SLA - Ready
Making Cloud SLAs readily usable in the EU private sector

www.sla-ready.eu

Title: A Common Reference Model to describe, promote and support the uptake of SLAs

Author(s): Ruben Trapero, Neeraj Suri, TUDA

Contributor(s): Arthur van der Wees, Arthur; Jesus Luna, CSA

Date: 31 May, 2016

HORIZON 2020

Coordination and Support Action
Grant Agreement no: 644077
ICT-07-2014: Advanced Cloud Infrastructures and Services

Executive Overview

SLA-Ready aims to increase the trust on Cloud Service Providers (CSP) to consequently leverage the higher uptake of Cloud services. As the CSP and user linkage transpires typically via contractual Service Level Agreements (SLAs), the standardisation and transparency of SLAs is paramount to provide Cloud Service Customers (CSCs) with enough information about what services to use, what to expect from them and what to trust.

To this end, SLA-Ready provides a common understanding of SLAs for Cloud services with the creation of a Common Reference Model (CRM) that integrates SLA components (e.g., terminology, SLA attributes, Service Level Objectives (SLOs), guidelines and best practices).

SLA-Ready has developed the Common Reference Model by analysing the requirements that were elicited in deliverables D2.1 (Requirements emerging from a state-of-the-art analysis) and D2.2 (Requirements emerging from a state-of-the-art analysis – Final report). The result of the analysis is reported in this deliverable (D2.3 - A Common Reference Model to describe, promote and support the uptake of SLAs) that not only reports the CRM but also validates it with respect to the current state of practice in different domains. As a result, D2.3 focuses on:

- The creation of the initial version of the CRM that is based on the requirements elicited in D2.1 and D2.2.
- The analysis of the CRM with respect to the current state of practice in the standardization community.
- The analysis of the CRM with respect to the current state of practice in the industry, by analysing sector specific use cases.
- An initial introduction to the evaluation of SLAs readiness by using the CRM.

D2.3 is the initial iteration over the process of creation and evaluation of the CRM. The final CRM version will be refined in D2.4 (A Common Reference Model to describe, promote and support the uptake of SLAs – Final report). D2.4 will also include a more comprehensive analysis of the state of practice and a possible refinement of the CRM based on (a) the results obtained during the initial validation of the CRM, and (b) incorporating the feedback received from different stakeholders through surveys and use cases evaluations.

Table of Contents

Table of Tables

Table of Figures

Document information

Deliverable number	D2.3
Deliverable title	A Common Reference Model to describe, promote and support the uptake of SLAs
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	31 May 2016
Actual delivery date	31 May 2016
Author(s)	Rubén Trapero, Neeraj Suri, TUDA
Contributor(s)	Jesús Luna, CSA; Arthur van der Wees, Arthur's Legal
Reviewer(s)	Silvana Muscella, Roberto Cascella; Trust-IT
Task(s) contributing to the deliverable	Task 2.3 – SLA challenges and requirements in cloud landscape
Target audience(s)	Project partners, members of the SLA-Ready Advisory Board and other external experts, European Commission, project reviewers
Total number of pages	81

Disclaimer

SLA-Ready has received funding under Horizon 2020, ICT-07-2014: Advanced Cloud Infrastructures and Services. The information contained in this document is the responsibility of SLA-Ready and does not reflect the views of the European Commission.

List of Acronyms

CRM	Common Reference Model
CSA	Cloud Security Alliance
CSC	Cloud Service Customer
CSP	Cloud Service Provider
ICT	Information and Communications Technology
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
FP7	The Seventh Framework Programme (2007-2013)
H2020	Horizon 2020
ICT	Information and communications technology
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
MSA	Master Service Agreement
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SLO	Service Level Objective
SME	Small and Medium-sized Enterprise
WCAG	W3C Web Content Accessibility Guidelines

Glossary[1]

Cloud Service Provider Data	Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider. Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on
Data controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data
Data Integrity	The property of protecting the accuracy and completeness of assets

[1] In order to use community-consistent terminology, the glossary is extracted from the relevant standards. The exception is the term "SLA-Readiness Index" which has been proposed by the SLA-Ready consortium.

Data Intervenability	The capability of a cloud service provider to support the cloud service customer in facilitating exercise of data subjects' rights. Note: Data subjects' rights include without limitation access, rectification, erasure of the data subjects' personal data. They also include the objection to processing of the personal data when it is not carried out in compliance with the applicable legal requirements
Data processor	A natural or legal person, public authority, agency or any other body which processes Personal data on behalf of the Data controller
Data protection	The employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework
Data Subject	An identified or identifiable natural person, being an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
Disaster recovery	Ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption
Failure notification policy	Specifies the process by which cloud service customers can notify the cloud service provider that a service outage has been observed, the process by which the cloud service provider notifies cloud service customers that a service outage has occurred, the process for providing updates on service outages, who receives notifications and updates, the maximum time between the detection of a service outage and the issuance of a notice of service outage, the maximum time interval between service outage updates and how service outage updates are described
Identity Assurance	The ability of a relying party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's true, accurate and correct identity
(Master) Cloud services agreement (MSA)	A legal document is the overarching part relating to the Cloud service, which describes the terms agreed between the provider and the customer under which the cloud service is made available and used. The MSA has a number of synonyms such as "Customer Agreement", "Terms of Service" or simply "Agreement". The MSA references a number of subsidiary parts, such as the Cloud SLA, Security and Privacy Policies, the Acceptable User Policy, the Business Continuity Policy and the Service Description.
Metric	A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of

	a measurement
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
Personally Identifiable Information (PII)	Documented agreement between the service provider and customer that identifies services and service level objectives
Remedy	Compensation available to the cloud service customer in the event the cloud service provider fails to meet a specified service level objective
Resilience	Ability of a cloud service to recover operational condition quickly after a fault occurs
Service Level Agreement (SLA)	Documented agreement between the service provider and customer that identifies services and service level objectives
Service Level Objective (SLO)	A specific, measurable characteristic of a cloud service for which the cloud service provider makes a commitment
SLA-Readiness Index	A quantitative metric that can be used to compare the CSPs contained in the SLA Repository
Vulnerability	A weakness of an asset or group of assets, e.g. software or hardware related, that can be exploited by one or more threats

1. Introduction

This deliverable develops and validates the initial version of SLA-Ready's Common Reference Model (CRM), an integrated set of SLA components (i.e., attributes and SLOs), plus guidelines/state of practice and standard terminology fulfilling the requirements identified by the consortium[2]. A high-level view of the process followed to develop and validate the CRM presented in this report is illustrated in Figure 1.

