and describe Use Cases for Cloud Scenarios. A specific focus will be on those scenarios which impact or interact with communications service providers.	44. General & Fundamentals	It has just stated. Could be considered for future liaison.

Organization for the Advancement of Structured Information Standards (OASIS)

- Type: *Industry Consortium*
- Scope: OASIS is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. It produces standards for security, e-business, web services, application-specific markets as well as facilitates standardization efforts in the public sector. OASIS Technical Committees do work on a wide variety of technologies which will be critical for and widely used in the Cloud Space, e.g. web services, WS-I profiles, security and identity, provisioning, modeling, etc. Much of that work had as its orientation SOA based and enabling technologies, much of which will be directly applicable to the Cloud. In the absence of specific guidance from the SGCC, the criteria used here to determine which Technical Committee's work should be listed in the table is whether the TC's charter work targets Cloud-specific requirements. At this time the OASIS Identity in the Cloud TC is the only one which meets those criteria.

Following the table is a list of OASIS TCs whose work the SGCC might wish to investigate further if the ultimate *criteria it adopts is broader.*

Spec.	Type	Timeline	Scope	Issue related	Comments
Identity in the Cloud Use	*Specification*	*H2 2011*	*Definition of use cases for identity deployment, provisioning and management in a Cloud Computing context.*	45. Security 46. Data ownership 47. Data privacy 48. Inter-Cloud	*OASIS Identity In the Cloud TC Committee*

Cases			*These may be existing use cases or new use cases as the TC determines. Identify gaps in existing in existing Identity Management standards with respect to Cloud.*	Interoperability 49. Patterns for interoperation and interconnection of Clouds 50. Platform APIs 51. Infrastructure APIs 52. Identity	*Draft*

The following table lists TCs that may require further investigation if a broader "relevancy" criteria is adopted. Some of these TCs are quite mature, having mostly completed their work and are in a maintenance mode. Others are actively developing their deliverables and may decide to focus more on Cloud related issues in the future.

Technical Committee	Example Deliverables
OASIS Content Management Interoperability Services (CMIS) TC	CMIS
OASIS Privacy Management Reference Model (PMRM) TC	PMRM
OASIS Provisioning Services TC	SPML
OASIS Security Services (SAML) TC	Security Assertion Markup Language (SAML)
OASIS Service Component Architecture / Assembly (SCA-Assembly) TC (and related Policy, BPEL, and Bindings TCs)	SCA Assembly
OASIS SOA Repository Artifact Model and Protocol (S-RAMP) TC	S-RAMP
OASIS Symptoms Automation Framework (SAF) TC	SAF,
OASIS Web Services Business Process Execution Language (WSBPEL) TC	WS-BPEL
OASIS Web Services Reliable Exchange (WS-RX) TC	WS-ReliableMessaging, WS-MakeConnection
OASIS Web Services Secure Exchange (WS-SX) TC	WS-Trust, WS-SecureConversation
OASIS Web Services Security Maintenance (WSS-M) TC	WS-Security
OASIS Web Services-Interoperability (WS-I) Member Section	Basic Profiles 1.1, 1.2, 2.0, Reliable Secure Profile 1.0, Basic Secure Profile 1.1

Object Management Group (OMG) – no activities

[Note: There is nothing specific to Cloud activities at this point in time. A number of workshops have been held and are planned, but as yet no concrete white papers or specifications are available. I note that there is a specification called SoaML (SOA markup language) which is relevant to WG2, though it is not clear if it has direct relevance to this Cloud activity.]

Storage Networking Industry Association

- Type: *Industry Consortium (US 501 (c) 6 non-profit association)*
- Scope: SNIA's Cloud Technical Working Group (Cloud TWG) is focused on standardizing interactions between Cloud-based storage services and clients by developing specifications that deliver architectural semantics and implementation details to application developers. RESTful HTTP-based protocols are used to enable Cloud service providers to offer interoperable Cloud storage management and access to their consumers and developers.

Spec.	Type	Timeline	Scope	Issue related	Comments
CDMI	Consortium (Proposed PAS submission)	April 2010	The *Cloud Data Management Interface (CDMI)* specification describes an open, secure API for self-provisioning and use of Data-Storage as a Service (DaaS) from a Cloud service provider.	53. Data/Service Lock-in 54. Inter-Cloud Interoperability 55. Self-provisioning 56. Data ownership and use 57. Chargeback	Eventually: federation and inter-Cloud data access issues.
SMI-S	ISO IS24775-2006. Replaces ANSI INCITS 388: 2004	2004 - 2007	The Storage Management Initiative - Specification (SMI-S) enables fine-grained heterogeneous storage management through the use of DMTF's CIM modeling and profiling.	58. Lower level storage management	Later spec revisions are on ANSI INCITS/Fast Track to ISO

ITU-T Focus Group on Cloud Computing

- Type: *International standard organization*
- Scope: The Focus Group analyzes the standardization needs from the telecommunication view point for Cloud Computing. It is focusing on transport via telecommunications networks, security aspects of telecommunications, service requirements, etc.

Spec.	Type	Timeline	Scope	Issue related	Comments
Eco-system:	deliverable	planned in June 2011	This document tries to define the bases of Cloud Computing: taxonomy, definition, use case, general requirement, in order to understand the benefit for telecommunication	59. General & Fundamentals	Very general document focused on Telecommunication ecosystem. It doesn't answer to any specific Issue
Requirements & Reference architecture	deliverable	planned in June 2011	This document proposes architecture to understand better the Standardization needs for telecommunication.	60. Patterns for interoperation and interconnection of Clouds	This is an informative and general document. Future standardization activities could consider this document as an input.
Infrastructure & Network enabled Cloud	deliverable	planned in June 2011	This document defines the functional requirements for a Cloud Computing infrastructure	61. Partly Inter-Cloud Interoperability. 62. Partly Patterns for interoperation and interconnection of Clouds	This is an informative and general document. Future standardization activities could consider this document as an input.
Security	deliverable	planned end of 2011	this document tries to identify necessary study subjects on "Cloud Security" to be worked and	None	This is an analysis which aims new work item proposal, but it is

			studied in ITU-T		still a long list of existing standards, specifications and white paper.
Overview of SDO: Gap analysis	deliverable	planned in June 2011	This document is a list of existing standards, specifications and white papers related to Cloud Computing.	None	The list doesn't really analyze all the standards, specifications and white papers.
Benefits from Telecommunication perspectives	deliverable		This document includes a list of candidate study items.	None	This is an analysis which aims new work item proposal.

Open Cloud Manifesto

- Type: Industry Consortium
- Scope: The Open Cloud Manifesto is an Industry Consortium who is tasked with developing a core set of principals regarding freedom of choice, flexibility and openness in Cloud Computing.

Spec.	Type	Timeline	Scope	Issue related	Comments
Cloud Computing Use Cases	White paper	July 2010	Industry consortium tasked with developing a core set of principles regarding freedom of choice, flexibility and openness.	63. Definitions and Taxonomy 64. Use Case Scenarios 65. Customer Scenarios 66. Developer Requirements 67. Security Scenarios 68. Security Use Case Scenarios 69. SLA	
Moving to the Cloud	White paper	Feb 2011	This paper presents a three-step process for evaluating Cloud Computing: 1. Classify Your Information Assets: Understand the function and value of the organization's applications and data and the risks to the organization if they are lost or compromised. 2. Determine Your Requirements and Risks: Define the requirements of the organization and determine if a Cloud provider exists that is capable of delivering those requirements while keeping the risks at an acceptable level. 3. Calculate Your Return on Investment (ROI): Using the organization's needs, assets, risks and requirements, calculate the cost of moving to the Cloud and compare that to your	70. Classifying Your Information Assets 71. Determine Your Requirements 72. Calculate Your ROI	

			existing costs.		

W3C

[Note: The W3C will not be creating any Cloud-related specifications. Thus, it is recommend that there

needs to be no entries in the table.]

CCF (Cloud Computing Forum in Korea)

- Type: *National Industrial Consortium*
- Scope: CCF is government funded non-profit organization for the standardization of Cloud Computing and Service in Korea. Under CCF, there are 6 WG for policy and certification, Cloud Computing technology framework, media Cloud, storage Cloud, Cloud Computing technology for Green IDC, and mobile Cloud, and it has aim to develop recommendations until Year 2011

KCSA (Korea Cloud Service Association)

- Type: *National Industrial Consortium*
- Scope: KCSA is non-profit organization to realization of Green IT and reinforcing national competition power by sharing information, development of application services based on Cloud and promoting Cloud services based on next-generation internet in Korea. The KCSA has 4 activities as followings:
  - Create of the needs and promotion of the services on Cloud Computing in Korea;
  - Make the environment for the service activation;
  - Promote and enhance the awareness of the services ;
  - Support members and reinforce the network.

The Open Group

- Type: *Industry Consortium*
- Scope: The Open Group Cloud Work Group exists to create a common understanding among buyers and suppliers of how enterprises of all sizes and scales of operation can include Cloud Computing technology in a safe and secure way in their architectures to realize its significant cost, scalability and agility benefits. It includes some of the industry's leading Cloud providers and end-user organizations, collaborating on standard models and frameworks aimed at eliminating vendor lock-in for enterprises looking to benefit from Cloud products and services. http://www.opengroup.org/cloudcomputing

Spec.	Type	Timeline	Scope	Issue related	Comments

Building Return on Investment From Cloud Computing	White Paper	Published	Building Return On Investment from Cloud Computing, *http://www.opengroup.org/cloud/whitepapers/ccroi/index.htm*	73. General & Fundamentals	Targets Cloud consumers, business level
Strengthening Your Business Case for Using Cloud	White Paper	Published	Business use cases and analysis http://www.opengroup.org/cloud/whitepapers/wp_cbuc/index.htm	74. General & Fundamentals	Business level use cases based on actual business scenarios
Cloud Buyers Decision Tree	White Paper	Published	Decision tree to quickly determine if Cloud is a good fit for the business situationhttp://www.opengroup.org/cloud/whitepapers/wp_cloud_dt/index.htm	75. General & Fundamentals	Business level, for Consumers who are buyers
Cloud Buyers Requirements Questionnaire	White Paper	Published	Q&A to collect a potential Cloud solution buyer's business problem and requirements in a standard structure http://www.opengroup.org/cloud/whitepapers/wp_cloud_rq/index.htm	76. General & Fundamentals	Business level, for Consumers who are also buyers
Cloud Computing Explained white paper	White Paper	Drafting Publish: 1H2011	CC Definition, Terms, Benefits, Stakeholders, Standards, interoperability, overview of TOG Cloud deliverables	77. General & Fundamentals	Introductory paper, defines buyers
Cloud Computing Architecture	Technical Standard	Drafting Final: 2H2011	Cloud meta model and architecture based on the SOA RA consistent with CCE and use cases	78. General & Fundamentals 79. 80. Explains these: Quality of Service 81. Security 82. Virtualization 83. Pricing/ chargeback	Under development, Metamodel drafted, inputs from IBM, Boeing, Capgemini
Service Oriented Cloud Computing Infrastructure Framework	Technical Standard	2Q2011	(Joint work with SOA WG) is defining architecture and recommendations for provisioning infrastructure as a service in both SOA and Cloud architectures and solutions.	84. General & Fundamentals 85. Quality of Service 86. Device Independence 87. Virtualization	Defines concepts and ABBs for IaaS
Security For Cloud and SOA Reference Architecture	Technical Standard	Drafting Final: 1Q2011	(Joint work with SOA WG) will be defining a Cloud security reference architecture which will define building blocks that address the appropriate confidentiality, integrity, and availability requirements of SOA and Cloud Computing.	88. General & Fundamentals 89. Quality of Service 90. Security 91. Data Confidentiality and 92. Auditability 93. Data ownership 94. Data	Defines concepts/arch for security

				privacy	
Open Group Cloud Security position paper		2Q2011	Compare and Contrast SOA Security RA with other industry Security standards	95. General & Fundamentals 96. Security 97. Data Confidentiality and 98. Auditability 99. Data ownership 100. Data privacy	Compares security standards

