ETSI SR 003 392 V2.1.1 (2016-02)

Cloud Standards Coordination Phase 2;
Cloud Computing Standards Maturity Assessment;
A new snapshot of Cloud Computing Standards

Reference
DSR/NTECH-00033

Keywords
Cloud computing, maturity assessment

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

List of figures

List of tables

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Network Technologies (NTECH).

The present document is approved by the NTECH Technical Committee and for publication of the Cloud Standards Coordination website (http://csc.etsi.org).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Cloud Computing is increasingly used as the platform for ICT infrastructure provisioning, application/systems development and end user support of a wide range of core services and applications for businesses and organizations.

Cloud Computing is drastically changing the way ICT is delivered and used. However, many challenges remain to be tackled. Concerns such as security, vendor lock-in, interoperability and accessibility, service level agreements more oriented towards users are examples of issues that need to be addressed.

In February 2015, the Cloud Standards Coordination (CSC) Phase 2 (CSC-2) was launched by ETSI to address issues left open after the Cloud Standards Coordination Phase 1 (CSC-1) work was completed at the end of 2013, with a particular focus on the point of view of the Cloud Computing users (e.g. SMEs, Administrations).

The present document describes the results of the second Cloud Computing Standards Maturity Assessment held by CSC-2, roughly two years after the first one.

1 Scope

The present document describes the results of the second assessment of Cloud Computing Standards maturity held by CSC-2, roughly two years after the first one.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Cloud Standards Coordination, Final Report, November 2013.

NOTE: See: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF.

[i.2] ETSI SR 003 381 (10-2015): "Cloud Standards Coordination Phase 2; Identification of Cloud user needs".

[i.3] ETSI SR 003 382 (10-2015): "Cloud Standards Coordination Phase 2; Cloud Computing Standards and Open Source; Optimizing the relationship between standards and Open Source in Cloud Computing".

[i.4] ETSI SR 003 391 (10-2015): "Cloud Standards Coordination Phase 2; Interoperability and Security".

[i.5] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.

NOTE: See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025.

[i.6] Communication from the Commission to the European Parliament, the Council, The european Economic and Social Committee and the Committee of the Regions: "Unleashing the Potential of Cloud Computing in Europe".

NOTE: Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

[i.7] ISO/IEC 17789: "Information technology -- Cloud computing -- Reference architecture".

[i.8] Recommendation ITU-T Y.3502: "Information technology - Cloud computing - Reference architecture".

[i.9] ISO/IEC CD 19944: "Information Technology - Cloud computing -- Data and their Flow across Devices and Cloud Services".

[i.10] ISO/IEC 17788: "Information Technology - Cloud computing --Overview and vocabulary".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

specifications: output from an SSO (see [i.5]) that may become a standard when ratified by an SDO

standards: output from an SDO (see [i.5])

Standards Development Organization (SDO): organization that develops standards that has a formal recognition by international treaties, regulation, etc.

NOTE 1: In the list of SSOs presented in Annex A, the SDOs are: ETSI, IEC, ISO, ITU, ITU-T.

NOTE 2: The SDOs are a subset of the SSOs.

Standards Setting Organization (SSO): any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining specifications and standards that address the interests of a wide base of users outside the standards development organization

NOTE: As an example, the organizations listed in Annex A are SSOs.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
3GPP	Third Generation Partnership Project
CADF	Cloud Auditing Data Federation
CAMP	Cloud Application Management for Platforms
CC	Cloud Computing
CCM	Cloud Control Matrix
CCSL	Cloud Certification Schemes List
CDMI	Cloud Data Management Interface
CDN	Content Delivery Network
CIMI	Cloud Infrastructure Management Interface
CSA	Cloud Security Alliance
CSC	Cloud Service Customer
CSC-1	Cloud Standards Coordination Phase 1
CSC-2	Cloud Standards Coordination Phase 2
C-SIG	Cloud Selected Industry Group
CSP	Cloud Service Provider
CTP	Cloud Trust Protocol
DMTF	Distributed Management Task Force
DSCI	Data Security Council of India
EC	European Commission

ENISA	European Union Agency for Network and Information Security
EU	European Union
HLUC	High- Level Use Cases
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LI	Lawful Intercept
MEF	Metro Ethernet Forum
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NIST	National Institute of Science and Technology
OASIS	Advancing Open Standards for the Information Society
OCCI	Open Cloud Computing Interface
OCF	Open Certification Framework
ODCA	Open Data Center Alliance
ODP	Open Data Protocol
OGF	Open Grid Forum
OSS	Open Source Software
OVF	Open Virtualization Format
PaaS	Platform as a Service
PAS	Publicly Available Specification
PII	Personal Identifiable Information
PLA	Privacy Level Agreement
SaaS	Software as a Service
SDN	Software Defined Networks
SDO	Standards Development Organization
SIIF	Standard for Intercloud Interoperability and Federation
SLA	Service Level Agreement
SME	Small or Medium Enterprise
SNIA	Storage Networking Industry Association
SSO	Standards Setting Organization
STF	Specialist Task Force

NOTE: An ETSI structure for internal projects.

TCI	Trusted Cloud Initiative
TIE	Trusted Information Exchange
TMF	TeleManagement Forum
TOSCA	Topology and Orchestration Specification for Cloud Applications
UC	Use Cases
VM	Virtual Machine
VNF	Virtual Network Function

4 Cloud Computing Standards Maturity Assessment

4.1 Context

The Cloud Standards Coordination project (CSC)

Cloud Standards Coordination Phase 1 took place in 2013 as a community effort supported by ETSI and primarily addressed the Cloud Computing standards roadmap. In December 2013 the results were publicly presented in a workshop organized by the European Commission (EC).

The CSC Final Report [i.1] provides a "snapshot" on the Cloud Computing standardization landscape at the end of 2013. It is available at: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF.

Cloud Standards Coordination Phase 2

Given the dynamics of the Cloud Computing market and standardization, Cloud Standards Coordination Phase 2 (CSC-2) was launched in February 2015 with, in particular, the main objective of producing an updated version of the Maturity Assessment of the Cloud Computing standardization landscape. CSC-2 aimed at better taking into account the needs of Cloud Computing customers on their Cloud related requirements and priorities. This has allowed CSC-2 to further assess the maturity of Cloud Computing standards and to evaluate how standards can support the Cloud Computing customers' priorities.

Cloud Computing Standards Maturity

At the time of CSC-1, the European Commission Communication on the European Cloud strategy (COM(2012) 529: "Unleashing the Potential of Cloud Computing in Europe" [i.7], September 2012, pp. 10-11) identified a key action for standardization in the context of promoting the uptake of cloud computing technologies:

- Key action 1: Cutting through the jungle of standards [...]:
  - Promote trusted and reliable cloud offerings by tasking ETSI to coordinate with stakeholders in a transparent and open way to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility).
  - Enhance trust in cloud computing services by recognizing at EU-level technical specifications in the field of information and communication technologies for the protection of personal information in accordance with the new Regulation on European Standardization.

To answer the request from the European Commission, ETSI launched the Cloud Standards Coordination (CSC-1). Its overall objective was to present a report [i.1] which is useful for its target audience and which effectively supports the European Commission's work on implementing its Cloud strategy and therefore the broad uptake of standards-based cloud computing technologies in Europe - driving innovation and growth with the Cloud.

The present document describes the results of the second assessment of Cloud Computing Standards maturity held by CSC-2, roughly two years after the first one. In contrast to CSC-1, which was more oriented towards the provider side of Cloud Computing, CSC-2 has a particular focus on the point of view of the Cloud Computing users (e.g. SMEs and Administrations).

4.2 Objectives

The main objectives are to:

- Provide an updated list of identified Cloud Computing standards (and an updated list of the organizations that develop them).
- Analyse the progress of coverage of the Cloud Service life-cycle (as done in phase 1).
- Analyse the main customers' and users' concerns and how standards help their resolution.
- Identify areas of maturation and areas where standards have to progress in the future.
- Provide conclusions based on the analysis.

4.3 Approach

The analysis of Cloud Computing standards has addressed those that have been identified during CSC-1 and those who have emerged since then, i.e. between the end of 2013 and the time of writing the present document.

Unlike for CSC-1, Certification has been addressed. Some relevant certification schemes have been analysed with the same approach as for the Cloud Computing standards.

Some general-purpose standards may be useful in the context of Cloud Computing, but the analysis will not address them in details (though in some cases, some of them may be mentioned). Setting up a list of commonly used general-purpose standards in Cloud Computing could be part of future work.

The same applies to other issues that relate to standards, such as legislation or regulation that will be addressed on a case-to-case basis.

4.4 Target audience

The audience for the present document on Cloud Computing Standards Maturity Assessment includes:

- Cloud service customers, who should be able, from knowing the standards and specifications applied by a cloud service provider, to understand how their requirements can be covered by the current and future offerings and to have confidence in the service offering.
- All sizes of cloud service providers and cloud service customers from small businesses to public procurers and multinationals.
- Administrations that have to act as cloud service customer.
- Governmental authorities that have to act as cloud regulators.
- Cloud service providers who should be able to use it to understand which standards and specifications they may wish to select and apply to their services in order to better satisfy their customers' needs.

4.5 Content of the present document

Clause 5 of the present document recalls how actors, roles and Use cases have been defined in Cloud Standards Coordination phase 1. This is meant to make the present document as self-contained as possible, as the CSC-1 one was.