The purpose of this deliverable is to develop a SLA-usage reference document, which will be transferred onto the SLA-READY marketplace as an easy to read reference for the SLA-READY stakeholders which are herewith categorised as: 1. SMEs, 2. Large Companies, 3. Cloud Service Providers, and 4. Cloud Service Customers.

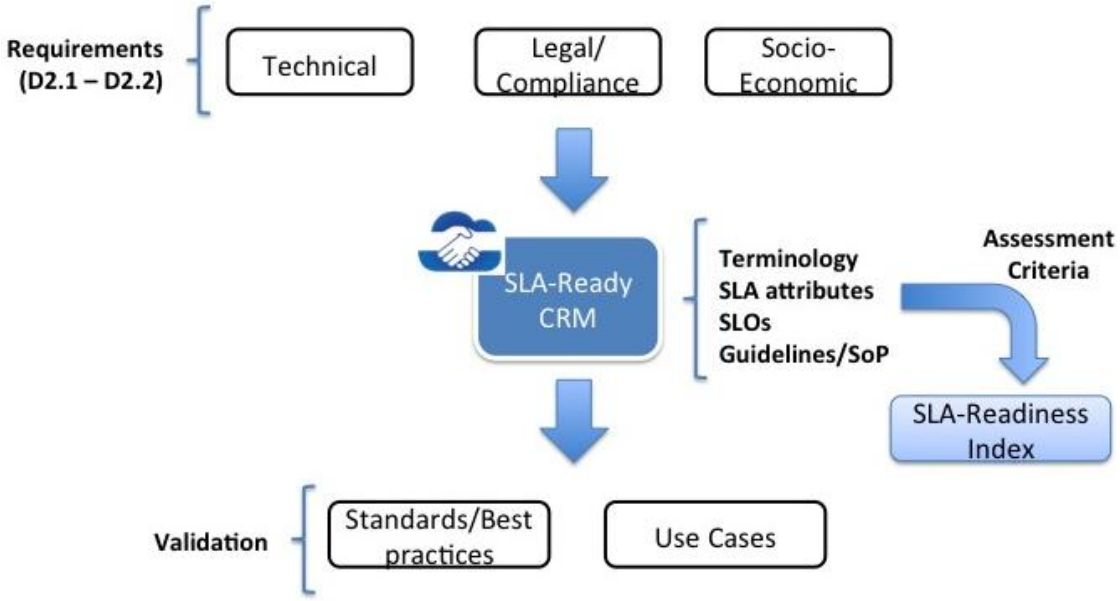


Figure 1. Developing and validating the SLA-Ready CRM.

Taking as a starting point the elicited requirements (i.e., technical, legal, and socio-economic) from deliverables D2.1/2.2, this deliverable proposes a set of elements for the CRM, which are validated over the following different perspectives of:

- Relevant standards and best practices.
- Sector-specific use cases.

Subsequently, the validation process refines the CRM components in order to provide an initial version of the associated SME best practices/usage guidelines.

[2] Please refer to Deliverable 2.1 and Deliverable 2.2

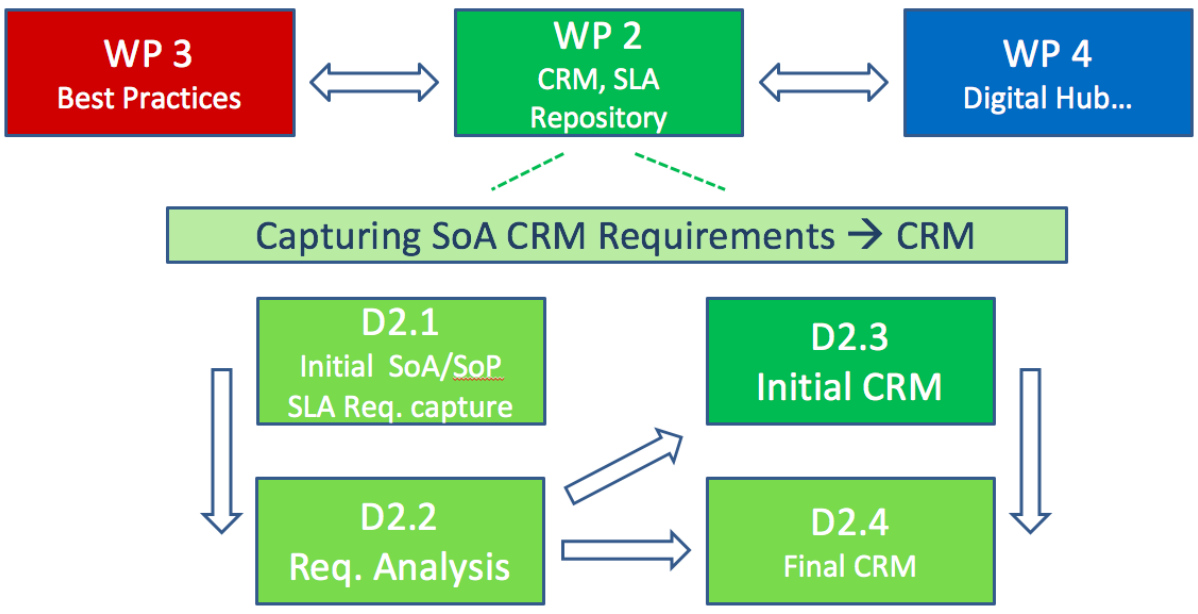
Finally, this deliverable also proposes the "SLA-Readiness Index" i.e., a quantitative metric that can be used to compare the CSPs contained in our SLA Repository. The SLA-Readiness Index is based on the contributed CRM, and it is expected to become part of both SLA-Ready's Social Marketplace and CSA STAR repository.