Study Group on Smart Cloud (Japan) – TBD

European Network and Information Security Agency (ENSIA) – TBD

ISO/IEC JTC 1/SC 27

- Type: *International standard organization*
- Scope: The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as management of information and ICT security; security processes, controls and services; cryptographic and other security mechanisms for protecting the accountability, availability, integrity and confidentiality of information; Security aspects of identity management, biometrics and privacy; Conformance assessment, accreditation and auditing requirements in the area of information security;

Spec.	Type	Timeline	Scope	Issue related	Comments
Spec.	*Can be International /regional/ National Standard, Technical specification, Technical report, deliverable (like SGCC deliverables)*	*Can be Published, planned in month, year*	*limited to 5 lines*	101. Issue listed in Appendix 6 of N126 and future update: 102. General & Fundamentals 103. Data/Service Lock-in 104. Quality of Service 105. Security 106. Data Confidentiality and 107. Auditability 108. Data ownership 109. Data privacy 110. Software	*Advantages* *Disadvantages* *Technology neutral?* *Lacks…*

				Licensing 111. Legal 112. Inter-Cloud Interoperability 113. Device Independence 114. Virtualization 115. Pricing/chargeback 116. Cloud management 117. Patterns for interoperation and interconnection of Clouds 118. Platform APIs 119. Infrastructure APIs 120. Data APIs 121. Environment 122. Management 123. Identity…	
Report on Study Period “Cloud Computing security and privacy“	*deliverable*	*Planed in April 2011*	*The objective of the Study Period is to identify the scope and audience of new international standards in the field of „Cloud Computing security and privacy“.*	124. General & Fundamentals 125. Security 126. Data privacy	
ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements “	*International Standard*	*Published in 2005, currently under revision*	*This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks.*	127. General & Fundamentals 128. Security 129. Data privacy 130. Data Confidentiality and Auditability 131. Management	
ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management	*International Standard*	*Published in 2005, currently under revision*	*This International Standard provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.*	132. Security 133. Data privacy 134. Data Confidentiality and Auditability	
ISO/IEC 27005 Information technology — Security techniques — Information security risk management	*International Standard*	*Published in 2008, update planned for 2011*	*This International Standard provides guidelines for information security risk management. It provides guidance on implementing a process oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001.*	135. Security 136. Management	
ISO/IEC 27036 Information technology –	*International Standard (multi-part)*	*Currently on WD level*	*This international Standard provides guidelines how to manage the information security risks in supplier relationships. It provides further*	137. Security 138. Data privacy 139. Data Confidentiality and Auditability	

Security techniques – Information security for supplier relationships			*detailed implementation guidance on the controls dealing with supplier relationships that are described at a basic standardized level in ISO/IEC 27002.*		
ISO/IEC 29100 Information technology — Security techniques — Privacy framework	*International Standard*	*Currently on FCD level*	*This International Standard provides a privacy framework applicable to the safeguarding of privacy when PII is being processed in ICT systems. It is applicable to individuals and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating ICT systems or services where privacy controls are required for the processing of PII*	140. General & Fundamentals 141. Security 142. Data privacy 143. Identity	
ISO/IEC CD 29101 Information technology – Security techniques – Privacy reference architecture	*International Standard*	*Currently 2nd CD*	*This International Standard describes a reference architecture that should guide individuals and organizations who specify, procure, architect, design, develop, implement, test, maintain, administer, and operate ICT systems on how to: address privacy safeguarding requirements when processing PII,*	144. General & Fundamentals 145. Security 146. Data privacy 147. Identity	
ISO/IEC CD 24760 Information technology — Security techniques — A framework for identity management	*International Standard (multi-part)*	*(Part 1 currently on FCD level)*	*This International Standard specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management and privacy protection. It also provides a bibliography of documents related to standardization of various aspects of identity management.*	148. General & Fundamentals 149. Security 150. Data privacy 151. Identity	
ISO/IEC WD 29146 Information technology — Security techniques — A framework for access management t	*International Standard*	*Currently on WD level*	*This International Standard defines and establishes a Framework for Access Management (AcM) and the secure management of the process to access information and ICT information resources, associated with the accountability of an entity within some context.*	152. General & Fundamentals 153. Security 154. Data privacy 155. Identity	

Institute of Electrical and Electronic Engineers (IEEE)

- Type: SDO
- Scope: (TBD)

Spec.	Type	Timeline	Scope	Issue related	Comments
IEEE P2301 Guide for Cloud Portability and	SDO	May 2012	This guide advises Cloud Computing ecosystem participants (Cloud vendors, service providers, and users) of	156. General & Fundamentals 157. Data/Service Lock-in 158. Quality of Service	The purpose of this guide is to assist Cloud Computing vendors and users in developing, building,

Interoperability Profiles (CPIP)			standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions. This guide groups these choices into multiple logical profiles, which are organized to address different Cloud personalities.	159. Security 160. Data Confidentiality and Auditability 161. Data ownership 162. Data privacy 163. Software Licensing 164. Legal 165. Inter-Cloud Interoperability 166. Device Independence 167. Virtualization 168. Pricing/chargeback 169. Cloud management 170. Patterns for interoperation and interconnection of Clouds 171. Platform APIs 172. Infrastructure APIs 173. Data APIs 174. Environment 175. Management 176. Identity	and using standards-based Cloud Computing products and services, which should lead to increased portability, commonality, and interoperability. Cloud Computing systems contain many disparate elements. For each element there are often multiple options, each with different externally visible interfaces, file formats, and operational conventions. In many cases these visible interfaces, formats, and conventions have different semantics. This guide enumerates options, grouped in a logical fashion called "profiles," for such definitions of interfaces, formats, and conventions, from a variety of sources. In this way, Cloud ecosystem participants will tend towards more portability, commonality, and interoperability, growing the Cloud Computing adoption rate overall.
IEEE P2302 Standard for Intercloud Interoperability and Federation (SIIF)	SDO	October 2012	This standard defines topology, functions, and governance for Cloud-to-Cloud interoperability and federation. Topological elements include Clouds, roots, exchanges (which mediate governance between Clouds), and gateways (which mediate data exchange between Clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit. The standard does not address intra-Cloud (within Cloud) operation, as this is Cloud implementation-	177. Data/Service Lock-in 178. Quality of Service 179. Security 180. Data Confidentiality and Auditability 181. Data ownership 182. Data privacy 183. Software Licensing 184. Legal 185. Inter-Cloud Interoperability 186. Device Independence 187. Pricing/chargeback 188. Cloud management 189. Patterns for interoperation and interconnection of Clouds 190. Management 191. Identity	This standard creates an economy amongst Cloud providers that is transparent to users and applications, which provides for a dynamic infrastructure that can support evolving business models. In addition to the technical issues, appropriate infrastructure for economic audit and settlement must exist.

			specific, nor does it address proprietary hybrid-Cloud implementations.		

CESI (China Electronics Standardization Institute)

- Type: *National Standard Organization*
- Scope: CESI, founded in 1963, is a governmental standardization institute in the field of electronics and IT industry under the Ministry of Industry and Information Technology(MIIT) China. Currently, CESI has two working groups involved in the field of Cloud Computing standards, including SOA-WG and ITSS-WG. On 19, Nov. 2010, a worldwide conference was held to analyze standard requirements and promote communications between government, industry, SDOs, academia and customers.

Spec.	Type	Timeline	Scope	Issue related	Comments
Cloud Computing Standardization Study	Deliverable	Draft version published in 11, 2010	This document tries to give key supporting technologies and relevant SDOs on Cloud Computing. Besides, a standard framework on Cloud Computing is given, which consists of five parts: fundamentals, key technologies & products, management, testing and security.	192. General & Fundamentals	This is an informative and general document. It doesn't answer to any specific Issue.
Operation Requirements for Cloud Computing services	Deliverable	Draft version published in 11, 2010	This document summarizes the internal elements and external characteristics of Cloud Computing service and defines a service model. Four basic internal elements of service: people, resource, technology and process. This proposal provides guide to improve quality of providers' services.	193. Quality of service & management	The document proposes methods and principles to evaluate the capability of Cloud Computing service providers.

Cloud Industry Forum (CIF)

- Type: *Industry Association*
- Scope: The Cloud Industry Forum focuses on building trust between suppliers and consumers of Cloud services for doing business in the Cloud. A major part of this scope is a certifiable Code of Practice covering transparency, capability, and accountability of participating service providers. The outcome requires the provision of key organizational, commercial and operational information in a consistent format that will assist end users in determining how they adopt Cloud services and from whom.

Spec.	Type	Timeline	Scope	Issue related	Comments
Cloud	Code of	Published	The Code of Practice defines	Disclosure, plus all other	Scheme is

Industry Forum Code of Practice	Practice (deliverable)	November 2010 (V5)	certifiable requirements for disclosure (both public and under NDA terms), capability (comparable to mini-ISO 9001s), and accountability.	categories. (The Code of Practice does not mandate any specific technical standards, but provides for disclosure of such information. In particular, it requires disclosure of information which will allow purchasers to make informed decisions about the supplier, including for issues related to ownership, security, regulation, standards supported, and technological lock-in.) The Code of Practice requires all self certified organisations to present the public information in a standard format to enable effective comparison by end users.	based on self-certification, with program of independent confirmation audits. Third-party independent certification option is planned.

Annex 3: Report of the Analysis of Standards Requirements for Cloud Computing

We give an analysis on Cloud Computing related SDOs and corresponding specifications, through which we point out the focus of current study and what we should do in future.