Clause 6 of the present document is analysing the recent evolution of the Cloud Computing standardization landscape. Some of the results of the CSC-2 user survey regarding standards are recalled. A list of relevant Cloud Computing SSOs is provided (together with a list of associated standards in Annex A). A mapping of these standards on the Cloud Computing Service life-cycle is done, as it was in CSC-1, and the major conclusions are drawn (support material can be found in Annex B). In particular, the standards gaps are clearly noted, together with an evaluation of their importance.

Clause 7 is presenting customers' and users' concerns regarding Cloud Computing (drawn from the results of the CSC-2 user survey [i.3]) that are compared to those identified in CSC-1 and analysed in order to outline how they can be addressed by standards.

Clause 8 highlights preliminary conclusions and recommendations from the analysis done in the present document.

Clause 9 suggests some areas for further study.

Annex A is presenting the list of SSOs that have been considered as relevant to Cloud Computing standardization. For each of these organizations, a table of the related Standards and Specifications (that they have published or were developing at the time) is added.

Annex B is presenting the Cloud Computing Service life-cycle in three phases (Acquisition, Operation, Termination) and the activities that are undertaken by the Cloud Service Customer or the cloud Service Provider in each of these phases. These activities are used for the mapping of the Cloud Computing Standards in clause 5.

5 Actors, Roles and Use Cases

5.1 Introduction

This clause introduces briefly the definition of actors, roles and use-cases of CSC-1. This definition has been re-used in CSC-2, in particular in order to maintain comparability between the two reports.

5.2 Roles

The objective is to provide a high level taxonomy of stakeholders, individuals and/or organizations that play a role in the provision and/or consumption of cloud services.

Input was collected from, in particular, the following organizations: DMTF, ITU-T and NIST. Two main elements have been addressed: roles and parties.

Role: The following roles have been defined:

- Cloud Service Customer: The Cloud Service Customer role consists of those consuming one or more cloud services provided by a Cloud Service Provider.
- Cloud Service Provider: The Cloud Service Provider role consists of those providing cloud services to one or more Cloud Service Customers.
- Cloud Service Partner: The Cloud Service Partner role consists of those providing support to the provisioning of cloud services by the Cloud Service Provider, or to the consumption of cloud service by the Cloud Service Customer (e.g. service integration).
- Government authority: The government authority role consists of those interacting with providers, customers and partners for the purpose of regulation, law enforcement, inspection, economic stimulation, etc.

Roles can be refined into sub-roles.

Party: An individual or an organization. Parties can play one or more roles.

Note that one party can play several roles at the same time. Consider for example an SME that deploys a specific piece of software on a PaaS cloud service, offering the Software as a Service to other SMEs. In this case, the SME plays both the roles of Cloud Service Customer, as well as Cloud Service Provider. Consider as a second example a government agency that could play the role of provider (offering a governmental cloud appstore, for instance) or play the role of customer (consuming an email as a service solution, for example). Each party may have either or both of the responsibilities of data processor or data controller depending on use case.

The relations between the roles (and parties) are depicted in figure 1.

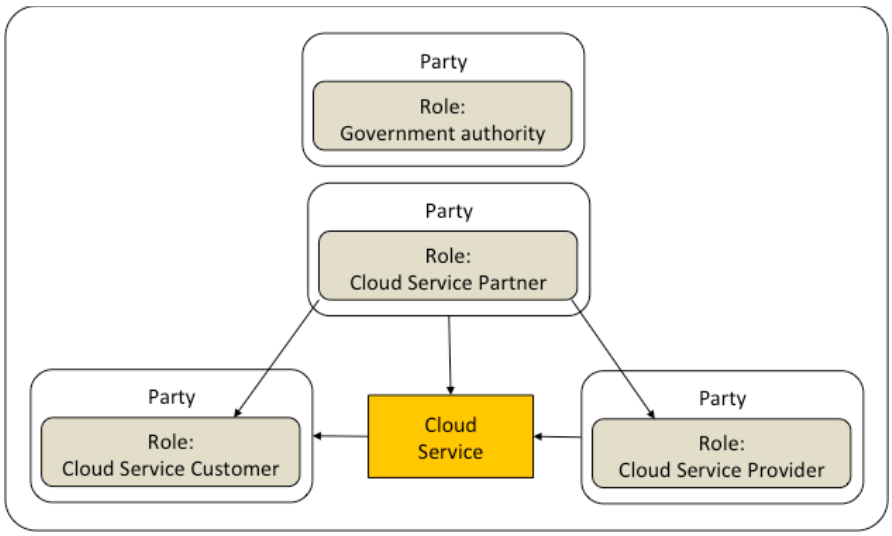

Figure 1: Roles and parties in Cloud Computing

5.3 Use Cases

Use Cases (UC) have been collected in CSC-1 through an open call from organizations that have been contributing to CSC-1.The collection phase has led to the identification of 110 Use Cases that have then been:

- categorized according to criteria that could help in the following phases of the activity, i.e. Data Security and Privacy, Service Level Agreements, Interoperability, Data Portability, Reversibility, Support EU Policies, Based on Real life situations; and
- ranked on a four level scale indicating their relevance (not a UC, broad UC, UC, detailed UC).

By filtering out the collected UCs ranked "not a UC", the total number of UCs was reduced to 90.

Given the large number and the lack of homogeneity of the Use Cases, it has been agreed to provide a high level view of UCs over which to map all the submitted ones, in order to provide a clearer representation for Cloud Services Use Cases. This is achieved with the definition of High- Level Use Cases (HLUC):

- Set-Up Cloud Service;
- Prepare & Procure service;
- Operate the service;
- Use Service; and
- Assure Quality.

These HLUCs (and a refinement for some of them) are represented in figure 2.

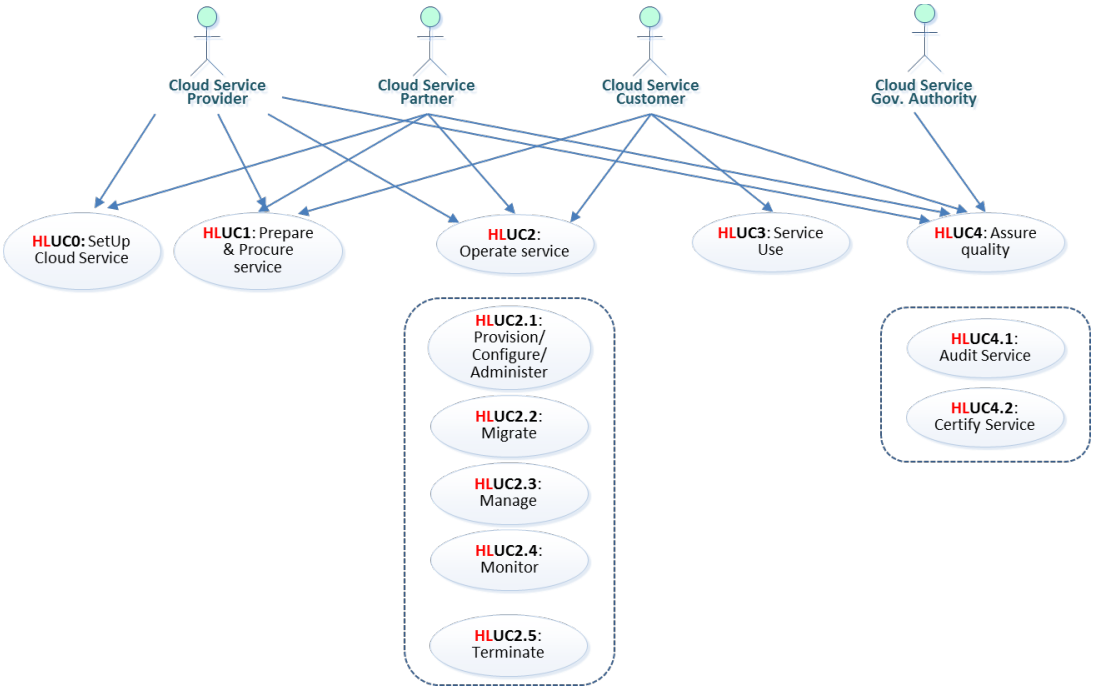

Figure 2: High Level Use Cases

In parallel, the Use Cases were grouped by family and for each of the families, a "master" UC was identified. With this, it was possible to filter the list of (90) UCs down to 21 very representative UCs that could be mapped with the HLUCs.

6 Evolution of the Cloud Computing standards and specifications landscape

6.1 Introduction

This clause is based on the results of the CSC-2 user survey (see [i.2]).

The clause first provides a list of organizations active in the field of Cloud Computing standardization, specifications and certification.

It also presents the Cloud Service life-cycle (a concept that was introduced by CSC-1) and a comprehensive mapping of the existing standards onto the Cloud Computing life-cycle.

6.2 Customers and Users view on Cloud Computing Standards, Specifications and Certification

6.2.0 Introduction

The CSC-2 User survey came with two major observations:

- standards are seen as able to positively address the Cloud customer and Cloud user concerns; and
- there is insufficient knowledge of existing standards and specifications on the side of Cloud customers and Cloud users.

Based on the responses received by mid June 2015, a first tentative and high-level analysis has been made. The most significant trends are presented below.

NOTE: In the remainder of the present document, the term "User " refers to both "User" and "Customer".

6.2.1 Moving to the Cloud

There is a high perception among the respondents that the transition to Cloud Computing should be carefully planned and organized, in particular in areas pertinent to data (classification, storage, etc.), processes and security. More detailed information can be found in the CSC-2 User Survey report (see [i.2]).