1.1. Positioning D2.3 within SLA-Ready

This deliverable (D2.3) is the first of two iterations for the creation of the Common Reference Model (CRM) to define cloud SLAs. D2.3 is the initial version that uses the results reported in D2.2 which analysed the state of practice of the SLA-definition and SLA-management from the technical, economical, sociological and legal perspectives. The analysis of D2.2 also extracted the requirements from different domains, including the research community, the industry and the standardization communities. The elicitation of these requirements is used in D2.3 to provide the initial version of the CRM along with a comparative analysis of its usage via sector specific use cases. The second iteration of this document (D2.4) will provide the final version of the CRM with a comprehensive analysis with respect to the current market status.

Figure 2 shows the relationship of D2.3 with the rest of the WP2 deliverables. The CRM is created with the inputs received from WP3 (International cooperation, consensus and standardisation), from the analysis of the state of practice carried out in D2.2, and from the feedback received from the SLA-Ready's Advisory Board.

Figure 2. D2.3 within SLA-Ready



1.2. Structure of this report

This report is organized as follows:

- Section 2 utilizes the elicited SLA requirements (from D2.2) covering the technical, sociological, economic and legal/governance perspectives, to develop SLA-Ready's initial CRM.
- Section 3 compares the initial version of the CRM with the main standards and best practices, and also maps the CRM components to the SLA models produced by the standardization community. This section analyses the coverage of the CRM with respect to those standards.
- Section 4 describes the comparison of the CRM with sector specific use cases from several domains, including financial, public and SMEs.
- Section 5 describes the dominant techniques to assess SLAs that will be used to evaluate the readiness of the CRM created in WP2.
- Section 6 presents our summary observations on the CRM.

The listing of the considered use cases and the CRM questionnaire for CSPs appears respectively in Annexes A and B.

2. *Initial version of the Common Reference Model*

This section overviews the SLA-Ready's proposed CRM. Section 2.1 summarizes the requirements elicited from D2.2, while Section 2.2 outlines the initial version of the CRM.

2.1. Elicited CRM Requirements

As derived from D2.2, Table 1 lists the 26 requirements as elicited by Tasks 2.1 (SLA challenges and requirements in a cloud landscape) and 2.2 (Legal, privacy and data governance issues) and reported in D2.2. The list of requirements is the result of a comprehensive analysis covering the different perspectives spanning:

- **Technical perspectives** by examining SLA components from several domains, including the standardization community that is working on the definition of SLAs (such as the ISO 19086 specification), and the research community participating in projects related to the specification and management of SLAs (such as CUMULUS, SPECS or A4Cloud).
- **Sociological perspectives** by examining the requirements demanded by cloud customers and the characteristics of the SLAs provided by the industry.
- **Economical perspectives**, by examining the characteristics of the SLAs provided by different types (big and small) of CSPs, with special focus on the economic features (such as billing and cost related clauses).
- **Legal and governance perspectives** by examining the current state of practice of CSPs with respect to current regulations and legal obligations or contract management.

The evaluation of the previous perspectives was summarized into 26 requirements as reported in Table 1. The requirements have been categorized into different groups, according to the aspects analysed as:

- **General requirements (GR):** derived mostly from the analysis of the legal domain representing the aspects to be included in any contract (such as the duration of the SLA) or simply general procedural aspects (such as the number of pages of the SLA).
- **Responsibility requirements (RR):** derived mostly from the sociological and legal analysis, include requirements related to the regulations applied or the responsible parties involved in the SLA.
- **Economic requirements (ER):** derived from the economical analysis, this group contains requirements related to charging and billing.

- **Technical SLOs requirements (TS):** derived from the technical analysis, this group contains specific requirements derived from technical components found in SLAs from different domains (industry, research and standardization community).

Table 1. CRM Requirements and Fulfilment (from D2.2)

Item	Type	Name of CRM requirement
1	GR	SLA URL
2	GR	Findable
3	RR	Contact details
4	RR	Contact availability
5	GR	Number of pages
6	GR	SLA language
7	GR	Machine-readable format
8	GR	Revision date
9	GR	Update frequency
10	GR	Previous versions and revisions
11	GR	SLA duration
12	RR	Unilateral change
13	RR	SLA change notifications
14	RR	SLA transparency
15	RR	SLA reporting
16	RR	SLA continuous reporting
17	ER	Service Credit
18	ER	How are service credits assigned
19	ER	Maximum service credits
20	RR	General carve-outs
21	RR	Choice of law
22	TS	Possibility of specials and other customisations
23	TS	Performance SLOs
24	TS	Security SLOs
25	TS	Data Management SLOs

Item	Type	Name of CRM requirement
26	RR	Personal Data Protection SLO

This core table of requirements has been used to develop the elements that comprise the initial version of the Common Reference Model as described in the next subsection.

2.2. The SLA-Ready CRM

The SLA-Ready Common Reference Model includes common vocabularies, SLO metrics/measurements, best practices, recommendations and standard templates that can be used to define SLAs for different use cases and applicable certifications. To this end, the requirements elicited in D2.2 and described in Section 2.1 are used to identify the elements that represent an SLA. The CRM follows a hierarchical structure (Figure 3). The top level represents the main Groups that organize the rest of the elements of the CRM. The core of the CRM is the Element level that includes the main parts that can be mapped to the different aspects of SLAs. The lowest level comprises the CRM Components (e.g., SLA attributes and SLOs) that could be part of some CRM elements. Figure 4 explains an example CRM component and elements relationship.

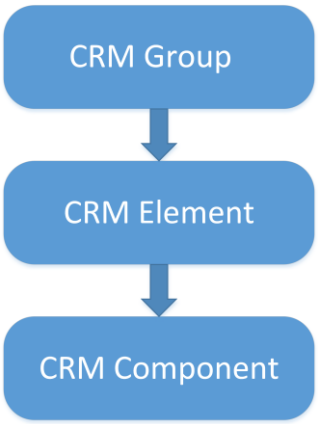


Figure 3. CRM hierarchical specification

Overall, 70 CRM elements were identified and organized into 8 groups shown in Table 2.