Table 1. A list of Cloud Computing related deliverables

DeliverNo	DocName	SDO
D01	Cloud Computing Use Cases White Paper	CCUCDG (Cloud Computing Use Case Discussion Group)
D02	Security Guidance for Critical Areas of Focus in Cloud Computing	CSA
D03	Top Threats to Cloud Computing	CSA
D04	CSA Cloud Controls Matrix	CSA
D05	Domain 12: Guidance for Identity & Access Management	CSA
D06	Open Virtualization Format Specification	DMTF
D07	Interoperable Clouds	DMTF
D08	Architectures for Managing Clouds	DMTF

Formatted: Font: Not Bold, No underline, Font color: Auto

Formatted: Font: Not Bold

D09	Common Information Model System Virtualization	DMTF
D10	Use Cases and Interactions for Managing Clouds	DMTF
D11	Grid and Cloud Computing Technology: Interoperability and Standardization for the Telecommunications Industry.	ETSI TC Grid
D12	Use Cases and Functional Requirements for Inter-Cloud Computing	GICTF
D13	Distributed Computing: Utilities, Grids & Clouds.	ITU-FG
D14	Repository on activities in Cloud Computing Standardization.	ITU-FG
D15	NIST definition of Cloud Computing	NIST
D16	MalStone: A Benchmark for Data Intensive Computing	OCC
D17	Open Cloud Manifesto	(OCM) Open Cloud Manifesto
D18	Open Cloud Computing Interface Specification	OGF
D19	Open Cloud Computing Interface - Use cases and requirements for a Cloud API	OGF
D20	Cloud Storage for Cloud Computing	OGF & SNIA
D21	Cloud Data Management Interface (CDMI)	SNIA
D22	Managing Data Storage in the Public Cloud	SNIA
D23	Building ROI from Cloud Computing white paper	TOG
D24	Strengthening your Business Case for Using	TOG

	Cloud white paper	
D25	Cloud Buyers' Decision Tree V1 white paper	TOG

In our analysis, we divide the current study on Cloud Computing into 5 issues: fundamental, interoperability, management, security and testing. Table 2 gives a matrix between SDO and five issues.

Table 2 An overview of Cloud Computing issues and corresponding SDOs

Issue SDO	Fundamental	Interoperability	Management	Security	Testing	Count
CCUCDG	D01					1
CSA				D02,D03, D04,D05		4
DMTF		D06,D07,D09	D08, D10			2
ETSI	D11					1
GICTF	D12					1
ITU-FG	D13,D14					2
NIST	D15					1
OCC					D16	1
OCM	D17					1
OGF		D18,D19,D20				3
SNIA		D21,D22				2
TOG	D23,D24,D25					3
SUM	10	8	2	4	1	25

From table 2, it can be seen that most SDOs and their deliverables focus on fundamental and interoperability issues. We further analyze deliverables on these two issues. The analysis on fundamental issue is illustrated in table 3. In table 3, it can be seen that current study on fundamental covers four aspects, including definition & principle, requirements & use case, comparison with other paradigms, economy analysis. Among them, requirement and uses case dominate and covers 50% of all.

Table 3 An overview of fundamental issues and corresponding SDOs

Fundamental SDO	Definition & Principle	Requirement & Use case	Comparison with other paradigms	Economy analysis
CCUCDG		D01		
ETSI			D11	
GICTF		D12		
ITU-FG		D14	D13	
NIST	D15			
OCM	D17			
TOG		D24		D23,D25
SUM	2	4	2	2

The analysis on interoperability is illustrated in table 4. In table 4, we divide interoperability into requirement and three types of APIs: infrastructure API, data API and platform API.

Table 4 An overview of interoperability issues and corresponding SDOs

Interoperability SDO	Infrastructure API	Data API & Platform API	Requirement
DMTF	D06		D07, D09
OGF	D18	D20	D19
SNIA		D21,D22	
SUM	2	3	3

From above analysis, we draw the following conclusions:

1. Cloud Computing standard study is still at a primary stage and most of current study focuses on fundamental issues.

2. Interoperability is an important issue to be studied. Although there are some efforts on infrastructure API and data API, there are still many unsolved problems. Besides, as more and more SaaSs are put into operation, requirements on common platform API are at need.

3. Since Cloud Computing is a new type of computing paradigm which covers large area of aspects, it is an important problem to evaluate service providers with different capabilities. Although current study on testing is very little, it could be a prominent area.

Annex 4: Future Reference Architecture Work

Note: The material in this annex will be considered by the SC38 CCSG to decide if a NWI on a Cloud Computing Reference Architecture is appropriate. NBs and liaisons are requested to provide comments on this material, the existing problems/issues already identified and the feasibility of such an NWI.

Note: NBs and liaison are requested to provide comments on aligning the material in this Annex with other material the draft CCSG report especially the adopted NIST Cloud Computing definition (from N164).

5.4a Components of Cloud Computing

Figure 5.1~~Figure 5.1Figure 5.1~~ depicts the basic entities associated with Cloud Computing.

Cloud Services include products, services and solutions that are delivered and consumed in real-time over the Internet. For example, Web Services which may be accessed by other Cloud Computing components, software, e.g., Software plus services, or end users directly. Also, Cloud Services leverage the Cloud in software architecture, often eliminating the need to install and run the application on the customer's own computer.

Cloud Platform is the delivery of a computing platform, and/or solution stack as a service, which facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.

Cloud Infrastructure is the delivery of computer infrastructure, typically a platform virtualization environment.

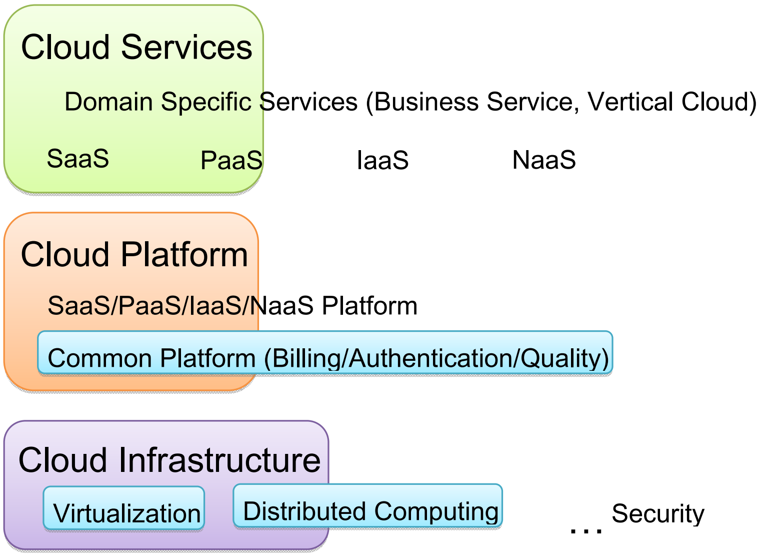
Cloud Services
Domain Specific Services (Business Service, Vertical Cloud)
SaaS
PaaS
IaaS
NaaS
Cloud Platform
SaaS/PaaS/IaaS/NaaS Platform
Common Platform (Billing/Authentication/Quality)
Cloud Infrastructure
Virtualization
Distributed Computing
...
Security

Figure 5.1 - Conceptual Diagram of Cloud Computing

In Figure 5.1~~Figure 5.1Figure 5.1~~, domain-specific services are located in the Cloud Services layer. These are Clouds specializing in certain industries, such as the healthcare field, financial institutions, IPTV field, media field, and etc, as a kind of intra-industry "mutual aid organization."

Formatted: Font: 12 pt

Formatted: Font: 12 pt, No underline, Font color: Auto

Examples of how such a Cloud might form include present-day third-party vendors, or an industry-leading large company possibly opening up its internal resources to allow third-party access.

Editor's Note: The term NAAS from Figure 5.2 is undefined. A description is required. It is for further study whether this diagram accurately portrays the definitions as provided in this report.

Editors Note: (N149/DE010) The terms “SaaS”, “IaaS”, “PaaS”, and “NaaS” are not explain yet. What is “NaaS”? Network as a Service?

Add definitions of the terms mentioned to the explaining text for Fig. 2.

Editors Note: (N177/CA021) Canada has noticed that security, management and governance are not explicitly identified as components.

Review and update Figure 5.2 and the accompanying text to reflect the accepted set of Cloud Computing components. This should include security, operations and policy management.

Editors Note: (N149/DE011) As shown and marked in editor's note there's no definition for NaaS.

Please explain which service is mentioned with NaaS. Add the definition of NaaS to 3.1 or remove it from text and figure 5.2

Editors Note: (N149/DE012)The Term "domain specific services" is not defined clearly. As shown in figure 5.2 it might be a service like PaaS, SaaS, IaaS or NaaS. What's the difference between IaaS and the "domain specific services"?

Please add a definition to 3.1 . A clarification should be added in 3.1.

Editors Note: (N177/CA020) Table 6.1 provides a significant amount of information about the Cloud Service Models (IaaS, PaaS and SaaS) that needs to be captured in Section 5

Text coming from N126 that should be moved here:

"There are a large number of Internet users and SMEs with different functional requirements, and different businesses also lead to different requirements for Cloud Services. The customers/users need to reduce the total cost of ownership (TCO) of the infrastructure, make the business mode more flexible, and improve the driving ability of business, etc. Cloud Computing can help to provide shared resources which are customized for the common requirements of different users, so we still depend on the value-added service provider to customize personalized services to meet the needs of different users and form a complete service framework. Currently, this is especially important for enterprise applications.”

The first part of section 6.3 and Table 6.1 should be moved to Section 5.4 to add more explanation for Figure 5.2.

NOTE: This change has been included in the proposed revised Section 5 attached to these comments.

Editors Note: (N189/CN011) 1.What does NaaS mean? If it means Network-as-aService, it is not at the same level as IaaS. It may be involved in IaaS.

2.SaaS also includes domain specific services.

3.The term Cloud Platform and Cloud Infrastructure need more explanation.

4.There need some explanation about the relationship between Figure 5.2 and the following standardization requirement.

Remove Figure 5.2.

Editors Note: (N188/GB011) Entities defined in Figure 5.2 are not all explained in the accompanying text - such as "NaaS" and "Common Platform"

Provide clear definitions of all the entities in the diagram that have names or acronyms applied to them.

Editors Note: (N149/DE019, DE031) The definition of NaaS should be added

Add the definition as mentioned above.

Editors Note: (N175/INLAC02) There are many terms that do not appear in the main body of the text. Some examples are:

1.Claimant

2.Digital identity

3.Identity proofing

4.IdP

5.

MDA

6.NaaS

Content of this section must be reviewed and only the necessary terms shall be part of it.

Editors Note: (N189/CN02) It should be commented why only Iaas, Paas and Saas be announced except Naas. In Section5.4, there is a basic description about both Iaas, Paas, Saas and Naas in the components of Cloud Computing.

Give the description of NaaS

Editors Note: Japan has proposed the following alternative to the above section.

5.4b Service models of Cloud Computing

Figure 5.2 depicts the Service Models of Cloud Computing.

Information system is decomposed into three layers, infrastructure, platform and application (or software). Cloud Computing is categorized into three service models.

IaaS (Infrastructure as a Service) is a service model whose boundary to consumer is an infrastructure.

PaaS (Platform as a Service) is a service model whose boundary to consumer is a platform.

SaaS (Software as a Service) is a service model whose boundary to consumer is an application (or software).

Service model depends on which layer faces to consumers.