6.2.2 Standards and specifications

In general, the role of standards and specifications is seen as important and there is a growing level of awareness. 38 % of the respondents indicate that standards and specifications are used while 27 % indicate that they are considered. This shows a promising insight into the value and importance of standards and specifications. However, in terms of knowledge on the existing set of Cloud standards and specifications the insight is quite limited.

However, the CSC survey clearly indicates that the awareness and use of Cloud Computing standards and specifications is still low among existing and potential users of Cloud Computing.

One conclusion and recommendation made in the CSC- 2 User survey is that more education on the benefits that come from using Cloud Computing standards and specifications should be made. Further work on aligning standards and specifications and increased collaboration between Standards Development/Setting Organizations (SDOs/SSOs) should also be encouraged.

6.2.3 Main areas of concern

Unsurprisingly, the more distinct findings mainly deal with two areas: security and interoperability.

Security, Integrity and Data Privacy: These topics are seen as major concerns. This is not a new finding, but the fact that the concern is still very much present is a clear indication on the perceived challenge ahead for security standards, specifications and Cloud certification in particular.

Interoperability and Portability: These areas are ranked high: concerns are most likely linked to the issue of vendor lock-in, e.g. because of non-interoperable APIs, the unclear capabilities of individual cloud service offerings ability to move data or applications from one service to another and the lack of standards or specifications in support of portability for cross-Cloud scenarios in general.

The WP3 report ETSI SR 003 391 [i.4] addresses these areas in detail.

6.2.4 Certification

Finally, a very large majority (79 %) of the respondents confirms the role of certification as a very useful way to improve confidence in Cloud Computing. Amongst the cross cutting aspects for which certification is seen as most critical, data security and data privacy are regarded as the most significant areas for certification among the respondents. Cloud Service certification (per cloud service, covering all partners and providers in the end-to-end chain) and Cloud Provider certification are considered as the preferred types of certification while self-certification is only seen as an acceptable certification scheme.

Under the first objective of the EU Cloud Strategy, the EC together with the Cloud Selected Industry Group (C-SIG) and ENISA have setup the Cloud Certification Schemes List (CCSL). CCSL gives an overview of different existing certification schemes, which could be relevant for Cloud Computing customers. The survey shows that only 31 % of respondents are aware of CCSL. This is clearly showing a need for increasing awareness of the Cloud Computing community on CCSL and for facilitating the access to pre-analysed certification schemes.

6.3 Cloud Computing Standardization and Certification

The organizations in table 1 have been considered for the elaboration of Standards, Specifications and Certification dedicated to Cloud Computing.

NOTE 1: The Cloud Standards Coordination Phase 2 approach to relevant standards and specifications in Cloud Computing is to consider the standards and specifications that are specific to Cloud Computing rather than more generic all-purpose standards.

NOTE 2: The column "Number of standards and certifications" refers to the number of standards or certifications from this organization presented in the list of standards of Annex A.

NOTE 3: Some of the organizations that were listed in Cloud Standards Coordination Phase 1 are not in this list because they have not produced Standards, only White Papers or Reports.

Table 1: Cloud Computing Standards, Specifications and Certification Setting Organizations

Organization	Type	Name	Number of standards or certifications
ATIS	SDO	Alliance for Telecommunications Industry Solutions	7
CSA	Certif.	Cloud Security Alliance	6
DMTF	SSO	Distributed Management Task Force	6
ETSI	SDO	European Telecommunications Standards Institute	55
EuroCloud	Certif.	EuroCloud	1
GICTF	SSO	Global Inter-Cloud Technology Forum	4
IEC	SDO	International Electrical Commission	See note
IEEE	SSO	Institute for Electrical and Electronics Engineers	1
ISO	SDO	International Organization for Standardization	18
ITU-T	SDO	ITU Telecommunication Standardization Sector	19
NIST	Agency	National Institute of Standards and Technology	6
OASIS	SSO	Organization for the Advancement of Structured Information Standards	4
ODCA	SSO	Open Data Center Alliance	28
OGF	SSO	Open Grid Forum	5
SNIA	SSO	Storage Networking Industry Association	1
TIA	SSO	Telecommunications Industry Association	1
TMF	SSO	TeleManagement Forum	6
NOTE: Common with ISO.			

There are 168 documents from 16 organizations, 114 with the status "Published", 48 with the status "Draft" and 6 with the status "In progress". Two organizations in table 1 were in the table for "White Papers, etc." in CSC phase 1. More details can be found in the Annex A of the present document.

This is to be compared with the list of CSC-2 that included 65 documents from 17 organizations, 50 with the status "Published" and 15 with the status "Draft".

Some preliminary remarks can be made regarding the Cloud Computing standardization landscape:

- The number of SSOs involved is slightly lower than for the same table of CSC-1. The main reason for this is that a number of the standard of CSC-1 have been transferred to SDOs and the organizations at the origin have stopped working on them.

- The overall number of standards is higher than in CSC-1, in particular for the "Published" ones. This is showing both that considerable progress has been made in delivering cloud standards since CSC-1 and that the coverage of the standards is larger than during CSC-1 (as anticipated) and that more support from standards can be expected for the organizations, in particular the Cloud Service Customers, that want to adopt Cloud computing.
- This is indicating that some consolidation of the standardization landscape has taken place since CSC-1. The consolidation can be observed both because of the number of actors (SSOs) has not increased since CSC-1 but rather slightly decreased and because of a greater importance of Standards versus White Papers and Reports (which were playing a greater role in CSC-1).

6.4 Cloud Computing Standards and specifications and the Cloud Service life-cycle

6.4.1 Introduction

CSC-2 has used the same approach as CSC-1 for mapping standards and specifications to the Cloud Computing Service life-cycle. To achieve comparability across the two "snapshots", the Cloud Computing Service life-cycle framework that was developed for Cloud Standards Coordination (phase 1) has been largely reused for this new maturity assessment.

The Service life-cycle is decomposed in three major phases:

- Phase 1: The Acquisition of a Cloud Service
- Phase 2: The Operation of a Cloud Service
- Phase 3: The Termination of a Cloud Service

In addition to these phases, some pre-conditions have been defined that refer to the Overview and Concepts that are common to all phases.

Within each of these phases, some activities have been identified in CSC-1 (via selected Use Cases). These activities can be performed by the Cloud Service Customer or the Cloud Service Provider.

The naming of the activities in CSC-2 - used by tables 2 to 5 - refers to the naming in CSC-1, so as to allow more easy comparison.

NOTE: These activities are not those defined in ISO/IEC 17789 [i.7] and Recommendation ITU-T Y.3502 [i.8].

Clauses 6.4.2 to 6.4.5 are presenting the mapping of Cloud Computing standards (identified at the time of writing the present document) on the activities within each of the phases.

6.4.2 Standards and specifications as pre-conditions to all (life-cycle) phases

Table 2 lists the applicable standards and specifications. Both standards and specifications are added to the lists according to the definition of SSO, SDO, standards and specifications in clause 3.

NOTE: In tables 2 to 5, the number between [ ] (e.g. [ISO11]) refers to the numbering in Annex A.

Table 2: Standards and specifications as pre-conditions to all (life-cycle) phases

Short Summary	Role	Related Standards & Specifications	Status	Remark
Overview and Concepts	CSC, CSP	[ISO11] ISO/IEC 19086-1	In progress	
		[ISO2] ISO/IEC 17788	Published	
		[ITU5]] ITU-T Y.3500	Published	Same as ISO/IEC 17788
Terminology and Metrics	CSC, CSP	[NIST7] SP 500-307	Draft	
		[ISO2] ISO/IEC 17788	Published	
		[ITU5]] ITU-T Y.3500	Published	Same as ISO/IEC 17788
		[ISO12] ISO/IEC 19086-2	In progress	

6.4.3 Standards and specifications in support of (life-cycle) Phase 1: Acquisition of Cloud Service

Table 3 lists the applicable standards.

Table 3: Standards and specifications in support of (life-cycle) Phase 1: Acquisition of Cloud Service