Table 2. CRM Groups

CRM Group	Description
General	Describe general purpose features of the SLA
Freshness	Describe features related to the validity of the SLA
Readability	Describe features related to the level of understanding of the SLA
Support	Describe features related to the level of support that customers can receive from

CRM Group	Description
	the CSP
Credits	Describe features related to the costs and billing management of the SLA
Changes	Describe features related to eventual modifications carried out in the SLA and the management associated to those changes
Reporting	Describe the features related to the communications that the CSP transmit to the customers with respect to the SLA managed
SLO & Metrics	Describe the features related to the technical elements of the SLA and its corresponding components.

As an example, the CRM group of "SLO & Metrics" contains 8 elements where 7 elements are compliant with the classification of SLOs as described in the ISO 19086 specification. Figure 4 outlines the elements of the SLO & Metric group, and also the components related to each element. Two of the illustrated elements provide general information about the SLO & Metrics group as:

- The "Specified SLO metrics" element is used to represent the existence of SLOs and metrics in the description of the SLA. Obviously, if the SLA does not specify such information, the rest of the components of this group will also not appear in the SLA.
- The "General" element is used to represent whether the general elements of the ISO19086 specification are included in the SLA. More specifically, the two components expected under this element are (i) the existence of a field in the SLA to describe the roles and responsibilities and (ii) the existence of a field to explain the cloud SLA definitions.

The rest of the elements of this group represent technical aspects of the SLA (such as security or privacy). For consistency, the naming convention used herein has been taken from the ISO 19086 specification. These components of the CRM are used to check whether those technical aspects are included in SLAs.

Figure 4. Components of the SLO & Metrics element of the CRM

On this background, the following sections analyse the CRM from varied perspectives of:

- From the **standardization community**, by analysing the level of compliance of the prominent standards on SLA specifications.
- From the **industrial perspectives** by analysing use cases from representative sectors (such as financial, SME and public sectors).
- From the **research community** with an initial description of the techniques to assess SLAs that can be used to assess their level of compliance with respect to the CRM.

On this background of capturing the relations across the Groups, Elements and Components, the resultant CRM is summarized in Table 3.

Table 3. CRM summary

Group	Name of CRM element	Component (if applicable)
General	SLA URL	n/a
	Findable	n/a
	Choice of law	n/a
	Roles and responsibilities	n/a
	Cloud SLA definitions	n/a
Freshness	Revision date	n/a
	Update Frequency	n/a

	Previous versions and revisions	n/a
	SLA duration	n/a
Readability	SLA language	n/a
	Machine-readable format	n/a
	Nr. of pages	n/a
Support	Contact details	n/a
	Contact availability	n/a
Credits	Service Credit	n/a
	Service credits assignment	n/a
	Maximum service credits (Euro amount) provided by the CSP	n/a
Changes	SLA change notifications	n/a
	Unilateral change	n/a
Reporting	Service Levels reporting	n/a
	Service Levels continuous reporting	n/a
	Feasibility of specials & customisations	n/a
	General Carveouts	n/a
SLOs & Metrics	Specified SLO metrics	n/a
	General SLOs	Service monitoring
		Accessibility
		Availability
		Termination of service
		Cloud Service Support
		Governance
		Attestations, certifications and audits
	Cloud Service Performance SLOs	Response time
		Capacity
		Elasticity
	Service Reliability SLOs	Service Resilience
		Customer data backup/restore

		Disaster Recovery
	Data Management SLOs	IPR
		Cloud Service Customer Data
		Cloud Service Provider Data
		Account Data
		Derived Data
		Data portability
		Data deletion
		Data location
		Data examination
		Law Enforcement Access
	Security SLOs	Organization of Information Security
		Human Resources Security
		Asset Management
		Access Control
		Cryptography
		Physical and Environmental Security
		Operations Security
		Communications Security
		Systems Acquisition, Development and Maintenance
		Supplier Relationships
		Information Security Incident Management
		Business Continuity Management
		Compliance
	Personal Data Protection SLOs	Consent and choice
		Purpose legitimacy and specification
		Collection limitation
		Data minimization
		Use, retention and disclosure limitation
		Accuracy and quality

		Openness, transparency and notice
		Individual participation and access
		Accountability
		Privacy compliance

3. CRM mapping to standards and best practices

In order to maximize the impact and facilitate the adoption of the contributed CRM by industrial stakeholders, and in particular by SMEs, it is necessary to ensure its alignment with relevant standards and best practices. This task will also benefit SMEs, who are typically not cloud experts, and often with very limited understanding of cloud SLAs and especially the role of relevant related standards/best practices.

Consequently, this section starts the alignment process by conducting a gap analysis of the CRM from the standardisation perspective by using as input the work done by SLA-Ready's WP3 (International cooperation, consensus and standardisation), in particular D3.2 (Standardisation and international cooperation report) which reports relevant standards/best practices in this field. Our goal is to ascertain the degree of standardisation related coverage of the CRM, such that the SMEs using it have assurance that the provided SLA guidance is aligned with the relevant standards and best practices. Furthermore, the results of the gap-analysis performed in this section can be used by the SLA-Ready marketplace (please refer to WP4) in order to create interactive guides that, based on the SMEs requirements, can realise both the (i) CRM elements to consider for their own use cases, and (ii) outline standards/best practices that could be taken into consideration either as development guidelines or references.

3.1. Initiatives being analysed

Based on the outcomes from Deliverable 3.2, this section focuses on gap analysing the contributed CRM with respect to the following relevant set of standards and best practices:

Table 4. Standards and best practices relevant for validating the CRM

Organisation	Initiative acronym	Initiative	Relevance to the CRM
CSCC	CSCC SLA	Practical Guide to Cloud Service Level Agreements – v2 [1]	The 10 recommended CSCC SLA steps are state of practice.
EC	C-SIG SLA	Cloud SLA Standardisation Guidelines [2]	These guidelines became part of the EC contribution to ISO/IEC 19086-1, and represent one of the main results from the respective C-SIG group.
EC	SMART	Standards terms and performance criteria in service level agreements for Cloud	The proposed Model SLA is the most current EC-sponsored study in this field.