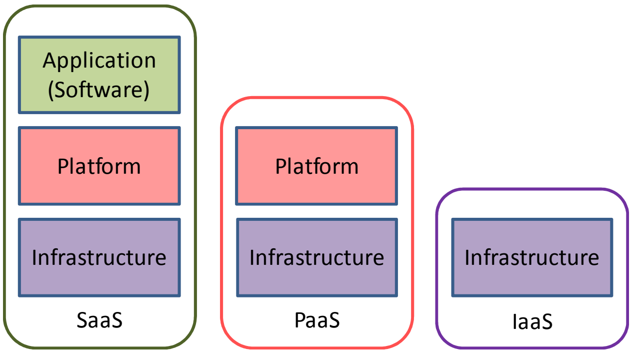

Figure 5.2 Service models of Cloud Computing

5.5a Cloud Computing Roles

TBD

Editors Note: (N171/FI14) There are no comments on use cases expected to be utilized with Clouds nor set of current references

Add to 5.5. Subsections role, use scenarios, customer concerns.

Common use scenarios: "Cloud Computing business use cases have been modeled by e.g. the Google Cloud use cases group (Google Use cases 2010), NIST use cases group (Badger et al. 2010) and the Open Group Cloud Use Cases (CBA)"

Customer concerns: common concerns are explicated e.g. in IDC (2010) report, UCB report (Armbrust et al 2009) and the Forbes (2010) report. The concerns differ between private and public Clouds (Forbes 2010).

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2009), "Above the Clouds: A Berkeley View of Cloud Computing", Publication of Reliable Adaptive Distributed Systems Laboratory, University of California, Berkeley

Badger, Lee; Bohn, Robert; Chandramouli , Ramaswamy, Grance, Tim, Karygiannis , Tom, Patt-Corner, Robert and Voas, Jeffrey Voas (2010), "Cloud Computing use cases", NIST Information Technology Laboratory, 2010, Available from: http://www.nist.gov/itl/Cloud/use-cases.cfmForbes (2010), "Seeding the Clouds: Enterprises set their strategies for Cloud Computing", Forbes Insight, 2010

IDC (2010), "Cloud Computing 2010: an IDC update", Available from: http://www.slideshare.net/JorFigOr/Cloud-computing-2010-an-idc-updateGoogle use cases group (Cloud Computing use case discussion group) (2010), "Cloud Computing use cases", version 4, July 2nd, 2010, available from: http://opencloudmanifesto.org/Cloud Computing Use Cases Whitepaper-4 0.pdf

Editors Note: (N171/FI15) 5.5. Cloud role discussion could be beneficial

Add a section describing role definitions on Cloud consumer, cloud provider, Cloud integrator or other 3rd parties (e.g. brokers, publishers, mediators, service rating providers, notaries etc).

It would be preferable that roles are attached to some kinds of perspective that is used otherwise implicitly e.g. design time or runtime of service, based on point-to-point service use, ecosystem of service or industry ecosystem (in which case consulting etc. becomes relevant) or some other constraint.

Editors Note: (N189/CN12) There are many roles, such as “Infrastructure provider”, “Service Provider”, “Consumer”, “End-User”, ”Third-party”, used in Section 6 and Figure 6.1, and “Cloud Consumer”, “Cloud Provider” and “Cloud Developer” used in Section 10.1.

In Section 5.5, it is supposed to define and list all the Cloud Computing roles.

Editors Note: Japan has proposed the following alternative to the above section.

5.5b Players in Cloud Computing

Figure 5.3 depicted players in Cloud Computing. Main players in Cloud Computing are Provider and Consumer.

Provider, who provides a service of Cloud Computing (any of service models).

Consumer, who uses a service of Cloud Computing which is provided by Provider.

In the Cloud Computing ecosystem, there are another two roles.

Enabler, who deploys and enables Cloud Computing. For instance, solution (hardware/software) vendor, and integrator are Enablers.

Operator, who operates and manages services of Cloud Computing. Operator may be the same with Provider. But in some case, Operator is different from Provider.

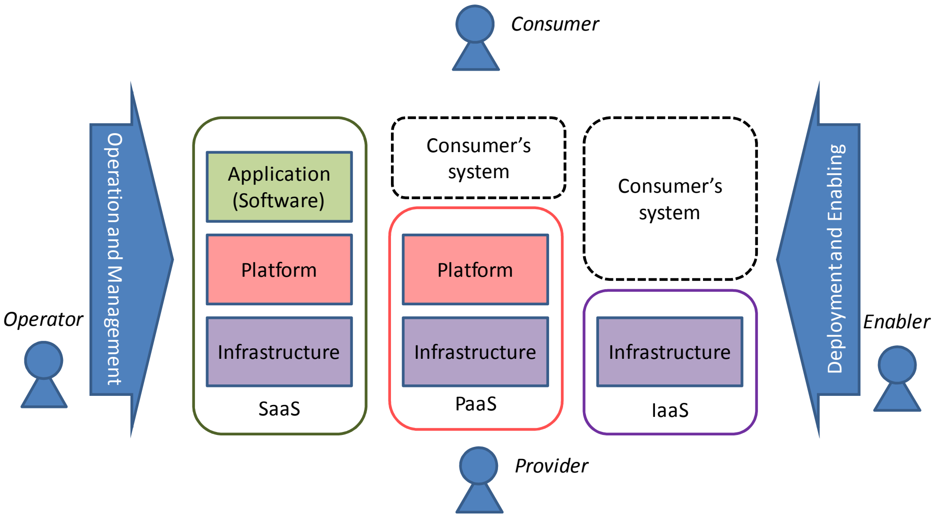

Figure 5.3 Players in Cloud Computing

In some case, Consumer may become a Provider. For instance, Consumer who uses a PaaS can add an application on top of the PaaS and provide another service of SaaS to someone as shown in Figure 5.4 (a). Thus End user can be defined as a special role of Consumer.

End user, who uses a Cloud service by itself and does not provide Cloud service to anyone. End user is a Consumer, but Consumer may not be an End user.

Figure 5.4 (b) and (c) depicts simple cases of End user. Consumer of IaaS may be an End user as Figure 5.4 (c).

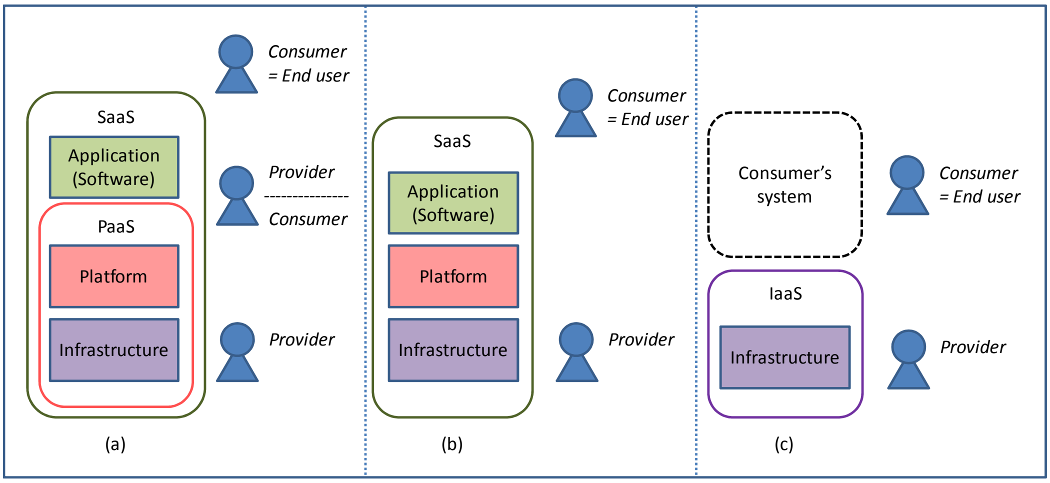

Figure 5.4 (a)-(c) Examples of relationship for Provider and Consumer

Part 2: Standardization Requirements for Cloud Computing

Cloud Computing Industry Ecosystem

The Cloud Computing scenarios described in Section 6.1 include several representative roles in Cloud Computing. In fact, the different roles of Cloud Computing service providers, users and regulatory bodies at all levels come together as a Cloud Computing industry ecosystem.

As shown in Figure 6.1, roles in Cloud Computing can be divided into four categories corresponding to the different sectors in the Cloud Computing industry ecosystem:

1. The Cloud Service Creator is responsible for creating a Cloud service, which can be run and offered through a Cloud Service Provider to the Cloud Service End Users. Typically, Cloud Service Creators build their Cloud services by leveraging functions which are exposed by a Cloud Service Provider. A Cloud Service Creator designs, implements and maintains runtime and management artefacts specific to a Cloud service. The Cloud Service Creator can be an organization (for profit or open source) or a human being. There might different kinds of service creators. Some of them are original service developers, while Cloud Service Composers leverage and combine existing services to create new capabilities. Cloud Service Offering Managers look at these services and find ways to package and offer them in different ways that are meaningful in the market place.

2. The Cloud Service Provider is responsible for providing Cloud services to Cloud Service End Users. A Cloud Service Provider is defined by the ownership of a common Cloud management platform (CCMP). This ownership can either be realized by truly running a CCMP by himself or consuming one as a service. Based on the kinds of Cloud services he provides, the Cloud Service Provider can be an IaaS Provider, PaaS Provider, SaaS Provider or BPaaS [1]Provider. And many times, Cloud Service Providers tend to mix the type of services they provide so the distinction is not always clear cut. A Cloud Service Provider and a Cloud Service End User at the same time would be a partner of another Cloud service provider reselling Cloud services or consuming Cloud services and adding value add functionality on top, which would in turn be provided as a Cloud service. Such people are classified as Value-added Cloud Service Provider. In support of these, there is the Infrastructure provider who provides the servers, storage, network connectivity, and other facilities such power, staffing, space and premise security etc.

Formatted: Tab stops: Not at 18 pt

3. A Cloud service end user is an organization, a human being or an IT system that consumes service instances delivered by a particular Cloud service provider. The service end user may be billed for all (or a subset of) its interactions with Cloud service and the provisioned service instance(s). The Cloud service end user typically browses the service offering catalog and triggers service instantiation and management from there. The Cloud Service End User includes individual users (internet users and mobile device users, such as the white-collar Mary in Scenario 1), enterprise users (such as the small company established by Tom in Scenario 2, the large corporation JumboJoe in Scenario 3), and regulatory bodies.

4. Last but not least is the third-party Audit and Governance who will coordinate, mediate, arbitrage or mitigate conflict of interests for common good or for a particular dispute.