Short Summary	Role	Related Standards & Specifications	Status	Remark
Requirements specification	CSC	None at this time. GAP Gap resolution: nice-to-have		Standards needed. Such standards may help comparison of providers.
Security & Privacy Requirements specification	CSC	ISO 27000 family CSA PLA [CSA4].	Published In progress	Non Cloud Computing-specific
Service assessment and comparison	CSC	[OGF4] GFD.192	Published	
		[CSA1] CCM 3.0.1	Published	
		[ISO5] 27001	Published	
		[ISO6] 27002	Published	
Negotiation with one provider	CSC	[OGF5] GFD.193	Draft	
Negotiation for multiple providers	CSC	None at this time. GAP		
Determining SLA targets / thresholds	CSP	[OGF4] GFD.192	Published	
Standards expression of SLA	CSC	[ISO12] ISO/IEC 19086-2	In progress	
		[ISO13] ISO/IEC 19086-3	In progress	
		[ISO14] ISO/IEC 19086-4	In progress	
SLA publication	CSP	[OGF4] OGF GFD.192	Published	
		[CSA1] CCM 3.0.1	Published	
Enabling Interoperability	CSC	[OGF1] GFD.183 OCCI	Published	
		[OGF2] GFD.184 OCCI	Published	
		[OGF3] GFD.185 OCCI	Published	
		[DMTF1] DSP0263	Published	
		[ISO4] ISO/IEC 17826	Published	Same as SNIA CDMI
		[OASIS1] CAMP	In progress	
		[OASIS2] TOSCA	Published	
		[ISO16] ISO/IEC 19941	In progress	
		[OGF] OCCI 1.2	In Progress	
Enabling Data Portability	CSC	[ISO1] ISO/IEC 17203	Published	Same as DMTF DSP0243
		[OASIS2] TOSCA	Published	
		[ISO1] ISO/IEC 19941	Published	
Integration of cloud solution with legacy systems	CSC	None at this time. GAP Gap resolution: to be left to market		
Data Provisioning in Multiple Clouds	CSC	[OGF1] GFD.183 OCCI	Published	
		[OGF2] GFD.184 OCCI	Published	
		[OGF3] GFD.185 OCCI	Published	
		[DMTF1] DSP0263	Published	
		[ISO4] ISO/IEC 17826	Published	Same as SNIA CDMI
		[OASIS1] CAMP	In progress	
		[OASIS2] TOSCA	Published	
		[ISO1] ISO/IEC 17203	In progress	Same as DMTF DSP0243
Enabling Application Portability	CSC	OASIS2] TOSCA	Published	
		[OASIS1] CAMP	Published	
Strategy	CSC, CSP	None at this time. GAP Gap resolution: to be left to market		
Risk Assessment	CSC, CSP	None at this time. GAP Gap resolution: critical		

6.4.4 Standards and specifications in (life-cycle) Phase 2: Operation of Cloud Service

Table 4 lists the applicable standards and specifications.

Table 4: Standards and specifications in (life-cycle) Phase 2: Operation of Cloud Service

Short Summary	Role	Related Standards & Specifications	Status	Remark
Deployment over multiple providers	CSC	[OGF3] GFD.185 OCCI	Published	
		[DMTF1] DSP0263	Published	
		[OASIS2] TOSCA	Published	
Independent monitoring of SLA	CSC	[CSA2] CTP	Published	
		[CSA3] A6	Published	
		[DMTF4] DSP0262	Published	
		[DMTF5] DSP2038	Published	
Receiving and processing SLA reports	CSC	[CSA2] CTP	Published	
		[CSA3] A6	Published	
		[DMTF1] DSP0262	Published	
		[DMTF5] DSP2038	Published	
Reporting SLA infringements	CSC	[OGF4] GFD.192	Published	
Responding to SLA infringements	CSC	None at this time. GAP Gap resolution: critical		
Resolving SLA infringements disputes	CSC	None at this time. GAP Gap resolution: nice-to-have		
Administration of users, identities and authorizations	CSC	No Cloud Computing specific standards at this time but non Cloud Computing-specific standards could be adapted. GAP Gap resolution: critical		There is a number of non Cloud Computing-specific but widely used and very relevant security Standards and Specifications.
Creation of a VM image for a public cloud	CSP	[ISO1] ISO/IEC 17203	Published	Same as DMTF DSP0243
Provision of an infrastructure to allow the creation and management of (a set of) VMs	CSP	[OGF1] GFD.183 OCCI	Published	
		[OGF2] GFD.184 OCCI	Published	
		[OGF3] GFD.185 OCCI	Published	
		[DMTF3] DSP0263	Published	
		[ISO1] ISO/IEC 17203	Published	Same as DMTF DSP0243
Monitoring Service Levels	CSP	[OGF4] GFD.192	Published	
		[CSA2] CTP	Published	
		[CSA3] A6	Published	
Monitoring Availability	CSP	None at this time. GAP Gap resolution: critical		Monitoring needed of the CSP services to enable efficient and informative reporting towards their CSCs and to enable the CSCs to retrieve information needed to monitor the fulfillment of their SLAs and to take proactive actions in case of degradation of one ore more relevant metrics
Monitoring Incident management	CSP	No Cloud Computing specific standards at this time but non Cloud Computing-specific standards could be adapted. GAP Gap resolution: critical		There is a number of non Cloud Computing-specific specifications, like, e.g. the DSCI Security Framework
Monitoring Storage performance	CSP	None at this time. GAP Gap resolution: critical		As above: Monitoring needed of the CSP services
Monitoring Processing performance	CSP	None at this time. GAP Gap resolution: critical		As above: Monitoring needed of the CSP services

Short Summary	Role	Related Standards & Specifications	Status	Remark
Monitoring Networking performance	CSP	None at this time. GAP Gap resolution: critical		As above: Monitoring needed of the CSP services
Monitoring Access security event information	CSP	None at this time. GAP Gap resolution: critical		As above: Monitoring needed of the CSP services
Monitoring uptime	CSP	None at this time. GAP Gap resolution: critical		As above: Monitoring needed of the CSP services
Preventative response to SLA infringement	CSP	None at this time. GAP Gap resolution: critical		
Enabling Application Portability	CSC	OASIS2] TOSCA	Published	
		[OASIS1] CAMP	Published	

6.4.5 Standards and specifications in (life-cycle) Phase 3: Termination of Cloud Service

Table 5 lists the applicable standards and specifications.

Table 5: Standards and specifications in (life-cycle) Phase 3: Termination of Cloud Service

Short Summary	Role	Related Standards & Specifications	Status	Remark
Termination process initiation	CSC	None at this time. GAP Gap resolution: to be left to market.		Difficult to standardize
Termination: SLA evaluation	CSC	[OGF4] GFD.192	Published	
Contract termination	CSC	[OGF4] GFD.192	Published	
Providing an evaluation report	CSP	None at this time. GAP Gap resolution: critical		Standards needed.
Resolving disputes	CSP	No Cloud Computing specific standards at this time but non Cloud Computing-specific standards could be adapted. GAP Gap resolution: to be left to market		There are non Cloud Computing-specific best practices and standards, such as ISO 10000, ITIL and FitSM
Transaction records retention	CSP	None at this time. GAP Gap resolution: nice-to-have.		

7 Users concerns: how standards and specifications can help

7.1 Introduction

This clause investigates how standards and specifications can help addressing the users' concerns. These concerns, identified in the CSC-2 survey (see [i.2]), are compared with those identified in CSC-1 to show how some of these concerns remain persistent over time. The level of support provided by a standard or a specification is presented for each concern.

7.2 Comparison of user concerns: how standards and specifications can help

Figure 3 shows customers' and users' concerns in decreasing order with respect to the percentage of customers and users considering the concerns as critical or very critical. The numbers are based on the results of the CSC-2 survey (see [i.2]).

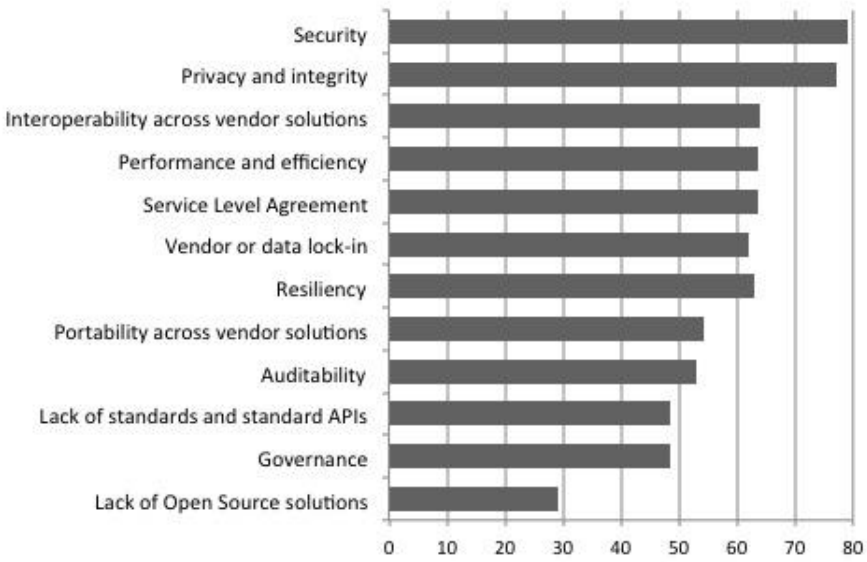

Figure 3: Users' concerns in the Cloud Standards Coordination Phase 2 survey

In the 2013 report summarizing the findings of CSC-2 (see [i.1]) three areas of concern were identified:

- Service Level Agreement
- Interoperability
- Security

As can be seen from the two lists above, the three areas of concern identified in CSC-1 are still ranked as top concerns according to the outcome of the CSC-1 User survey (see [i.2]).

7.3 How standards and specifications are in support of users' concerns

7.3.0 Introduction

This clause addresses the users concerns listed above and identifies which standards or specifications apply in this context. This clause complements the CSC-2 "Interoperability and Security" report (see [i.2]).

7.3.1 Cloud Service Level Agreements

Addressing the concerns related to Service Level Agreements also involves providing support for relating cross cutting aspects, such as performance and efficiency, resiliency, auditability.

The published standards and specifications that apply in this context are:

- Cloud specific

  CSA A6

  CSA CCM

  CSA CTP

  DMTF DSP0262

  DMTF DSP2038

  ISO/IEC 17788 / Recommendation ITU-T Y.3500

  ISO/IEC 17789 / Recommendation ITU-T Y.3502

- Non Cloud specific

  ISO/IEC 27001

  ISO/IEC 27002

  OGF GFD.192

In the future, the following ones will be also available:

- Cloud specific

  ISO/IEC 19086-1

  ISO/IEC 19086-2

  ISO/IEC 19086-3

  ISO/IEC 19086-4

  NIST SP 500-307

- Non Cloud specific

  OGF GFD.193

7.3.2 Interoperability

Addressing the concerns related to Interoperability includes addressing those related to interoperability across vendor solutions, vendor or data lock-in, portability across vendor solutions.