Organisation	Initiative acronym	Initiative	Relevance to the CRM
		computing services [3]	
ETSI	TR 103 125	SLAs for Cloud services [4]	The defined SLA template is relevant to the industry.
ISO	19086-1/-4	Cloud SLAs terminology, and security and privacy [5]	Both standards are generating high expectations with the industry, so CRM alignment with them will also maximize its chances for industrial adoption.

Please note that the approach followed in this section is easily extendable (after the end of SLA-Ready) as new standards and best practices (also relevant to the CRM) get released.

3.2. Results of the analysis

Table 5 summarizes the results of the performed gap analysis. For each analysed standard/best practice, we assess if the corresponding CRM element is being referenced or not.

The primary conclusions from our analysis are the following:

1. The analysis of the CRM with respect to surveyed standards and best practices shows that there is good coverage related to the CRM's SLOs elements. However, general-purpose SLOs (e.g., related to existing certifications, and SLA governance) are only discussed in ISO/IEC 19086-1 and the Cloud Standards Consumer Council's (CSCC) "Practical guide to Cloud SLAs version 2"[1].
2. None of the analysed works utilized any standardized or consistent formats to specify the actual SLO metrics to use (please refer to Deliverable 2.2 for examples), although in many cases they provided selective high-level metrics as examples.
3. Unfortunately, relevant standards such as the upcoming ISO/IEC 19086-1/-4 do not contain any reference related to essential CRM's elements that SLA-Ready has identified as significant means to empower/guide SMEs in their transition to the Cloud. For example, the advocated elements such as SLA findability, update/validity period, available languages, are still not addressed by the standards. The same situation occurs with known best practices such as the "Cloud SLA checklist" contained in the SMART EC report [3].

4. From the analysed-standards/best-practices, only the CSCC report provided the highest CRM coverage. However, we note that the CSCC report still has conspicuous gaps related to CRM's elements such as choice of law and others as reported in ISO/IEC 19086-1/-4.
5. It is also worth mentioning that, despite not being cloud-specific, the SLA template defined by ETSI in their "ETSI EG 202 009-3" report also shown a good coverage[3] of the CRM elements. This was expected due to the fact that such template was referenced in ETSI's "SLAs for Cloud Services" technical report.

From the performed analyses it may be noted that the contributed D2.3 CRM has the potential to improve cloud customers' understanding related to SLAs, while at the same time providing good coverage of the elements included in these relevant standards/best practices. The most evident benefit of the CRM with respect to surveyed works is in the following groups:

- General
- Freshness
- Readability
- Credits

As already mentioned, the results shown in Table 5 can be used to structure SLA-Ready's guidance documents to be produced by WP3 and WP4. Automated marketplace tools can then be designed, as based on Table 5, in order (for example) to (a) list relevant CRM elements based on the SME's selected cloud SLA standards/best practices, and (b) allow SMEs to focus on a specific set of CRM elements which can then be referenced to the pertinent standards and best practices.

[3] With the exception of cloud-specific elements

Table 5. CRM coverage of relevant standards and best practices

CRM element	CRM coverage to relevant standards (Yes/No)				
	ISO/IEC 19086[4] (Part 1 and Part 4)	Cloud SLA checklist[5]	Guide for Evaluating Cloud SLAs[6]	C-SIG SLA Guidelines	ETSI's cloud SLA template[7]
SLA URL	No	No	No	No	No
Findable	No	No	No	No	No
Choice of law	No	No	No	No	No
Roles and responsibilities	Yes	Yes	Yes	No	Yes
Cloud SLA definitions	Yes	No	No	Yes	Yes
Revision date	No	No	Yes	No	Yes
Update Frequency	No	No	Yes	No	Yes
Previous versions and revisions	No	No	Yes	No	Yes
SLA duration	No	No	Yes	No	Yes
SLA language	No	No	No	No	No
Machine-readable format	No	No	No	Yes	No

[4] Analysis performed with the latest versions available at the time of writing this document: 19086-1 (DIS) and 19086-4 (WD)

[5] Please refer to Annex 1 in "Standards terms and performance criteria in service level agreements for cloud computing services (SMART 2013/0039) Model SLA"

[6] Please refer to "Practical guide to Cloud SLAs version 2", Cloud Standards Consumer Council. 2015.

[7] Please refer to "SLAs for Cloud Services", ETSI TR 103 125, 2012 and the "Template for SLAs", ETSI EG 202 009-3, 2006.

	CRM coverage to relevant standards (Yes/No)				
CRM element	**ISO/IEC 19086[4] (Part 1 and Part 4)**	**Cloud SLA checklist[5]**	**Guide for Evaluating Cloud SLAs[6]**	**C-SIG SLA Guidelines**	**ETSI's cloud SLA template[7]**
Nr. of pages	No	No	No	No	No
Contact details	Yes	Yes	Yes	Yes	Yes
Contact availability	No	No	Yes	Yes	Yes
Service Credit	No	No	Yes	No	No
Service credits assignment	No	No	No	No	No
Maximum service credits (Euro amount) provided by the CSP	No	No	No	No	No
SLA change notifications	Yes	Yes	Yes	Yes	Yes
Unilateral change	No	Yes	Yes	No	No
Service Levels reporting	Yes	Yes	Yes	Yes	Yes
Service Levels continuous reporting	No	Yes	Yes	No	Yes
Feasibility of specials & customizations	No	No	Yes	No	No
General Carveouts	Yes	No	Yes	No	No
Specified SLO metrics	Yes	No	Yes	Yes	Yes
General SLOs	Yes	Yes	Yes	No	Yes
Cloud Service Performance SLOs	Yes	Yes	Yes	Yes	No
Service Reliability SLOs	Yes	Yes	Yes	Yes	Yes
Data Management SLOs	Yes	Yes	Yes	Yes	Yes
Security SLOs	Yes	Yes	Yes	Yes	Yes
Personal Data Protection SLOs	Yes	Yes	Yes	Yes	No

4. Sector specificity of CRMs

The value of the CRM comes from its customizability to the varied application domains, and hence this section analyses the CRM by studying several use cases from varied domains. Each of use case is analysed by first taking the CRM as a reference, and then assessing which CRM elements are actually applicable along with considering their priorities therein.