[1] **Business-Process-as-a-Service**

"*Business process services are any business process (horizontal or vertical) delivered through the Cloud service model (Multi-tenant, self-service provisioning, elastic scaling and usage metering or pricing) via the Internet with access via Web-centric interfaces and exploiting Web-oriented cloud architecture. The BPaaS provider is responsible for the related business function(s).*" [Source: IBM MI and IPR definition bridge between Gartner and IDC, Aug 19, 2010]

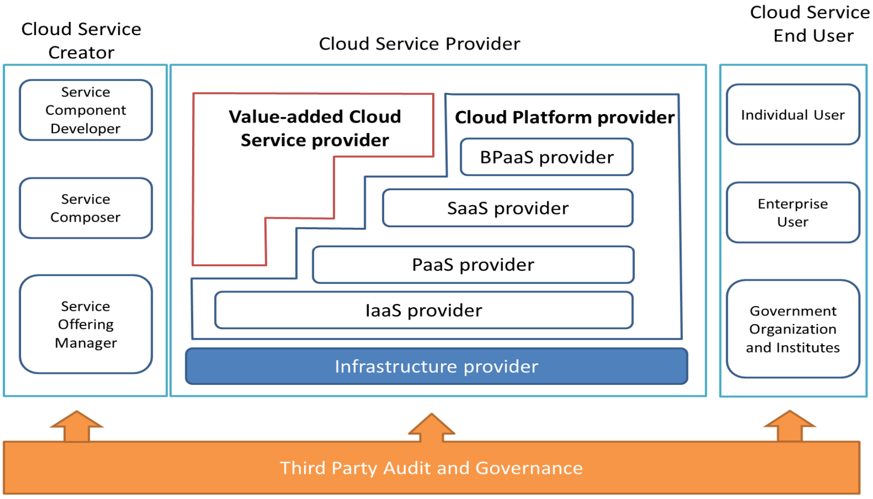

Figure1.1 Cloud Computing Industry Ecosystem Analysis

Editors Note: The above diagram is related to the diagrams in the previous clause in this Annex.

As can be seen from Figure 1.1, the value of the Cloud Computing industry ecosystem is delivered through services, forming a multi-level structure. The end users' demands also transfer from the end users to the service provider, even to the infrastructure provider, through the opposite direction of the service delivery. Cloud Service Providers must work together to ensure that the challenges to Cloud adoption (security, integration, portability, interoperability, governance/management, metering/monitoring) are addressed through open collaboration and the appropriate use of standards. Cloud Service Providers must use and adopt existing standards wherever appropriate to protect the IT investment the whole ecosystem has already made. Cloud Service End User needs, not merely the technical needs of Cloud Service Providers, should be the primary driving force for the ecosystem community efforts such that Cloud Computing standards organizations, advocacy groups, and communities should work together and stay coordinated, making sure that efforts do not conflict or overlap.

6.2 Typical Scenarios and Analysis of Cloud Computing

Editors Note: (N189/CN13) The following sub-clause defines how the components in the previous Annex 4 clause figure (Figure 1.1 "**Cloud Computing Industry Ecosystem Analysis"**) are used.

There has long been envisioned for Information Technology service providers to provide computing capabilities for their customers/users in a utility manner similar to t water, electricity, gas etc. Cloud Computing is widely believed to be able to make this vision into reality. Many individuals, enterprises and service providers are all beginning to test water with Cloud Computing. However, the ubiquity and convenience of Cloud Computing also comes with its own share of issues. We illustrate here a few sample scenarios to explain the necessity and challenge of Cloud Computing related standards.

Scenario 1: for an individual user

Although fairly new to Cloud Computing , Mary decides to store most of her personal data, such as mails, photos, diaries, etc., in the Cloud, because it is easier to share them with her friends this way, and she can access her own them anywhere. In this scenario, she need not worry about data loss due to viruses and hardware failures at home or office, because the SLA she has with the service provider clearly states the availability and data backup plan. However, should she feel the need to switch to another service provider, or should her current service provider go out of business, it will be very difficult to transfer the data to another service provider. At the same time, she is reading so many media discussions on privacy horror stories that she begins to wonder whether it's wise to place some private files in "somebody else's place", because her SLA with the service provider does not say anything about it.

Some similar scenarios from standards development organizations working on Cloud Computing, including:

- Cloud Computing Use Cases White Paper. URL: http://cloudusecases.org/ • Strengthening your Business Case for Using Cloud: Cloud Business Use-Case Analysis. URL http://www.opengroup.org/cloud/whitepapers/wp_cbuc/cbuc-analysis.htm • Reaching for the Cloud(s): Privacy Issues related to Cloud Computing. URL: http://www.priv.gc.ca/information/pub/cc_201003_e.cfm • The future of Cloud Computing: Opportunities for European. Expert Group Report, European Commission, 2010. URL: cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

These scenarios indicate that the Cloud Computing still challenged the following problems. Vendor lock-in, privacy and SLA. With privacy problem, it is vital that a Cloud provider deliver the added controls needed to protect sensitive data, including the ability for the user to audit the Cloud provider to prove that if followed the appropriate procedures. Availability is a clear requirement for any system. Where it is in the Cloud or in the data centre down the hall. Business continuity and disaster recovery are also part of availability. All the things need to be considered by the end user of the Cloud Computing.

Scenario 2: for a small-medium enterprise

Tom has just started his own eCommerce business, but he does not have the budget or skills to build or maintain his own IT infrastructure. Fortunately, an IT service provider ClearSky is able to provide him a suite of applications from the internet with a flat monthly fee as a starter: e-mail, customer relationship management, sales analytics, data analytics and so on. Tom is happy with the functionality of the suite, and the price tag. He is every more happy with the fact that he can focus on his own business competency, ie. managing online sales and promotion. However, the service can be unavailable occasionally. Some of such incidences last week resulted in business interruption and loss of sales, . Besides, interoperability among service providers is also becoming a big concern now. For example, Tom loves the data analytics from RainShelter his friend Jerry has been showing him, but he could not find a way to pipe his CRM data and sales number from ClearSky to RainShelter. Tom is worried if he has to hire someone to do the job, and its future maintenance cost.

Some similar scenarios from standards development organizations working on Cloud Computing, including:

- Cloud Computing Use Cases White Paper. URL: http://cloudusecases.org/ • The future of Cloud Computing: Opportunities for European. Expert Group Report, European Commission, 2010. URL: cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

These scenarios indicate that the Cloud Computing still challenged by lack of service related standards and specifications. How to define function, data format, QoS and interface of services, different service providers give different answers, which results in difficulty in service selection, service immigration, and service integration. Standards should be developed to allow users to choose a proper service provider which can guarantee the QoS requirements of their business, and to allow users to establish connectivity between Cloud A and Cloud B systems through integration appliances.

Scenario 3: for a large enterprise

JumboJoe is a globally well recognized industry leader. In order to maintain its leadership, it speeds huge amount of money to maintain its IT infrastructure. However, a recent audit finds that most of these money are spent on maintenance, with less than 10% for new initiatives. Furthermore, 50% of the machines seat idle 80% of the time; machines in use have only 30% CPU utilization on average. JumboJoe also maintains a set of very expensive software licenses which they uses only a couple of times a year. In an extreme case, JumpboJoe has be maintaining a software license that they have not touched for 5 years. JumboJoe would love to be able to purchasing servers and storage as demand increases and pay a usage fee for those occasionally used software. They figure they can save up to 50% of the equipment budget. And further saving can be archived because they can reduce the size of their data centres, and well as they maintenance staff. However, JumboJoe is concerned with a number of technicality issues, such as: (a) there only a very limited number range of parameters they can specify for the servers they would buy, and if the servers are delivered as specified. (b) current SLA and security assurance from the service provider might not meet JumboJoe's corporate instruction on IT infrastructure, particularly the company's data security policies might not allow mission critical data be to stored on a server outside the company premise; and (c) JumboJoe is confused which service provider to choose because there are so many of them. JumboJoe does not have a framework to compare their quality of service, the range of products, the relative ranking of performance, and most of all the peace of mind that the rating from a trusted authority.

There are many public uses cases from different SDO and vendors. For example the white paper from opencloudmnifesto.org (http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf) listed several scenarios related to enterprises usage of Cloud Computing.

The second and third problems listed for large enterprise scenario are related to standardization and interoperability, security and privacy, which need to be clearly stated and emphasized.

Scenario 4: Individual Developer and Start-up Software Company

David was an individual developer and would like found a start-up company to build web application to provide innovation service to consumer. But he and his team members have less IT Professional knowledge about how to deploy and manage web server and database with high availability and scalability requirement. They are also lack of money to setup or rent bunch of servers to support development, testing and production operation. Cloud Computing Platform which provides Platform as a Service could offer low cost entry with various kinds of resources, such as computing instance, storage, database, distributed cache, workflow, service bus and more. Based on the popular industry interoperability standards, David also could integrate their web application with the web and data services provided by other web applications on internet. Based on the architecture and capability of the Cloud Computing platform, the web application could dynamically scale out to handle the increasing workload and scale down due to the workload decreasing. David is not required to know the details of provision of the backend server and related resource. David and his team member could focus on the business implementation and deliver the web application in time. the current existing industry standards can be leveraged to serve the purpose of securing the interoperability of the services and data. Currently the implementations of

PaaS, such as programming mode, distributed storage, distributed cache, are still in initial stage. We should be open for these technology innovations.

Annex 5: Operational Requirements for Cloud Computing Services

Introduction

Cloud Computing is a paradigm shift from the traditional computing model, whereby the IT infrastructure, software and data are provided to users as on-demand network-based services. From a technical perspective, it is a natural evolution of the widespread adoption of distributed or parallel computing, utility computing, virtualization, distributed storage and load balancing technologies. On the other hand, it is also a revolution of business model in IT services consumption and delivery. Cloud Computing has received extensive attentions in the industry, thanks to its great advantages such as low-cost, fast elasticity, high resource utilization, energy conservation and high performance computing.

While Cloud Computing services are finding more applications in business, some fundamental questions still puzzle Cloud service consumers, service developers and service providers. The questions include: what kinds of IT services are Cloud Computing services? What capabilities the service providers need to have in order to guarantee service quality? In order to answer these questions, It urgently needs to lay down some principles, requirements and criteria, thereby Cloud service consumers can effectively evaluate the capabilities of Cloud Computing service providers, and service providers can meet the service consumer's expectations. This in turn will promote accountability in Cloud Computing operations, ensuring the provision of reliable and safe service to users and thus building a more healthy ecosystem in the Cloud Computing industry.

This proposal investigates the internal elements, external characteristics and type of Cloud Computing service, their inter-relationships and defines a Cloud Computing service model. This model includes four external characteristics derived from the NIST definition: *on-demand self-service*, *rapid elasticity*, *broad network access* and *measured service*. Those characteristics can be used to judge if a IT service is a Cloud Computing service. Moreover, this model also defines four basic internal elements of Cloud Computing service: people, resource, technology and process. These internal elements describe service providers' capabilities required in service delivery. We are trying to clarify those aforementioned questions through this model and provide clear guidelines for service providers to improve Cloud Computing service quality. The remainder of this proposal are organized as follows. The first three chapters describe the scope, references, terms and definitions respectively. The forth chapter depicts the Cloud Computing service model. After that, the next four chapters specify the basic requirements that the Cloud Computing service provider should meet in the four elements of people, processes, technology and resources Finally, the ninth chapter presents the safety requirements of Cloud Computing service.