The standards and specifications that apply in this context are:

DMTF DSP0263

ISO/IEC 17203 (same as DMTF DSP0243)

ISO/IEC 17826 (same as SNIA CDMI)

OASIS CAMP

OASIS TOSCA

OGF GFD.183 OCCI

OGF GFD.184 OCCI

OGF GFD.185 OCCI

In the future, the following ones will also be available:

ISO/IEC 19041

ISO/IEC 19044

OGF OCCI 1.2

7.3.3 Security

Addressing the concerns regarding Security also includes addressing concerns related to privacy and integrity, Authentication, Identity & access management, Authorization & Security policy management.

The standards and specifications that apply in this context are:

- Cloud specific

  CSA CCM

ISO/IEC 27018

- Non cloud specific

  ISO/IEC 27001

  ISO/IEC 27002

  Kerberos

  Oauth 2.0

  SAML 2.0

In the future, the following ones will also be available:

ISO/IEC 27017 / Recommendation ITU-T X.1631

NOTE: There are other non Cloud Computing-specific but widely used and very relevant security standards and specifications that are not listed here. The CSC-2 "Interoperability and Security" report addresses some of them (see [i.4], clause 7).

7.3.4 Other concerns

Other concerns mentioned in the user survey include:

- Contract (besides or complementary to the SLA).
- Legal aspect and Legislation.
- Financial health of providers.

As was the case for CSC-1, the standards and specifications identified in CSC-2 may not be very much supportive.

7.4 Summary

As presented in the two Cloud Standards Coordination Phase 2 reports "Users survey" (see [i.2]) and "Interoperability and Security" (see [i.4]), there is still work to be done to fully address the main concerns of existing and future Cloud Computing users. Not all of these efforts however involve developing new standards or certification schemes.

As shown in the web survey, a growing awareness of already existing standards and certification schemes will most likely favorably change the experience of many users that the Cloud is insufficiently safe and reliable to use for enterprise class ICT (e.g. weak SLAs, insufficient recovery/fallback provisions for disasters in the past, data theft by, e.g. national intelligence agencies, industrial espionage). The analysis of the available standards that target the Cloud, both in the main areas of concern as well as in other areas, show that efforts are underway to at least partially address some of the major concerns.

Examples of significant ongoing developments include the work done in ISO/IEC where three parallel development projects are underway - on Cloud SLA, interoperability and portability and finally on security and the particular challenges that are created when users are increasingly using different devices, mixing personal and corporate data and accessing Cloud services from different locations (with potentially different regional and/or national legislation to be considered). ISO is addressing data in their on-going work on "Data and their flow across devices and Cloud services" (ISO/IEC CD 19944 [i.9]) as part of their JTC 1/SC 38 Cloud Computing and Distributed Platforms activities in WG5.

8 Conclusions and Recommendations

It is fair to claim that the evolution in terms of continued standards and specifications development is positive when comparing the situation when the CSC-1 was launched and the current status indicated by and presented in the CSC-2 reports.

However, further alignment and collaboration are needed on the one hand between SDOs and all SSOs, and on the other hand, with the Open Source projects as well as the Cloud Computing solution vendors that provide solutions that potentially require alignment to standards and specifications. Such an example can be found in the CSC-2 "Standards and Open Source" report (see [i.3]) where the support of Cloud Computing standards and specifications by Open Source projects is analysed.

As the Cloud Computing adoption continues and as the "gaps" are filled and outstanding standards and specifications that address current concerns are made available, there is a need to ensure that no fragmentation is created and that overlap and parallelism is avoided. From this standpoint, the conclusions made in clause 5 are quite encouraging and display a somewhat consolidated standardization landscape.

The following recommendations can be made:

1) Encourage the development of education and dissemination material of Cloud Computing standards and specifications (from a strictly objective standpoint, in particular across all concerned SSOs).

2) Encourage the large SDOs/SSOs to strengthen collaboration and cooperation, with the overarching objective to focus on chief concerns identified in clause 7 and to accelerate the provisioning of necessary Cloud Computing standards and specifications that will strengthen the adoption of Cloud Computing as the future main ICT platform, thus supporting the EC's objective to make the Cloud available and secure for the EU member states' citizens, public sector and private sector alike. This could, e.g. be done based on the JTC1 PAS process as a mechanism to enhance co-operation, as some of the SSOs already did.

3) Encourage SSOs and Open Source organizations to more systematically provide formally documented support to Cloud Computing standards and specifications within the Open Source implementations of Cloud Computing solutions.

4) Regularly organize "progress report" events to advertise the progress made with Cloud Computing standards, specifications and Open Source towards the Cloud Service Customers (e.g. SMEs, industries) thus supporting the EC's objective to make the Cloud available and secure for the EU member states' citizens, public sector and private sector alike.

5) As part of the progress report events the adoption of each appropriate standard or specification should be evaluated to provide an indication for the changes in the use of standards and specifications, e.g. increased or decreased use respectively.

6) There are many interoperability and portability standards and specifications that are supported by Cloud providers that are not Cloud-specific. Identifying and publishing a core set of these across Cloud providers would be helpful during the provider selection phase.

7) Gaps identified in the present document (marked in the tables in clauses 6.3.0 to 6.3.3) need further analysis to identify the relevance of each gap, e.g. which gaps are blocking and need to be addressed with priority.

8) Further analysis is needed to decide whether intervention by the EC is needed to organize the effort to close the gaps with a high priority or the respective communities will take care of and/or the market will drive the effort for closing the gaps.

9) Special attention should be given to the creation of standards and specifications for detailed monitoring of the CSP services to enable efficient and informative reporting towards their CSCs and to enable the CSCs to retrieve information needed to monitor the fulfillment of their SLAs and to take proactive actions in case of degradation of one ore more relevant metrics.

10) Encourage Open Source Projects, probably together with some incentives, to bring their APIs into SSO/SDOs for rendering them into a standard or a specification.

As such, Cloud Standards Coordination has limited means to act as a practical "coordinating force". However, its set-up may be modified to allow for some work of marketing and dissemination of Cloud Computing standards.

9 Areas for further study

Some areas for further study are possible:

- Updated and more complete list of Cloud Service life-cycle activities in Annex B. At this stage, the current list is based on the Use Cases of Cloud Standards Coordination Phase 1 - and to some extent to those addressed in the Cloud Standards Coordination Phase 2 "Interoperability and Security" report (see [i.3]). Other activities may be brought from the analysis of additional Use Cases.
- A more complete mapping of standards on the list of activities, provided it is modified as described above.
- More precision on the support of user concerns by standards in clause 7.
- More recommendations, in particular regarding the way to support the marketing and dissemination effort regarding emerging standards.
- A more complete list of Cloud Computing standards in Annex A if needed, in particular those who are not strictly Cloud Computing related.
- Expand the list of standards to relevant non Cloud Computing-specific standards.

Annex A:
Cloud Computing Standards Landscape

A.1 Presentation of results

For the assessment of the maturity of Cloud Computing standards, Cloud Standards Coordination has selected a list of organizations relevant in Cloud Computing standardization, together with a list of standards (published or draft) developed by these organizations, collected at the time of writing the draft CSC-2 reports ETSI SR 003 381 [i.2], ETSI SR 003 382 [i.3], ETSI SR 003 391 [i.4] and the present document, in July 2015.

CSC-1 had identified two classes of documents relevant to Cloud Computing:

- Standards and Specifications: a Standard is an output from a formally recognized SDO (such as ETSI or ITU-T), a Specification is an output from any other form of SSO that becomes a Standard when ratified by a recognized SDO. This classification is corresponding to the definition of the new regulation on European standardization (see [i.5]).
- Reports, White Papers and other types of documents.

CSC-2 has concentrated only on the list of Standards and Specifications. In the remainder of this clause, the name "Standard" will be used for either "Standard" or "Specification".

NOTE:

- The lists in clause A.2 gather both standards and certification schemes from SSOs and other actors (agencies, etc.).
- Lines in black font refer to standards already present in CSC-1. New standards are in bold black font.
- The status of a document that has changed from "Draft" to "Published" in CSC-2 is in bold black font.
- Lines in *italics* refer to standards that are in "Draft" status at the time of writing the final report.
- Some of the organizations that were listed in CSC-1 are not in this list because:
  - they have not produced standards, only White Papers or Reports; or
  - they have transferred their results to other organizations, like TOG;
  - they have stopped operations, like CSMIG.