4.1. Use case template

The use case analysis of the CRM presented in this section aims to (i) quantitatively assess the relative importance of each CRM element with respect to specific Cloud Service Customer (CSC) requirements/use cases, (ii) extrapolate the conclusions drawn from the CRM to the more general ETSI CSC use cases [6], and (iii) link the results from the presented analysis to the SLO metrics introduced in D2.2. These three goals are necessary to develop the guidance SLA-Ready will report in "D3.3 - A Business Guide to Service Level Agreements: How to be a well-advised user of cloud services".

For the analysis of the use cases, we will use the template shown in Table 6 where the detailed information about the target cloud scenario and the involved SLAs are collected. With respect to the former, the proposed template gathers information related to the more general 'Base Use Case' being used (as presented in D2.2), with the goal of relating/extrapolating the results of the analysis to the ETSI scenarios presented in Annex A of this report. The template also collects information related to the prospective SLA (i.e., cloud service life-cycle, preconditions and requirements), which will be used in D3.3 to develop the best practices related to the corresponding SLO metrics and SLA life-cycle stage (using also as input D2.2).

Moreover, the proposed template can be easily re-used and extended to document and analyse new use cases specific to the SMEs that would like to adopt SLA-Ready's approach to leverage the proposed CRM.

Table 6. Use Case Template

Identification	**Title**	UC name
	Base Use Case (cf., Deliverable 2.2)	Reference Use Cases as taken from the ETSI CSC report. One or more from: • AP: App on a Cloud • CB: Cloud Bursting • SD: Processing Sensitive Data • DI: Data Integrity • HA: High Availability Please refer to D2.2 for more information.
	Short description	Short summary/user-story of the use case

		highlighting applicable industrial sector
	Cloud Actors	List of involved actors/stakeholders from ETSI CSC: • Cloud Service Provider • Cloud Service Customer • Cloud Service Partner Please refer to Annex A for more information.
	Cloud Service life-cycle phase	Any of the following: • Acquisition • Operation • Termination Please refer to D2.2 for more information.
	Legal and Data Protection compliance criteria	List of legal and data protection requirements associated to the use case
Preconditions and Requirements	**Security and privacy requirements**	Summary of security requirements to be taken into account for the scenario
	Additional preconditions and requirements (e.g., performance)	Assumptions made prior to the execution of the use case
	Existing SLA standards and best practices to rely on	List of SLA standards/best practices to rely on: • ISO/IEC 19086 • SMART SLA Model • CSCC Practical Guide to Cloud SLAs • C-SIG SLA Guidelines • ETSI Cloud SLA template Please refer to Section 3 for more information.
	Additional comments	Add comments, remarks, suggestions, as you see fit
Summary	Conclusions related to the use case analysed	

4.2. Use cases and CRM mapping

This section demonstrates the applicability of the proposed template (cf. Table 6) for analysing the developed CRM from the use cases perspective. In particular, we focus on the analysis of four real-world use cases, chosen by the consortium because of their relevance to SMEs. As mentioned in the previous section, the performed analysis (and template) can be extended to other use cases reflecting the needs of specific SMEs willing to leverage SLA-Ready's outcomes.

4.2.1. Financial sector use cases

Most start-ups and (other) SMEs that are active in the Fintech industry (where the financial services meet new technologies and business models) wish to develop and exploit their respective services and products on top of cloud-based services, in particular either IaaS or PaaS. Cloud-by-default is becoming more and more the standard, as a basis to develop, rely, and exploit its own PaaS respectively SaaS. The use case has been simplified in order to make clear a major requirement on the SME side as an assertion

that 'one cannot acquire or procure anything without first assessing what it would like to acquire or procure'.

Identification	**Title**	Fintech Early Stage Seeking IaaS
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data • DI: Data Integrity • HA: High Availability
	Short description	There are lot of startups and SMEs that are active in the Fintech industry (where the financial services meet new technologies and business models) with an operational and business plan to develop and exploit cloud-based services to their customers and end-users. For this, most will consider procuring either IaaS or PaaS from respective CSPs that offer these cloud services, which will be used as a basis to develop, rely, and exploit their own PaaS respectively SaaS. This Use Case focuses on a Fintech company procuring IaaS from major IaaS CSP.
	Cloud Actors	IaaS CSP as vendor. Fintech Early Stage company as customer, with the intent to build and exploit their own SaaS to their own customers. In this use case these are financial institutions that wish their bank account holders to give access to said SaaS.
	Cloud Service life-cycle phase	Acquisition
	Legal and Data Protection compliance criteria	There are a number of steps that this Fintech Early Stage company takes before looking for appropriate IaaS CSPs, and finding and assessing the terms and conditions (including SLA) that may be applicable in the relationship between such IaaS CSP and the Fintech Early Stage company. Firstly, this Fintech Early Stage company (with founders and management with university degrees) maps the main legal compliance criteria it deems relevant in the initial phase. (1) The Fintech Early Stage company and its customer (bank) as well as its customers are based in The Netherlands. (2) Furthermore, the financial sector industry is high-regulated, including special requirements for vendors (including without limitation any CSPs), which include the right of the bank authority to be able to audit the vendors in the respective supply chain. (3) Personal data is involved, so the data protection regulation and legislation is applicable as well. These three main legal criteria are known to this Fintech Early Stage company. (4) Its prospective customers (banks) are known for their strict procurement, including information security requirements, and high level of expectation of service delivery. (5) There are no particular needs on IaaS, expect for that it should be relatively (a) cheap and (b) easy to develop, exploit and maintain its own SaaS on

		top of the IaaS of the selected CSP.
Preconditions and Requirements	**Security and privacy requirements**	The security requirements that are generally requested by prospective customers (banks) – to the extent known beforehand – and that are known to be common practice in the relevant market are taken into account.
	Additional preconditions and requirements (e.g., performance)	CSP Vendor pre-selection. After doing their internal desk research on the above, this Fintech Early Stage company starts with landscaping the results. Based on that it starts its pre-assessing of which IaaS CSP would be able to deliver, and on what conditions. With that, it will request proposals of the pre-selected CSPs.
	Existing standards and best practices to rely on	Neither the prospective customers (banks) nor the bank authorities have the standards or best practices that are commonly used. There is no FSI industry best practice available regarding cloud services. Bank authorities do not see it as their task to provide such standard, guidelines or the like.
	Additional comments	N/A
Summary	Without some reasonable assessment, it is impossible to procure cloud services. This basically goes for generally all procurement. However, it is especially relevant as there are many types of cloud services, services models, deployment models, and even in the right category there is a lot of variety in offerings and terms. This Use Case shows that without diligence and proper assessment and pre-selection landscaping, which could be a bit less comprehensive than in the Use Case described above, even a reasonably informed CSC is not able to start procuring the right cloud services	