Note that the word "service" mentioned in this document refers to Cloud Computing service if not explicitly qualified.

Scope

This proposal provides a common framework for Cloud Computing services, stipulating the conditions

and capabilities that the service providers should have on people, processes, technology and resources.

This document applies to:

a) establishing agreements between the service developers and the service providers;

b) capability self-assessment by the service providers;

c) selection and evaluation of service providers by the service consumers ;

d) service provider evaluation by the independent rating agencies.

Normative references

The following referenced documents are indispensable for the application of this document. For dated

references, only the edition cited applies:

NIST Cloud Definition v15
ISO/IEC 20000:2005

Terms and definitions

We here adopt the NIST definition of Cloud Computing that is listed below:

Cloud Computing is 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.

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).The consumer 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.

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer 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 application hosting environment configurations.

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

In addition, we defined the following terms used in this document:

Cloud Computing Service: A service delivered and consumed based on the Cloud Computing model defined by NIST, which is the provision of the IT capabilities of infrastructure, development environment and applications as services that can be accessed via the network.

Multi-tenancy: A technical mechanism in Cloud Computing that supports multi-tenants (i.e. customers) in the same operating environment. It ensures necessary isolation of customers' privilege resources in a shared environment. A key characteristic for multi-tenancy is that one tenant's data is effectively isolated from other tenants' authorization. Meanwhile, the operating environment sharing among tenants should not have impact on the application performance.

Cloud Computing service model

Model

Figure 1 describes the relationships of Cloud Computing service among internal elements, service type and external characteristics. With this model, we hope that service consumers can effectively evaluate the quality of the services based on the external characteristics; on the other hand, independent rating agencies can objectively assess service providers' capabilities based on the internal elements.

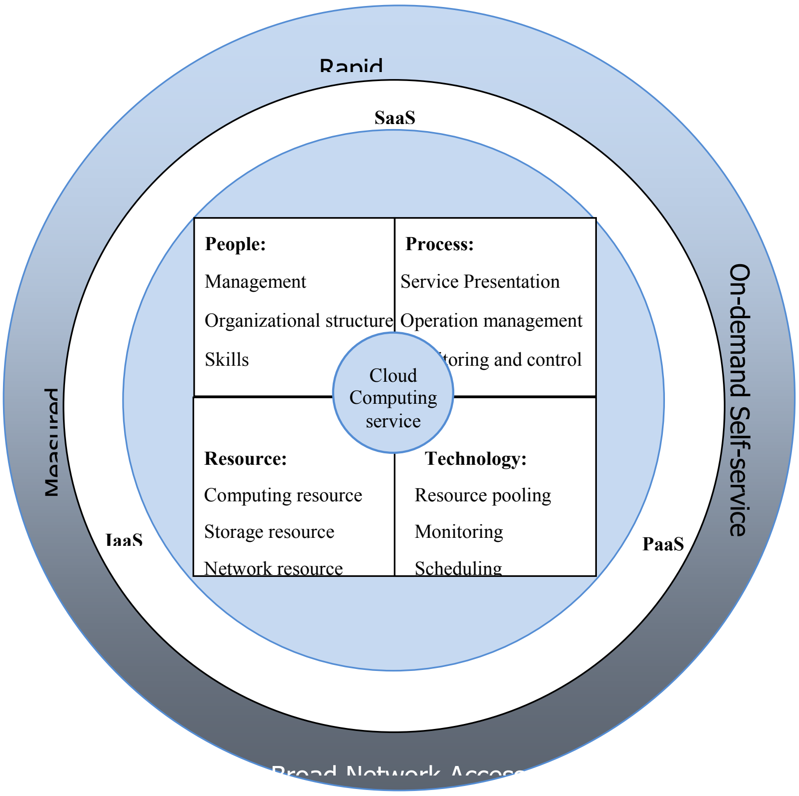

Figure 1 Cloud Computing Service Model

Internal Elements

The internal elements of service reflect the capability of service provision for Cloud service providers, mainly including four elements: people, process, resource and technology.

People: This element relates to human resource aspect of capabilities in delivering services. It includes workforce management, organizational structure and skills;

Process: The process element covers capabilities in service presentation layer, operation management layer and monitoring and control layer;

Technology: This element includes resource pooling technology, measurement technology, monitoring technology, scheduling technology and security technology;

Resource: Resource element includes computing resource, storage resource, network resource and facility resource.

Service Type

The type of service can be classified as IaaS、PaaS and SaaS. , whose level varies from bottom to top. However, each level of services can be offered by service providers independently.

External Characteristics

Here we refer the user-aware service characteristics as external characteristics, which are derived from NIST's Cloud Computing definition, i.e. *on-demand self-service*, *rapid elasticity*, *broad network access* and *measurable service*.

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's provider.

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, laptops, and PDAs).

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability1 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.

People

The people element ensures that the people involved in service design, development, test and delivery have required skills and capabilities, and the people management system follows the best practices in service management.

Management

Service provider shall fulfill the following requirements:

Management commitment

The service providers shall ensure that their people management practice comply with legal obligations, regulatory rules as well as meet customer requirements through clearly defined policies, roles and responsibilities, plus sufficient budgeted funding for service provision and operations.

Management process

Service provider shall establish management processes including recruitment, training, performance appraisal and separation. Service provider shall also effectively manage staff from business partners or suppliers who are involved in the service delivery.

Organizational structure

Service provider shall meet the following requirements on organizational structure:

a) establishing professional team to deliver service ;
b) defining roles and responsibilities in the provision of the service. Major positions include service management, technical support system operation & maintenance, etc.

Skills

Service provider shall satisfy the following requirements on staff skills:

a) Staff should possess relevant professional skills and qualifications;

b) Service provider should conduct staff skills assessment regularly. Only the staff with the right skills can be assigned to the service delivery team. Service provider should also set up a training system to ensure sufficient number of skillful resources are available to the service operation.

Processes

A *process* refers to a series of organized activities, which ensures the Cloud service delivery process and the outcome meet the stakeholders' expectations. Each process includes four parts: input, output, process control and process resources. Processes can be defined in different formats within organizations: policy, business rules, standards, guidelines, activities and commands, just to name a few.

To develop service management capabilities, service management process should be established on the following three layers respectively:

1. Service presentation layer: this layer facilitates the interactions between service provider and service customer. It helps to record the requirements provided by the consumer, as well as reporting service operation status and maintenance information to the consumer. The overarching objective of this layer is to achieve customer satisfaction.
2. Operation management layer: at this layer, service providers integrate relevant capabilities and resources to deliver high quality services to satisfy the service requirements, applying operation techniques such as planning, organizing, coordinating, orchestrating and controlling. The key activities at this process layer involve mainly resource integration, service decomposition, plus process definition, execution and optimization.
3. Monitoring & control layer: at this layer, service providers provide service assurance and support to their customers, conducting the like of service monitoring, tuning, metering, auditing and reporting activities based on administrative policies, rules and procedures.

Service Presentation Layer

Service Catalog Management

Through the management of the definition, maintenance and assessment of the service catalog, service providers should offer unified, accurate and complete service information to users. Service providers should:

a) Clearly define the roles and responsibilities in the process;

b) Specify and publish the service definitions;

c) Maintain up-to-date information in service catalog;

d) Regularly check the alignment between service capacity and service catalog;

e) Regularly assess the matching degree between service demand and service catalog;

f) Establish linkage between service catalog management and service level management.

Service Level Management

Through defining, signing and managing the service level agreements, service providers should ensure that the services meet the expectations. Service providers should:

a) Identify the demand of customers;

b) Define service items for the customers, and specify service descriptions and service quality plans;

c) Specify the service level agreements and the format of signing the related documents (electronic or hard copy);

d) Sign service level agreements and the relevant documents;

e) Establish service level monitoring and reporting mechanisms;

f) Regularly and casually verify whether the service quality meet the service level agreement, and put in plans for improvements.

Service Request Management

Through interpreting, distributing, approving and implementing of the service request, service providers should ensure that there are formal channels to receive and process the clients' service requests, complaints and evaluations, and provide feedback with the relevant information and service deliverables to the clients. Service providers should:

1. Make accurate interpretations of service requests;
2. Establish mechanisms for service request classification and distribution;
3. Setup technical and financial approval mechanisms for service requests;
4. Implement the realization process of service requests;
5. Regulate the conditions and criteria of service request refusal.

Service Report Management

Through timely, accurate and reliable reporting, service providers should establish effective communication mechanisms with their customers. Service providers should:

1. Establish management processes of service reporting, including the establishment, approval, distribution, archiving of reports, and so forth;
2. Define the users of the service reports and the main management concerns;
3. Define the content, scope, calculation and reporting templates of the service reports;
4. Define and implement the relative data collection, processing and reporting cycle of the service reports;
5. Define and implement the submitting form, user rights, and relevant assessment mechanisms of the service reports.

Operation Management Layer

The processes in operation and maintenance management layer shall satisfy the requirements of ISO/IEC 20000:2005.

Monitoring & Control layer

Monitoring and management

In order to ensure the status and information of relevant service components can be collected and displayed timely, service providers shall:

1. Define duties of monitoring;
2. Define scope and tools of monitoring;
3. Establish mechanisms for monitoring metrics and indicators design, review and routine adjustment;
4. Establish mechanisms for monitoring data test, process and analysis;
5. Establish relationship between the monitoring management and the process of the operation management layer.

Operation management

In order to ensure relevant service components can be operated according to clients' requirements and demonstrated the correct technological characteristics, service providers shall:

1. Define operation staff's duties and disciplines;
2. Produce system operation documents such as operation manuals, system logs, process charts etc;
3. Use suitable accessories, tools, software and scripts to control various manual intervention tasks on relevant service components during the execution of service (e.g. operation sequencing and execution, backup and recovery, print and output, user management, etc);
4. Establish procedures for escalation and communication in the operation management process;
5. Establish linkage between the operation management and the process of the monitoring and control management.

Technologies

Technology is the precondition for service providers to offer services. Cloud-computing technologies include resource pooling, measurement, monitoring, scheduling, security, etc. Service providers require those technologies to meet the clients' current and future business requirements. Moreover, they need to use those technologies to implement effective service management.

Resource Pooling

IaaS providers should equip with resource pooling technologies, which make the details of service infrastructure transparent to users. Resource pooling technologies enable management infrastructure in fine granularity, and provide elasticity of services. The resources managed in resource pool include computing, storage and network resources. An IaaS provider may not just offer services on single type of resources, but can also provide combos of different resources based on the underlying resource pooling technologies.

The granularity of resources, capacity of resource pool, and interfaces for resource subscribing and releasing are the primary concerns of resource pooling technologies.

Measurement

Service providers should have the following Service Measurement capabilities:

1. capable of defining corresponding measurement metrics (should at least contain Resource Service Duration, Resource Quantity, Resource Service Times, etc) according to the type of services;
2. capable of utilizing different measurement approaches according to the corresponding measurement metrics;

Measurement approaches and measurement metrics are the primary concerns of measurement technology.