A.2 SSOs and Standards list

A.2.1 ATIS - Alliance for Telecommunications Industry Solutions

Table A.1: Atis standards

CSC Reference	Source Reference	Title	Status
[ATIS1]	ATIS-0200003	CDN Interconnection Use Case Specification and High Level Requirements	Published
[ATIS2]	ATIS-0200004	CDN Interconnection Use Cases and Requirements for Multicast-Based Content Distribution	Published
[ATIS3]	ATIS-0200005	Cloud Framework for Telepresence Service	Published
[ATIS4]	ATIS-0200006	Virtual Desktop Requirements	Published
[ATIS5]	ATIS-0200008	Trusted Information Exchange (TIE)	Published
[ATIS6]	ATIS-0200009	Cloud Service Lifecycle Checklist	Published
[ATIS7]	ATIS-0200010	CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment	Published

A.2.2 CSA - Cloud Security Alliance

Table A.2: CSA standards

CSC Reference	Source Reference	Title	Status
[CSA1]	CCM 3.0.1	Cloud Control Matrix	Published
[CSA2]	CTP	Cloud Trust Protocol	Published
[CSA3]	A6	Cloud Audit	Published
[CSA4]	PLA	Privacy Level Agreement	Published
[CSA5]	TCI	Reference Architecture - Trusted Cloud Initiative	Published
[CSA6]	OCF	Open Certification Framework	Published

A.2.3 DMTF - Distributed Management Task Force

Table A.3: DMTF standards

CSC Reference	Source Reference	Title	Status
[DMTF1]	DSP0263	Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP Specification	Published
[DMTF2]	DSP0264	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM)	Published
[DMTF3]	DSP0243	Open Virtualization Format Specification V2	Published
[DMTF4]	**DSP0262**	**Cloud Auditing Data Federation (CADF) - Data Format and Interface Definitions Specification**	**Published**
[DMTF5]	**DSP2038**	**Cloud Audit Data Federation - OpenStack Profile (CADF-OpenStack**	**Published**
[DMTF6]	**DSP0265**	**Profile to Enable Automated Deployment of OVF Packages**	**Published**

A.2.4 ETSI - European Telecommunications Standards Institute

Table A.4: ETSI standards

CSC Reference	Source Reference	Title	Status
[ETSI1]	ETSI TS 103 142	Test Descriptions for Cloud Interoperability	Published
[ETSI2]	**ETSI GS NFV 001**	**Use Cases**	**Published**
[ETSI3]	**ETSI GS NFV 002**	**Architectural Framework**	**Published**
[ETSI4]	**ETSI GS NFV 003**	**Terminology for Main Concepts in NFV**	**Published**
[ETSI5]	**ETSI GS NFV 004**	**Virtualisation Requirements**	**Published**
[ETSI6]	**ETSI GS NFV-INF 001**	**Infrastructure Overview**	**Published**
[ETSI7]	**ETSI GS NFV-INF 003**	**Infrastructure; Compute Domain**	**Published**
[ETSI8]	**ETSI GS NFV-INF 004**	**Infrastructure; Hypervisor Domain**	**Published**
[ETSI9]	**ETSI GS NFV-INF 005**	**Infrastructure; Network Domain**	**Published**
[ETSI10]	**ETSI GS NFV-INF 007**	**Infrastructure; Methodology to describe Interfaces and Abstractions**	**Published**
[ETSI11]	**ETSI GS NFV-INF 010**	**Service Quality Metrics**	**Published**
[ETSI12]	**ETSI GS NFV-MAN 001**	**Management and Orchestration**	**Published**
[ETSI13]	**ETSI GS NFV-SWA 001**	**Virtual Network Functions Architecture**	**Published**
[ETSI14]	***ETSI GS NFV-IFA 001***	***Acceleration Technologies; Report on Acceleration Technologies & Use Cases***	***Draft***

CSC Reference	Source Reference	Title	Status
[ETSI15]	*ETSI GS NFV-IFA002*	*Acceleration Technologies; VNF Interfaces Specification*	*Draft*
[ETSI16]	*ETSI GS NFV-IFA003*	*Acceleration Technologies; vSwitch Benchmarking and Acceleration Specification Acceleration - Switching Aspects Spec*	*Draft*
[ETSI17]	*ETSI GS NFV-IFA004*	*Acceleration Technologies; Management aspects Specification Acceleration - Mgmt aspects Spec*	*Draft*
[ETSI18]	*ETSI GS NFV-IFA005*	*Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification*	*Draft*
[ETSI19]	*ETSI GS NFV-IFA006*	*Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification*	*Draft*
[ETSI20]	*ETSI GS NFV-IFA007*	*Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification*	*Draft*
[ETSI21]	*ETSI GS NFV-IFA008*	*Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification*	*Draft*
[ETSI22]	*ETSI GS NFV-IFA009*	*Management and Orchestration; Report on Architectural Options*	*Draft*
[ETSI23]	*ETSI GS NFV-IFA010*	*Management and Orchestration; Functional requirements specification*	*Draft*
[ETSI24]	*ETSI GS NFV-IFA011*	*Management and Orchestration; VNF Packaging Specification*	*Draft*
[ETSI25]	*ETSI GS NFV-IFA012*	*Management and Orchestration; Os-Ma-Nfvo reference point - Application and Service Management Interface and Information Model Specification Os-Ma-Nfvo ref point Spec - svc mgmt. & info model*	*Draft*
[ETSI26]	*ETSI GS NFV-IFA013*	*Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification*	*Draft*
[ETSI27]	*ETSI GS NFV-IFA014*	*Management and Orchestration Network Service Templates Specification*	*Draft*
[ETSI28]	*ETSI GS NFV-IFA015*	*Management and Orchestration; Report on NFV Information Model*	*Draft*
[ETSI29]	*ETSI GS NFV-EVE001*	*Virtualisation Technologies; Hypervisor Domain Requirements specification Hypervisor Rqmts spec*	*Draft*
[ETSI30]	*ETSI GS NFV-EVE002*	*Ecosystem; Report on MEF Carrier Ethernet Services Use Cases MEF Use Cases report*	*Draft*
[ETSI31]	*ETSI GS NFV-EVE003*	*Ecosystem; Report on NFVI Node Physical Architecture Guidelines for Multi-Vendor Environment NFVI Node Arch report*	*Draft*
[ETSI32]	*ETSI GS NFV-EVE004*	*Virtualisation Technologies; Report on the application of Different Virtualization Technologies in the NFV Framework*	*Draft*
[ETSI33]	*ETSI GS NFV-EVE 005*	*Ecosystem; Report on SDN Usage in NFV Architectural Framework*	*Draft*
[ETSI34]	ETSI GS NFV-PER 001	NFV Performance & Portability Best Practices	Published
[ETSI35]	ETSI GS NFV-PER 002	Proofs of Concept; Framework	Published
[ETSI36]	ETSI GS NFV-REL 001	Resiliency Requirements	Published
[ETSI37]	ETSI GS NFV-REL 002	Reliability; Report on Scalable Architectures for Reliability Management	Published
[ETSI38]	*ETSI GS NFV-REL003*	*Reliability; Report on Models and Features for E2E Reliability*	*Draft*
[ETSI39]	*ETSI GS NFV-REL004*	*Assurance; Report on Active Monitoring and Failure Detection Active monitoring & failure detection report*	*Draft*

[ETSI40]	*ETSI GS NFV-REL005*	*Accountability ; Quality Accountability Framework*	*Draft*
[ETSI41]	**ETSI GS NFV-SEC 001**	**NFV Security; Problem Statement**	**Published**
[ETSI42]	**ETSI GS NFV-SEC 002**	**NFV Security; Cataloguing security features in management software**	**Published**
[ETSI43]	**ETSI GS NFV-SEC 003**	**NFV Security; Security and Trust Guidance**	**Published**
[ETSI44]	**ETSI GS NFV-SEC 004**	**NFV Security; Privacy and Regulation; Report on Lawful Interception Implications**	**Published**
[ETSI45]	*ETSI GS NFV-SEC005*	*Trust; Report on Certificate Management Certificate mgmt. report*	*Draft*
[ETSI46]	*ETSI GS NFV-SEC006*	*Security Guide; Report on Security Aspects and Regulatory Concerns Sec & Regulation report*	*Draft*
[ETSI47]	*ETSI GS NFV-SEC007*	*Trust; Report on Attestation Technologies and Practices for Secure Deployments NFV Attestation report*	*Draft*
[ETSI48]	*ETSI GS NFV-SEC008*	*Security Monitoring and Management; Report on Use Cases, Requirements and Architecture Security Monitoring report*	*Draft*
[ETSI49]	*ETSI GS NFV-SEC 009*	*Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration*	*Draft*
[ETSI50]	*ETSI GS NFV-SEC010*	*NFV Security; Report on Retained Data problem statement and requirements*	*Draft*
[ETSI51]	*ETSI GS NFV-SEC011*	*Security; Report on NFV LI Architecture*	*Draft*
[ETSI52]	*ETSI GS NFV-SEC012*	*System architecture for execution of sensitive NFV components*	*Draft*
[ETSI53]	*ETSI GS NFV-SEC013*	*Security Management and Monitoring specification*	*Draft*
[ETSI54]	*ETSI GS NFV-TST001*	*Pre-deployment Testing; Report on Validation of NFV Environments and Services*	*Draft*
[ETSI55]	*ETSI GS NFV-TST002*	*Testing Methodology; Report on Interoperability Testing Methodology*	*Draft*

A.2.5 EuroCloud

Table A.5: Eurocloud standards

CSC Reference	Source Reference	Title	Status
[EuroCloud1]	Star Audit	EuroCloud Star Audit	Published

A.2.6 GICTF - Global Inter-Cloud Technology Forum

Table A.6: GICTF standards

CSC Reference	Source Reference	Title	Status
[GICTF1]		**Use case and functional requirements for Inter-Cloud Computing**	**Published**
[GICTF2]		**Inter-Cloud interface specification on protocols**	**Published**
[GICTF3]		**Inter-Cloud interface specification on resources data model for network control**	**Published**
[GICTF4]		**Network and technical requirements in support of Inter-Cloud**	**Published**