4.2.2. Gov cloud

The following use case is based on ENISA's "Security Framework for Governmental Clouds" report [7], more specifically on the Estonian Governmental Cloud (Gov Cloud) which offers services to both citizens and Public Administrations based on a geographically distributed cloud infrastructure. The use case has been simplified in order to focus on its SLA-related aspects.

This use case is relevant to SLA-Ready given that the requirements of small Public Administrations provisioned by the Estonian Gov Cloud resemble those typically elicited by European SMEs.

Table 7 describes this use case in further details based on the proposed template.

Table 7. Small Public Administration customer of the Estonian Gov Cloud

Identification	**Title**	Small Public Administration using Governmental Cloud

	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • HA: High Availability • DI: Data Integrity
	Short description	In 2013, the Government of Estonia took the first steps to deploy a Gov Cloud with three main principles guiding its development: • Using Cloud solutions located within Estonia's national borders, • Using international private Cloud resources, and • Using Data Embassies (cloud storage). The Estonian government has built the foundation of a highly developed information society, and its ICT development has taken Estonia to a stage where many registers and services only exist in digital form. This development requires a flexible and secure Gov Cloud solution. Sufficient flexibility has to be planned in advance. The State Infocommunication Foundation leads the Gov-Cloud development, which is responsible for the consolidation of server resources and provision of high-quality server hosting services within Estonia's national borders. The Estonian Public Administration (PA) is the main cloud customer of the national Gov Cloud. In some cases PAs are provisioned with IaaS resources (e.g., virtual machines), but also PAs provision Gov cloud-based services to citizens. The Gov Cloud system does not store personal identifiable data.
	Cloud Actors	List of involved actors/stakeholders: • Cloud Service Providers, which provision their services to the Gov Cloud according to the requirements specified by the Cloud Owner (Estonian Government), and usually described on Service Level Agreements (SLA) and other contracts. • Cloud Service Customer: the Public Administrations using Gov Cloud services This use case defines an additional actor, namely the Gov Cloud Owner, which relates to the organization that legally owns the Gov Cloud and defines policies and requirements. The analysis of this use case considers that the Gov Cloud Owner is the actor offering an SLA to the cloud customers (PAs). The offered SLA already takes into account the capabilities from participant CSPs.
	Cloud Service life-cycle phase	This use case is based on the *Operation* phase of the Gov Cloud.

	Legal and Data Protection compliance criteria	The Gov Cloud does not manage any PII data from the citizens. Legal compliance criteria are defined b the Estonian Public Procurement Act[8].
Preconditions and Requirements	**Security and privacy requirements**	The following standards and best practices are being leveraged by the Estonian Gov Cloud: ISO 27001, ISO 27002, BSI IT, and the Estonian ISKE security framework. [8]
	Additional preconditions and requirements (e.g., performance)	High availability is a main concern in this use case, in order to guarantee continuous provision of PA services to the citizens.
	Existing SLA standards and best practices to rely on	Not applicable
	Additional comments	N/A
Summary	This use case focused on a Gov Cloud user (probably a small municipality), which is not a cloud-computing expert but nevertheless needs to make use of this technology. This use case is relevant to validate the CRM from a (small) Public Administration perspective, and shows a particular focus on functional requirements. Also, this use case takes into account the fact that this sector is particularly important for CSPs, therefore some degree of flexibility in their SLAs could be expected.	

4.2.3. SMEs using SaaS

This use case is based on ENISA's "Cloud Security Guide for SMEs" [9], in particular related to the example scenario shown in Annex A of the referenced report (i.e., "ConsulLess, SME using SaaS"). The relevance of this use case for SLA-Ready is based on its focus on security, and also on SLAs for SMEs that are transitioning to the cloud.

Table 8 further documents this use case.

Table 8. ConsulLess, SME for using SaaS

Identification	**Title**	ConsulLess, SME for using SaaS
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data • DI: Data Integrity
	Short description	From ENISA's report: "ConsultLess is a small consultancy firm in the EU that has 20 employees (mostly legal and management experts). One of the employees is partner and also the Chief Information Officer (CIO) of the firm. ConsultLess decides to procure office software as a service (SaaS) for use by its employees: the cloud service offers document storage/editing, email and calendar. This cloud service should replace an internal mail-server and

[8] Please refer to https://www.riigiteataja.ee/en/eli/509072014009/consolide

		office software installed on computers." Compliance is a critical factor in this use case. Furthermore, some (not all) of the data stored and processed is sensitive, and data leaks could have a severe impact on the reputation/business of the firm.
	Cloud Actors	List of involved actors/stakeholders: • Cloud Service Provider, which provisions the storage/editing, email and calendar SaaS to ConsultLess. This is a public CSP. • Cloud Service Customer, is the ConsultLess SME using the CSP SaaS.
	Cloud Service life-cycle phase	This use case focuses on the *Acquisition* stage of the public SaaS.
	Legal and Data Protection compliance criteria	Process of sensitive data by ConsultLess should be compliant with applicable EU legislations.
Preconditions and Requirements	**Security and privacy requirements**	The following security and privacy requirements apply to ConsultLess: • Physical security of the cloud assets should be guaranteed by the CSP. • Timely patching and updating, adequate backups, and security as a service are all required by ConsultLess. • The CSP should demonstrate compliance through those certifications required by ConsultLess. • ConsultLess wants to avoid vendor lock-in issues.
	Additional preconditions and requirements (e.g., performance)	ConsulLess is an established SMEs that currently provisions in-house the ICT services being procured from the public SaaS.
	Existing SLA standards and best practices to rely on	Not being SLA savvy, ConsultLess CIO relays on the C-SIG SLA Guidelines for procuring its SaaS.
	Additional comments	ConsultLess is not subject to any specific legal requirements about cross-border processing or data transfers.
Summary	This use case considers an SME cloud customer, therefore with some background experience on this technology, which is planning to use a new CSP (SaaS). This use case validates the CRM from the perspective of a SME familiarised with cloud computing, and with a particular focus on the security/privacy implications of this technology.	