Monitoring

Service providers should fulfill the following monitoring requirements:

1. ability to monitor the service, collect and integrate performance data, provide unified external access interface;
2. ability to provide representation scheme and archiving mechanism for monitored data;
3. ability to provide the visualized solution which presents the current status and history information directly to the user.

The primary concerns of monitoring technology comprises service monitoring, performance collecting tool, visualized tool and the persistence storage of performance information.

Scheduling

Service provider should fulfill the following requirements in respect of scheduling：

1. be able to adjust network bandwidth according to the current network status. When the original network resource is unavailable, it will switch to the spare network resources automatically to guarantee service continuity;

2. be able to scale up application according to the current system computing load status. When the original assigned computing resources are under stress, it will add more computing resources automatically to guarantee service quality;

3. be able to add or extend storage capacity according to the current system storage usage status. When the original assigned storage is insufficient, it will add more storage resources automatically to guarantee service continuity.

The primary concerns of scheduling is composed of computing, storage, the availability of network resources, service continuity and resource adjustment mechanisms.

Facility

Resources form the foundation for service providers' capabilities in providing services. Resources include computing, storage, network, and other service resources. At any times, the service providers must have sufficient resources to meet the business requirements of their clients, and the ability to supervise the resources in the service environment effectively.

Infrastructure

The service providers should provide infrastructure to support an effective service operation environment. In particular, it should provide the following infrastructure resources and capabilities:

a) the capability of resource metering, which is precise to compute resource usage. For example, the computing resources can be metered by the number of CPU (including virtual CPU) and the size of memory (including virtual memory);

b) the ability of planning the resources (CPU, memory, storage, network bandwidth) capacity. For instance, the service providers are able to provide simple, effective and operable mechanisms for planning the resources capacity for the large-scale resource pool, and the mechanisms can be implemented by the existing staff, tools and processes;

c) the ability of monitoring the utilized resources. This includes tools, skillful operators and processes. The thresholds and alerting rules should be defined in the monitoring process to ensure early warning is available for load conditions of CPU, memory and other resources used in the service;

d) the ability of assigning the resources (CPU, memory, storage and network bandwidth) for the clients according to their orders. This includes assigning resources, tools, skillful operators and processes, which should be integrated with the resources monitoring process;

e) the ability of providing the services that are ordered by the clients using the standard interfaces on the network. The interfaces should have built-in security capabilities such as authentication, authorization control, secure data transmission, data secrecy and privacy;

f) the ability of dynamic scaling up or down the resources (CPU, memory, storage and network bandwidth). When the customers' business applications need more resources, it can add more resources for clients dynamically; when the customers' business applications have unutilized resources , it can take back those resources dynamically;

g) the ability of measure resource usage (CPU, memory, storage and network bandwidth). It should be able to accurately measure the resources used by a client in proper meter unit, for instance, the number of CPU used by a client;

h) the ability of resolving the failure of resources (CPU, memory, storage and network bandwidth). This includes three aspects: skillful people, process and tools. The tooling aspect includes the problem diagnosis tools, troubleshooting tools and problem defuse tools. The problem resolution process should be integrated with the resource monitoring process.

The metering model, the accounting of services execution and improving mechanism are the primary concerns of evaluating the infrastructure resources.

Supporting Environment

Service providers should have the ability to manage the supporting environment of Cloud efficiently, and should meet requirements in aspects such as:

1. Security

   This part should satisfy the constraints of physical security part in 9.1

2. Availability

   Taking into account the availability of the data center, computer room should equip with redundant power supply units and cooling facilities. In addition, it is recommended to have multiple backup data centers in multi-region to ensure availability.

3. Service Continuity

   Build disaster recovery center for Cloud Computing data center, regularly backup data to ensure service continuity;

   In the case of multiple data centers, mutual backup mechanisms can be designed so each data center can act as a backup data center for others.

4. Energy efficiency

   Service providers should employ data center energy management mechanisms to monitor data center facilities and the use of energy.

   Service providers should take measure to ensure energy-saving and cost-reducing on the aspects of room decoration, air distribution, power supply and distribution, air conditioning, cooling and lighting.

   Service providers should use renewable energy, energy saving technologies such as natural cooling where possible in data center operations.

The number of power and cooling equipments and capacity, the number of backup data centers and their distance, the measurement of green power-saving or third-party rating of energy efficiency, and improvement mechanism are the primary concerns of service supporting environment.

Security

Physical security

Service provider should fulfill the following physical security requirement:

1. The data center design and construction should comply with the relevant requirements of the security design of the computer room standards;
2. It is necessary to manage the division area of data center, physical isolation facilities should be set up;
3. Real time monitoring system should be equipped with environment and safeguard facilities of data center, staff on 24 hour duty should be arranged;
4. Management and control measures should be adopted for the management procedures, persons passing through safeguard facilities, and persons working or visiting data centers;
5. Service providers should establish maintenance, management and operating procedures for safeguarding facilities and infrastructure in their data center operations. The procedures must be strictly enforced.

Data center real-time monitoring system for environment and facilities, security and infrastructure maintenance, management and operating procedures, personnel management, the compliance of various regulations are primary concerns of measuring physical security.

Network security

Service provider should satisfy the following network security requirements：

1. Ensuring the information transmission security, implementing mechanisms to ensure the data confidentiality and integrity;
2. Provide network access control capabilities including authentication, authorization and auditing functions;
3. Ensure reliability and availability on connections across the network;
4. Have the ability to prevent malicious network attacks;
5. Can minimize the impact on network availability caused by network configuration errors.

Data transmission encryption and security mechanisms, defense against different types of network attacks, access authentication, authorization and auditing mechanisms are primary concerns of network security.

Server security

Service provider should satisfy the following server security requirements：

1. ensuring hardware and OS security of all hosts in the service environment;
2. ensuring the security of hypervisor, virtual machine and virtual machine OS when virtualization technology is used in the service environment;
3. providing default security configurations for the automatic supplied virtual machines;
4. cooperating the virtual machine automatic assignment process with host security management procedures to ensure the security of virtual machine;

Operating system privileges security, security isolation of virtual machines from host, security of passwords and permissions of virtualization management system are primary concerns of server security.

Application security

Service provider should meet the following application requirements：

1. It should follow the development standards of application software and Internet application software and ensure the applications provided to the users are secure.
2. It should have the ability to test application security. It should be able to prevent the known network attacks when the applications have passed the test.
3. It should have the ability to encapsulate the software of service. The stable software will provide the standard application program interface (short for API) to the user as the service interface standard. Then users can consume service through API from the network.
4. It should provide capabilities in administering and controlling the users in the service environment. In addition, it should be able to identify the logged-on users for verify their legitimacy and certification.
5. It should provide the unified account management, identity management, authorization management, audit management, single sign-on functions in the service environment.

The primary concerns of application security are grading access control, network attack detection and prevention for application user identification mechanism and centralized user management.

Data security

Service provider should satisfy the following requirements：

1. It should have the ability to encrypt data that can ensure the privacy of the confidential data in the service environment.
2. It should have the ability to store data reliably and ensure availability and integrity.
3. it should have a data backup and recovery plan. In addition, there should be at least one valid copy or backup of the data which are stored in a place complied with the provisions in the contract, service level agreements and regulations.
4. it should protect the user's data when processing data. Moreover, it should ensure the security of each individual user's data in a multi-tenancy environment.
5. it should have the ability reading and writing to ensure the data availability and integrity when processing the data.
6. the data should be monitored and have the proper security access control.

The primary concerns in measuring data security include data backup and recovery mechanisms, data isolation mechanisms between the tenants and data access logging mechanisms.

References

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia. “Above the Clouds: A Berkeley View of Cloud Computing”. Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA, Feb. 10, 2009.
2. Michael Armbrust, Armando Fox, Rean Griffith, et al, “A view of Cloud Computing”, Communications of the ACM, pp50 – 58, Apr. 2010.
3. Feng Liu, Li Li, and Wu Chou, “Communications Enablement of Software-as-a-Service (SaaS) Applications”, on Global Telecommunications Conference, 2009 (GLOBECOM 2009), pp1-8.
4. Viega, J. , “Cloud Computing and the Common Man”, IEEE Computer Society, pp106-108, Aug. 2009.
5. Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, INFOCOM, 2010, pp1-9
6. ITU Telecommunication Standardization Sector Focus Group on Cloud Computing, http://www.itu.int/ITU-T/focusgroups/cloud/tor.html
7. Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing
8. Amazon. Amazon elastic compute cloud (Amazon EC2). 2009. http://aws.amazon.com/ec2/
9. GARFINKEL, S. “An Evaluation of Amazon’s Grid Computing Services: EC2, S3 and SQS” . Tech. Rep. TR-08-07, Harvard University, August 2007.
10. D. Chappell. “Introducing the Azure services platform”.White paper, Oct. 2008.
11. IBM Cloud Computing White Paper. http://www.ibm.com/developerworks/websphere/zones/hipods/library.html
12. Sims K. “IBM introduces ready-to-use Cloud Computing collaboration services get clients started with Cloud Computing”. 2007.http://www-03.ibm.com/press/us/en/pressrelease/22613.wss
13. Boss G, Malladi P, Quan D, Legregni L, Hall H. “Cloud Computing”. IBM White Paper, 2007. http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf
14. Barroso LA, Dean J, Hölzle U. “Web search for a planet: The Google cluster architecture”. IEEE Micro, 2003,23(2):22−28.
15. VOGELS, W. “A Head in the Clouds—The Power of Infrastructure as a Service”. In First workshop on Cloud Computing and in Applications (CCA ’08) (October 2008).
16. CHENG, D. “PaaS-onomics: A CIO’s Guide to using Platform-as-a-Service to Lower Costs of Application Initiatives While Improving the Business Value of IT”. Tech. rep., LongJump, 2008.
17. T. Kwok, T. Nguyen, and L. Lam, “A software as a service with multi-tenancy support for an electronic contract management application,” in Proceedings of the International Conference on Services Computing (SCC). IEEE Computer Society, 2008, pp. 179–186.
18. PARKHILL, D. “The Challenge of the Computer Utility.” Addison-Wesley Educational Publishers Inc., US, 1966.
19. Foster and C. Kesselman (editors). “The Grid: Blueprint for a New Computing Infrastructure”. Morgan Kaufmann, 1999.
20. NURMI, D., WOLSKI, R., GRZEGORCZYK, C., OBERTELLI, G., SOMAN, S., YOUSEFF, L., AND ZAGORODNOV, D. “Eucalyptus: A Technical Report on an Elastic Utility Computing Archietcture Linking Your Programs to Useful Systems” .Tech. Rep. 2008-10, University of California, Santa Barbara, October 2008.
21. B. Rochwerger, A. Galis, E. Levy, J. A. Cáceres, et al, “RESERVOIR: Management Technologies and Requirements for Next Generation Service Oriented Infrastructures”, 2009 IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), pp307-310.
22. MCKEOWN, N., ANDERSON, T., BALAKRISHNAN, H., PARULKAR, G., PETERSON, L., REXFORD, J., SHENKER, S., AND TURNER, J. “OpenFlow: Enabling innovation in campus networks”. ACM SIGCOMM Computer Communication Review 38, 2 (April 2008).
23. Cloudera, Hadoop training and support [online]. Available from: http://www.cloudera.com/.
24. BIALECKI, A., CAFARELLA, M., CUTTING, D., AND O’MALLEY, O. “Hadoop: a framework for running applications on large clusters built of commodity hardware”. Wiki at http://lucene. apache. org/hadoop.