A.2.7 IEEE - Institute for Electrical and Electronics Engineers

Table A.7: IEEE standards

CSC Reference	Source Reference	Title	Status
[IEEE1]		**Standard for Intercloud Interoperability and Federation (SIIF)**	**In progress**

A.2.8 ISO/IEC - International Organization for Standardization / International Electrical Commission

Table A.8: ISO/IEC standards

CSC Reference	Source Reference	Title	Status
[ISO1]	17203	OVF	Published
[ISO2]	17788	Cloud Computing Overview and Vocabulary	Published
[ISO3]	17789	Cloud Computing Reference Architecture	Published
[ISO4]	17826	Cloud Data Management Interface (same as SNIA CDMI)	Published
[ISO5]	27001	Information security management systems - Requirements	Published
[ISO6]	27002	Code of practice for information security controls	Published
[ISO7]	*27017*	*Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002*	*Draft*
[ISO8]	27018	Code of practice for data protection controls for public cloud computing services	Published
[ISO9]	20000-1	Service management system requirements	Published
[ISO10]	27036-4	Information security for supplier relationships - Part 4: Guidelines for security of cloud services	Draft
[ISO11]	*19086-1*	*Cloud computing -SLA framework and terminology - Part 1: Overview and concepts*	*In progress*
[ISO12]	***19086-2***	***Cloud computing - SLA framework and technology - Part 2: Metrics***	***In progress***
[ISO13]	***19086-3***	***Cloud computing - SLA framework and technology - Part 3: Core requirements***	***In progress***
[ISO14]	***19086-4***	***Cloud computing - SLA framework and technology - Part 4: Security and Privacy***	***In progress***
[ISO15]	**19099**	**Virtualization management specification**	**Published**
[ISO16]	**19831**	**Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol - An Interface for Managing Cloud Infrastructure (same as DMTF CIMI)**	**Published**
[ISO17]	***19941***	***Interoperability and Portability***	***Draft***
[ISO18]	***19944***	***Data and their Flow across Devices and Cloud Services***	***Draft***

A.2.9 ITU-T - ITU Telecommunication Standardization Sector

Table A.9: ITU-T standards

CSC Reference	Source Reference	Title	Status
[ITU1]	X.1601	Security framework for cloud computing	Published
[ITU2]	Y.3501	Cloud Computing Framework & high-level requirements	Published
[ITU3]	Y.3510	Cloud Computing Infrastructure requirements	Published
[ITU4]	Y.3520	Resource management framework for e2e cloud	Published
[ITU5]	Y.3500	Cloud Computing overview and vocabulary	Published
[ITU6]	Y.3511	Framework of inter-cloud computing	Published
[ITU9]	**Y.3512**	**Functional requirements for Network as a Service (NaaS)**	**Published**
[ITU10]	**Y.3513**	**Functional requirements for Infrastructure as a Service (IaaS)**	**Published**
[ITU11]	**Y.3600**	**Requirements and capabilities for cloud computing based big data**	**Draft**
[ITU12]	**Y.DaaS-arch**	**Functional architecture of Desktop as a Service**	**Draft**
[ITU13]	**Y.CCNaaS-arch**	**Functional architecture of Network as a Service**	**Draft**
[ITU14]	**Y.CCIC-arch**	**Functional architecture of inter-cloud computing**	**Draft**
[ITU15]	**Y.oe2ecm**	**Overview of e2eCloud Computing Management**	**Draft**
[ITU16]	**Y.e2ecslm-Req**	**End-to-end cloud service lifecycle management**	**Draft**
[ITU17]	***Y.cctic***	***Cloud computing trusted inter-cloud***	***Draft***
[ITU18]	***M.rcsm***	***Requirements for Cloud Service Management***	***Draft***
[ITU19]	***X.1631***	***Code of practice for information security controls based on ISO/IEC 27002 for cloud services***	***Draft***

A.2.10 NIST - National Institute of Standards and Technology

Table A.10: NIST standards

CSC Reference	Source Reference	Title	Status
[NIST1]	**SP 500-291**	**NIST Cloud Computing Standards Roadmap**	**Published**
[NIST2]	**SP 800-145**	**NIST Definition of Cloud Computing**	**Published**
[NIST3]	SP 500-292	NIST Cloud Computing Reference Architecture	Published
[NIST4]	**SP 800-144**	**Guidelines on Security and Privacy in Public Cloud Computing**	**Published**
[NIST5]	***SP 500-299***	***NIST Cloud Computing Security Reference Architecture***	***Draft***
[NIST6]	**SP 800-125**	**Guide to Security for Full Virtualization Technologies**	**Published**
[NIST7]	**SP 500-307**	***Cloud Computing Service Metrics Description***	***Draft***

A.2.11 OASIS - Organization for the Advancement of Structured Information Standards

Table A.11: OASIS standards

CSC Reference	Source Reference	Title	Status
[OASIS1]	**CAMP**	**Cloud Application Management for Platforms (CAMP)**	**Published**
[OASIS2]	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA)	Published
[OASIS3]	ODP	Open Data Protocol	Published
[OASIS4]		**Identity in the Cloud Use Cases**	**Published**

A.2.12 ODCA - Open Data Center Alliance

Table A.12: ODCA standards

CSC Reference	Source Reference	Title	Status
[ODCA1]	n/a	Master Usage Model: Compute Infrastructure as a Service	Published
[ODCA2]	n/a	Master Usage Model: Service Orchestration	Published
[ODCA3]	n/a	Master Usage Model: Commercial Framework	Published
[ODCA4]	n/a	Usage: Data Security Framework	Published
[ODCA5]	n/a	Virtual Machine (VM) Interoperability in a Hybrid Cloud Environment	Published
[ODCA6]	n/a	Master Usage Model: Software-Defined Networking	Published
[ODCA7]	n/a	Master Usage Model: Scale out Storage	Published
[ODCA8]	n/a	Master Usage Model: Information as a Service	Published
[ODCA9]	n/a	Usage: Standard Units of Measure for IaaS	Published
[ODCA10]	**n/a**	**Usage Model: Cloud infrastructure**	**Published**
[ODCA11]	**n/a**	**Usage Model: Cloud based identity governance and auditing**	**Published**
[ODCA12]	**n/a**	**Usage model: Guide on identity management interoperability**	**Published**
[ODCA13]	**n/a**	**Usage Model: IaaS privileged user access**	**Published**
[ODCA14]	**n/a**	**Usage model: Guide to interoperability across clouds**	**Published**
[ODCA15]	**n/a**	**Usage Model: PaaS interoperability**	**Published**
[ODCA16]	**n/a**	**Usage Model: SaaS interoperability**	**Published**
[ODCA17]	**n/a**	**Usage model: Data management for Information as a Service**	**Published**
[ODCA18]	**n/a**	**Usage model: Single sign-on authentication**	**Published**
[ODCA19]	**n/a**	**Usage model: Security monitoring**	**Published**
[ODCA20]	**n/a**	**Usage model: Regulatory framework**	**Published**
[ODCA21]	**n/a**	**Usage model: Service orchestration**	**Published**
[ODCA22]	**n/a**	**Usage model: Provider assurance**	**Published**
[ODCA23]	**n/a**	**Usage model: Carbon footprint and energy efficiency**	**Published**
[ODCA24]	**n/a**	**Usage model: Service catalog**	**Published**
[ODCA25]	**n/a**	**Usage model: Cloud service brokering**	**Published**
[ODCA26]	**n/a**	**Usage model: Long-distance migration**	**Published**
[ODCA27]	**n/a**	**Usage model: Software entitlement management framework**	**Published**
[ODCA28]	**n/a**	**Usage model: e-discovery and forensics**	**Published**

A.2.13 OGF - Open Grid Forum

Table A.13: OGF standards

CSC Reference	Source Reference	Title	Status
[OGF1]	GFD.183	Open Cloud Computing Interface - Core	Published
[OGF2]	GFD.184	Open Cloud Computing Interface - Infrastructure	Published
[OGF3]	GFD.185	Open Cloud Computing Interface - RESTful HTTP Rendering	Published
[OGF4]	GFD.192	Web Services Agreement (WS-Agreement)	Published
[OGF5]	*GFD.193*	*WS-Agreement Negotiation*	*Draft*
[OGF6]		*OCCI1.2*	*Draft*

A.2.14 SNIA - Storage Networking Industry Association

Table A.14: SNIA standards

CSC Reference	Source Reference	Title	Status
[SNIA1]	CDMI	Cloud Data Management Interface - ISO 17826:2012	Published

A.2.15 TIA - Telecommunications Industry Association

Table A.15: TIA standards

CSC Reference	Source Reference	Title	Status
[TIA1]	ANSI/TIA-942-A	Telecommunications Infrastructure Standards for Data Centers	Published

A.2.16 TMF - TeleManagement Forum

Table A.16: TMF standards

CSC Reference	Source Reference	Title	Status
[TMF1]	**TR194**	**TR194 Multi-Cloud Service Management Accelerator Pack - Introduction**	**Published**
[TMF2]	**TR195**	**Multi-Cloud Service Management Pack - Business Guide**	**Published**
[TMF3]	**TR196**	**Multi-Cloud Service Management Pack - Technical Guide**	**Published**
[TMF4]	**TR197**	**Multi-Cloud Service Management Pack - SLA Business Blueprint Framework-Multi-Cloud Blueprint**	**Published**
[TMF5]	**TR198**	**Multi-Cloud Service Management Pack- Simple Management API (SMI) Developer Primer-Service Delivery Framework Cloud Interface**	**Published**
[TMF6]	**GB963**	**Cloud SLA Application Note**	**Published**

Annex B:
Standards in the CC Service life-cycle

B.1 Introduction

This annex is presenting the activities performed by the Cloud Service Customer (CSC) and the Cloud Service Provider (CSP) across the Cloud Service life-cycle.

The Service life-cycle is decomposed in three major phases:

- Phase 1: Acquisition of Cloud Service
- Phase 2: Operation of Cloud Service
- Phase 3: Termination of Cloud Service

On top of these phases, some pre-conditions have been defined that refer to the Terminology and Metrics that are common to all phases.

In each of the phases, all activities are associated to:

- A short summary that is used in clause 5 for the mapping of the Cloud Computing standards.
- A description of the activity.
- The role (CSC or CSP) involved in the activity.

NOTE 1: The lines for CSP activities have a slightly greyed background (to differentiate them from CSC ones).

NOTE 2: The activities presented in this Annex are based on the Use Cases that were developed during CSC (phase 1). Since then, two international standards for Cloud Computing now exist that address the notion of activities and could potentially replace the content of Annex, i.e. ISO/IEC 17788 [i.10] ([ISO2]) and ISO/IEC 17789 [i.7] ([ISO3]).

B.2 Pre-condition to all phases

Some preconditions apply to all Service life-cycle phases.

Table B.1: Pre-conditions to all (life-cycle) phases

Short Summary	Description	Role
Overview and concepts	It is a precondition for the following steps that each Cloud service is based on a commonly agreed high-level description of the concepts used.	CSC, CSP
Terminology and Metrics	It is a precondition for the following steps that each service level objective uses consistent and widely accepted and agreed terminology as well as clearly defined KQIs and metrics.	CSC, CSP

B.3 Phase 1 activities: Acquisition of a Cloud Service

The principal activities of the CSC in this phase are service selection and purchase, performed by the Customer Business Manager sub-role.

The principal activities in this phase are listed in table B.2.

Table B.2: Activities for "Acquisition of a Cloud Service"

Short Summary	Description	Role
Requirements specification	Functional requirements of a cloud service are specified by means of a service description. Non-functional requirements are specified by means of SLAs/certificates. The same applies for one or multiple provider(s). These requirements will be matched with the provider capabilities in the "Service Assessment and Comparison" activity.	CSC
Security & Privacy Requirements specification	The customer needs to analysed its Data Privacy obligations with respect to the Personal Data (outside Europe the term PII - Personal Identifiable Information - may refer to Personal Data) if any that will be processed by the cloud services, and build a set of security and privacy requirements that should be fulfilled by the cloud service provider. This list will be used afterwards (cf. "Service Assessment and Comparison" activity) to evaluate the different available cloud services. Particular attention should be paid to the rights that a Personal Data principal may have relating to their Personal Data (e.g. right to examine the data which the customer holds about the principal).	CSC
Service assessment and comparison	Examining the cloud service offerings of (one or more) cloud service providers to determine if the service offered meets the business and technical and security requirements of the customer and comparing it with other offerings on the market. This typically involves the reading of a service catalogue and documentation for each service, which should include information about the service and its SLAs, plus business information including pricing, and security & privacy. With respect to the latter, the customer retrieves information about the service offering from the provider's product catalog, including: Service availability, including redundancy & disaster recovery Confidentiality & integrity of data flowing between the customer and the SaaS application Measures to ensure availability, confidentiality and integrity of customer data that is stored on the providers systems and used by the SaaS application Location(s) for storage of the customer data Acknowledgement by the provider that the SaaS service involves the storage and processing of Personal Data and that the provider plays the role of Personal Data Processor in relation to this Personal Data. Logging and reporting capabilities, both of routine operations and also relating to security incidents. The examination of the Cloud Service Provider's security & privacy may be supported by a recurrent certification process.	CSC
Negotiation with one provider	Negotiation of the terms for the cloud service (if the Cloud Service Provider permits variable terms for the service) or selection among market offerings. If the cloud service provider permits variable terms for the service, then the customer might need to specify additional security & privacy requirements for the provider to implement. This includes the definition of the termination process, metrics and related actions such as data migration in the SLA.	CSC
Negotiation for multiple providers	Negotiation of the terms for the Cloud service is similar to the "Negotiation with one provider" activity. In addition, determining the individual providers for deployment of the different applications and the data according to the requirements of the service consumers.	CSC
Determining SLA targets / thresholds	Setting up targets and thresholds in the SLA (based e.g. on its capabilities and feedback from its business).	CSP
Standards expression of SLA	Agreement on SLA/certificate data format, acceptance of the contract for the cloud service and registration with the cloud service provider.	CSC
SLA publication	Drafting and publishing an SLA including compliance with regulatory norms.	CSP
Enabling Interoperability	Agreement on common interfaces between the provider and the customer, including management and administration interfaces.	CSC
Enabling Data Portability	Agreement on common formats of the Data (e.g. VMs image).	CSC
Integration of cloud solution with legacy systems	Integration with e.g. legacy OSS/BSS, security systems, etc.	CSC
Data Provisioning in Multiple Clouds	Regular upload/import of VMs and latest data from one provider to the other cloud providers (e.g. to facilitate data recovery).	CSC
Legal aspect and Legislation	Compliance with regulatory and/or national laws is one of the main concerns as it can block the adoption of Cloud in some cases	CSC

B.4 Phase 2 activities: Operation of a Cloud Service

The principal activities in this phase are listed in table B.3.

Table B.3: Activities in "Operation of a Cloud Service"

Short Summary	Description	Role
Deployment over multiple providers	Deployment of the different VMs with data and applications into the negotiated infrastructures of the different cloud providers.	CSC
Independent monitoring of SLA	Independent monitoring of service levels, including application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service.	CSC
Receiving and processing SLA reports	Receiving and processing service level reports from the cloud service provider (or a trusted third party (e.g. auditor)), comparing them with SLA objectives.	CSC
Reporting SLA infringements	Reporting service level agreement infringements detected by the cloud service customer or end-users.	CSC
Responding to SLA infringements	Responding to SLA infringements either as reports from the cloud service provider or detected by the cloud service customer (for example, informing their end-users of service interruptions, switching service to an alternate provider, raising a ticket, claiming service credits, etc.).	CSC
Resolving SLA infringements disputes	Resolving disputes around SLA infringements.	CSC
Administration of users, identities and authorizations	Administration of users, identities and authorizations.	CSC
Creation of a VM image for the public cloud	Creation of a VM image for the public cloud (B) corresponding to the exact functional objectives of the VM image running on the private cloud (A), for a coordinated use on A and B. This requires knowing exactly what functional differences could exist between B and A (if any).	CSP
Provision of an infrastructure to allow the creation and management of (set of) VMs	Provision of an infrastructure to allow the creation and management of (a set of) VMs • Upload the VM image onto the public cloud (B) • Start the technical process that will be able to start VM instances on B when required or start the VM instances on B: – An overview about the running phase – Monitoring of VMs (e.g. compliance with SLA) – Possibility to reconfigure resources (e.g. re-scaling resources - add or remove VMs)	CSP
Monitoring Service Levels	Monitoring service levels and reporting them to the cloud customer. The content of this activity depends strongly on the type of attributes/targets being monitored. Key examples are found in the sub-activities below. (See note)	CSP
Monitoring Availability	Monitoring service levels: Availability.	CSP
Monitoring Incident management	Monitoring service levels: Incident management (targets).	CSP
Monitoring Storage performance	Monitoring service levels: Storage performance.	CSP
Monitoring Processing performance	Monitoring service levels: Processing performance.	CSP
Monitoring Networking performance	Monitoring service levels: Networking performance.	CSP
Monitoring Access security event information	Monitoring service levels: Access security event information.	CSP
Monitoring uptime	Monitoring service levels: Uptime.	CSP
Preventive response to SLA infringement	Responding (in particular preventively) to SLA infringement incidents: • Availability, Incident Management, Elasticity, etc.	CSP
NOTE: The information contained in these reports may need to be sanitized to avoid disclosing sensitive data.		

B.5 Phase 3 activities: Termination of a Cloud service

The principal activities in this phase are listed in table B.4.

Table B.4: Activities in "Termination of a Cloud service"

Short Summary	Description	Role
Termination process initiation	Launching the termination process (as defined in Phase 1), which might include retrieval of image (IaaS) and data (SaaS, quick switch). Ensure both the return of all customer data (including Personal Data) and its secure deletion.	CSC
Termination: SLA evaluation	Evaluate whether the SLA was fulfilled, i.e. the outsourced application did run in the new environment and fulfilled all functional and non-functional requirements.	CSC
Contract termination	Terminating the contract as defined by SLA or on demand.	CSC
Providing an evaluation report	Provide an evaluation report on closing, including confirmation of deleting customer data at a defined point of time as agreed in the SLA.	CSP
Resolving disputes	Resolve disputes around cloud service termination.	CSP
Transaction records retention	Keep a record of past transactions, under data retention obligations.	CSP

Annex C: Change History

Date	Version	Information about changes
August 2015	1.0.0	First publication of the SR for comments
November 2015	2.0.0	Final publication based on the changes provided by: - Comments from the NTECH Technical Committee review - Comments from the public review gathered on http://csc.etsi.org - Additional changes proposed during the final review workshop

History

Document history		
V2.1.1	February 2016	Publication