25. Isard M, Budiu M, Yu Y, Birrell A, Fetterly D. “Dryad: Distributed data-parallel programs from sequential building blocks”. In: Proc. of the 2nd European Conf. on Computer Systems (EuroSys).,2007. 59−72.

26. Ghemawat S, Gobioff H, Leung ST. “The Google file system”. In: Proc. of the 19th ACM Symp. on Operating Systems Principles.New York: ACM Press, 2003. 29−43.

27. X. H. Li, T. Liu, Y. Li, and Y. Chen, “Spin: Service performance isolation infrastructure in multi-tenancy environment,” in Proceedings of the 6th International Conference on Service-Oriented Computing (ICSOC), ser.LNCS, vol. 5364. Springer, 2008, pp. 649–663.

28. Chang-Hao Tsai, Yaoping Ruan, Sambit Sahu, Anees Shaikh, and Kang G. Shin. “Virtualization-based techniques for enabling multi-tenant management tools”. In 18th IFIP/IEEE Int. Workshop on Distr. Systems: Operations and Management (DSOM), volume 4785 of LNCS, pages 171–182. Springer, 2007.

29. Aguilera MK, Merchant A, Shah M, Veitch A, Karamanolis C. “Sinfonia: A new paradigm for building scalable distributed systems”. In: Proc. of the 21st ACM Symp. on Operating Systems Principles. New York: ACM Press, 2007. 159−174.

30. Dean J, Ghemawat S. “MapReduce: Simplified data processing on large clusters”. In: Proc. of the 6th Symp. on Operating System Design and Implementation. Berkeley: USENIX Association, 2004. 137−150.

31. Burrows M. “The chubby lock service for loosely-coupled distributed systems”. In: Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2006. 335−350.

32. Chang F, Dean J, Ghemawat S, Hsieh WC, Wallach DA, Burrows M, Chandra T, Fikes A, Gruber RE. “Bigtable: A distributed storage system for structured data”. In: Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2006. 205−218.

33. Barham P, Dragovic B, Fraser K, Hand S, Harris T, Ho A, Neugebaur R, Pratt I, Warfield A. “Xen and the art of virtualization”. In: Proc. of the 9th ACM Symp. on Operating Systems Principles. New York: Bolton Landing, 2003. 164−177.

34. IBM. “IBM virtualization”. 2009. http://www.ibm.com/virtualization

35. Nelson M, Lim BH, Hutchins G. “Fast transparent migration for virtual machines”. In: Proc. of the USENIX 2005 Annual Technical Conf. Berkeley: USENIX Association, 2005. 391−394.

Annex 6: Cloud Computing Use Cases and Scenarios

Typical Scenarios and Analysis of Cloud Computing

There has long been envisioned for Information Technology service providers to provide computing capabilities for their customers/users in a utility manner similar to t water, electricity, gas etc. Cloud Computing is widely believed to be able to make this vision into reality. Many individuals, enterprises and service providers are all beginning to test water with Cloud Computing. However, the ubiquity and convenience of Cloud Computing also comes with its own share of issues. We illustrate here a few sample scenarios to explain the necessity and challenge of Cloud Computing related standards.

Scenario 1: for an individual user

Although fairly new to Cloud Computing~~-~~, Mary decides to store most of her personal data, such as mails, photos, diaries, etc., in the Cloud, because it is easier to share them with her friends this way, and she can access her own them anywhere. In this scenario, she need not worry about data loss due to viruses and hardware failures at home or office, because the SLA she has with the service provider clearly states the availability and data backup plan. However, should she feel the need to switch to another service provider, or should her current service provider go out of business, it will be very difficult to transfer the data to another service provider. At the same time, she is reading so many media discussions on privacy horror stories that she begins to wonder whether it’s wise to place some private files in “somebody else’s place”, because her SLA with the service provider does not say anything about it.

Some similar scenarios from standards development organizations working on Cloud Computing, including:

1. Cloud Computing Use Cases White Paper. URL: http://cloudusecases.org/
2. Strengthening your Business Case for Using Cloud: Cloud Business Use-Case Analysis. URL http://www.opengroup.org/cloud/whitepapers/wp_cbuc/cbuc-analysis.htm
3. Reaching for the Cloud(s): Privacy Issues related to Cloud Computing. URL: http://www.priv.gc.ca/information/pub/cc_201003_e.cfm
4. The future of Cloud Computing: Opportunities for European. Expert Group Report, European Commission, 2010. URL: cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Formatted: Tab stops: Not at 18 pt

These scenarios indicate that the Cloud Computing still challenged the following problems. Vendor lock-in, privacy and SLA. With privacy problem, it is vital that a Cloud provider deliver the added controls needed to protect sensitive data, including the ability for the user to audit the Cloud provider to prove that if followed the appropriate procedures. Availability is a clear requirement for any system. Where it is in the Cloud or in the data centre down the hall. Business continuity and disaster recovery are also part of availability. All the things need to be considered by the end user of the Cloud Computing.

Scenario 2: for a small-medium enterprise

Tom has just started his own eCommerce business, but he does not have the budget or skills to build or maintain his own IT infrastructure. Fortunately, an IT service provider ClearSky is able to provide him a suite of applications from the internet with a flat monthly fee as a starter: e-mail, customer relationship management, sales analytics, data analytics and so on. Tom is happy with the functionality of the suite, and the price tag. He is every more happy with the fact that he can focus on his own business competency, i.e. managing online sales and promotion. However, the service can be unavailable occasionally. Some of such incidences last week resulted in business interruption and loss of sales, . Besides, interoperability among service providers is also becoming a big concern now. For example, Tom loves the data analytics from RainShelter his friend Jerry has been showing him, but he could not find a way to pipe his CRM data and sales number from ClearSky to RainShelter. Tom is worried if he has to hire someone to do the job, and its future maintenance cost.

Some similar scenarios from standards development organizations working on Cloud Computing, including:

5. Cloud Computing Use Cases White Paper. URL: http://cloudusecases.org/
6. The future of Cloud Computing: Opportunities for European. Expert Group Report, European Commission, 2010. URL: cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Formatted: Tab stops: Not at 18 pt

These scenarios indicate that the Cloud Computing still challenged by lack of service related standards and specifications. How to define function, data format, QoS and interface of services, different service providers give different answers, which results in difficulty in service selection, service immigration, and service integration. Standards should be developed to allow users to choose a proper service provider which can guarantee the QoS requirements of their business, and to allow users to establish connectivity between Cloud A and Cloud B systems through integration appliances.

Scenario 3: for a large enterprise

JumboJoe is a globally well recognized industry leader. In order to maintain its leadership, it speeds huge amount of money to maintain its IT infrastructure. However, a recent audit finds that most of these money are spent on maintenance, with less than 10% for new initiatives. Furthermore, 50% of the machines seat idle 80% of the time; machines in use have only 30% CPU utilization on average. JumboJoe also maintains a set of very expensive software licenses which they uses only a couple of times a year. In an extreme case, JumpboJoe has be maintaining a software license that they have not touched for 5 years. JumboJoe would love to be able to purchasing servers and storage as demand increases and pay a usage fee for those occasionally used software. They figure they can save up to 50% of the equipment budget. And further saving can be archived because they can reduce the size of their data centres, and well as they maintenance staff. However, JumboJoe is concerned with a number of technicality issues, such as: (a) there only a very limited number range of parameters they can specify for the servers they would buy, and if the servers are delivered as specified. (b) current SLA and security assurance from the service provider might not meet JumboJoe's corporate instruction on IT infrastructure, particularly the company's data security policies might not allow mission critical data be to stored on a server outside the company premise; and (c) JumboJoe is confused which service provider to choose because there are so many of them. JumboJoe does not have a framework to compare their quality of service, the range of products, the relative ranking of performance, and most of all the peace of mind that the rating from a trusted authority.

There are many public uses cases from different SDO and vendors. For example the white paper from opencloudmnifesto.org (http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf) listed several scenarios related to enterprises usage of Cloud Computing.

The second and third problems listed for large enterprise scenario are related to standardization and interoperability, security and privacy, which need to be clearly stated and emphasized.

Scenario 4: Individual Developer and Start-up Software Company

David was an individual developer and would like found a start-up company to build web application to provide innovation service to consumer. But he and his team members have less IT Professional knowledge about how to deploy and manage web server and database with high availability and scalability requirement. They are also lack of money to setup or rent bunch of servers to support development, testing and production operation. Cloud Computing Platform which provides Platform as a Service could offer low cost entry with various kinds of resources, such as computing instance, storage, database, distributed cache, workflow, service bus and more. Based on the popular industry interoperability standards, David also could integrate their web application with the web and data services provided by other web applications on internet. Based on the architecture and capability of the Cloud Computing platform, the web application could dynamically scale out to handle the increasing workload and scale down due to the workload decreasing. David is not required to know the details of provision of the backend server and related resource. David and his team member could focus on the business implementation and deliver the web application in time.

the current existing industry standards can be leveraged to serve the purpose of securing the interoperability of the services and data. Currently the implementations of PaaS, such as programming mode, distributed storage, distributed cache, are still in initial stage. We should be open for these technology innovations.

Outstanding Issues

Editors Note: (N188/GB003) Business perspective. Although section 1 (Scope) states that the document reviews 'business perspectives on Cloud Computing', there is actual little coverage of this area, and the predominant focus of the document is on technical standards. Arguably, Cloud Computing is primarily a business phenomenon rather than a technological one, as almost all of the technologies and related issues have existed for a considerable time; and it is only the business drivers which have focused so much attention now on the failure satisfactorily to address the technological and security-type issues which have existed. This perspective is lacking from the current document.

The business perspective should be thoroughly integrated into the report, both in structure and in content, and not be relegated to being an area of passing observations (e.g. as an appendix as in the current draft) in a document otherwise dedicated largely to technical issues.

Consider the following:

- Providing a top-down business

perspective from the first paragraph of the report. Incorporate wording similar to that given in the comment column to the left.

- Restructuring the report, both for

overview purposes (section 5) and analysis purposes (section 6) into clearly separate sections such as:

o Business drivers and

requirements

o Legal and regulatory

requirements

o Security requirements

o Interoperability requirements

o Specific technology

requirements

- Adding relevant business requirements to

the list of criteria currently being used. The two specific categories suggested to be added to section 6.9 are for management standards, and for disclosure.

- Adding coverage to the report of related standards which have more management orientation, such as ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, ISO/IEC 19770-1, ISO 31000, etc.