4.2.4. SMEs migrating from one SaaS CSP to the other

This use case is based on several real life cases where a SME is using certain SaaS services, that at the time of procuring them were not felt to be that mission critical for the SME's business. Subsequently, it finds out that upon the plans made to shift from the existing SaaS CSP to a new SaaS CSP, the cloud services used and to be used have become mission critical for the survival and success of the SME.

Identification	**Title**	SME migrating from one SaaS CSP to the other
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data • DI: Data Integrity • HA: High Availability
	Short description	The SME is already using certain SaaS. At the time of procuring it, it was not felt to be sufficiently mission critical for the SME's business. Upon the plans made to shift from the existing SaaS CSP to a new SaaS CSP the cloud services used and to be used, the SME discovered that the use of this SaaS has become quite mission critical for the survival and success of the SME.
	Cloud Actors	The existing SaaS CSP as vendor, as well as the new SaaS CSP. SME as customer, with the intent to update and restructure the way the particular SaaS is used ad integrated in the organization of the SME.
	Cloud Service life-cycle phase	Termination & Consequences of Termination
	Legal and Data Protection compliance criteria	As quite common, the SME that is already using cloud services, in this case SaaS, finds out that when it wishes to change, amend or in this case terminate the respective cloud services it is bound by the standards terms and conditions of the CSP, including the SLA. To start with, the SME does not know which version of the terms and conditions it has accepted in the past (and the CSP generally does not know as well as per immature administration recording practices). Besides, most CSPs do not make or keep available the previous versions of its terms and conditions. In most cases, the CSP will refer to its recent standards terms and conditions of the CSP, applicable at the time of the request of the SME. So, regarding the first 14 of the 22+ CRM requirements, almost none are met automatically, meaning without the SME acting itself. This means that the SME has a huge disadvantage in terms of its legal position, negotiation power and has no alternative but to adhere to the terms and conditions provided by the CSP. Secondly, and regarding all 26 CRM requirements, the SME finds out that he does not have specific, tailored options beneficial for his needs to terminate the agreement with the CSP in a way that ascertain the business continuity of that SaaS, the assistance needed to migrate process flows, data (including metadata where necessary) to another SaaS CSP environment, and adequately and cost-effectively wind-down and discontinue the SaaS provided by the former CSP. In short, the former CSP is in full control, and the SME has a very weak bargaining position. It is a hard and expensive lessons-learned exercise for the SME, which

		intended to improve how it procures cloud services and follow the CRM where important for business and business continuity. Depending on the CSP the SME chooses, the SME may be able to succeed to some extent in these goals and approach, depending on the current immature nature of cloud SLAs and offerings of CSP. In any case, with the experience obtained and the CRM, the SME is now ready to make an informed decision what to choose.
Preconditions and Requirements	**Security and privacy requirements**	Non-applicable, as per this use case. However, the for this type of SME customary requirements has be taken into account while procuring the subsequent cloud services. No particulars to mention in this case.
	Additional preconditions and requirements (e.g., performance)	Non-applicable, as per this use case. However, for this type of SME customary preconditions and requirements have been taken into account while procuring the subsequent cloud services. No particulars to mention in this case.
	Existing SLA standards and best practices to rely on	Non-applicable, as per this use case. However, the for this type of SME customary best practices has been taken into account while procuring the subsequent cloud services. No particulars to mention in this case.
	Additional comments	N/A
Summary	**SMEs generally do not spend time or other resources on procuring cloud services, until they find out it is worthwhile to doing so.** This hampers their development and business opportunities, which SMEs find out when it may be too late already for them to change course, but it is also their moment to improve and pay more attention to procurement in general, and procuring cloud services in specific.	

4.2.5. CRM to use cases mapping

This section analyses the use cases described in the previous sections with respect to the CRM. Derived from the aforementioned analysis, we have found that some elements of the CRM are more important than others for some use cases. In general the priority between one element and another depends mostly on the domain in which the use case belongs to. The following represents the priorities of the CRM elements for every use case analyzed. A colour code is given, the “red” ones being the most important elements, followed by the “yellow”, and the “green” ones as being the less important. The level of importance given to elements of the CRM over others depends on the type of use case analyzed (including the type of domain, type of customers, the specific requirements for each use case, etc).

In the **Financial Sector (Fintech) use case** (Section 4.2.1), the CSC is considered to be at novice level. This means that the SME has no particular knowledge of what it needs, what cloud services are on the market, what and how to procure and how to execute or use

cloud services. It is fully new to them. However, this CSC does understand that it is important to do diligent internal desk research on the requirements and best practices, and to do reasonable assessment prior to procuring cloud services especially as its business will depend on it. Therefore, as mentioned above in Section 4.2.1 as well, this CSC finds the CRM Requirements 'Unilateral Change', 'Findable' and 'Choice of Law' as its top three most vital elements. This is because, the SLA is in place, it cannot therefore afford that the SLA is unilaterally changed by the CSP. In addition, it needs to be able to show its own customers the SLA of the IaaS CSP, as the services of this CSC are running on those IaaS cloud services. Furthermore, this CSC will not be able to 'resell' this IaaS together with its own services if the choice of law in the SLA is foreign or too unknown or uncomfortable for both the SME itself and its customers. This CSC wishes to build its business on IaaS, and after diligent assessment of what cloud services to procure it needs to be certain that the SLA cannot be changed to the detriment of its business or for its customers. From the SME's viewpoint the subsequent priorities to focus in the CRM therefore are 'Roles and responsibilities', SLA Duration', 'Contact Availability', 'SLA Change Notifications', and 'Services Level (Continuous) Reporting). Again, this CSC is at novice level, and is therefore basically most interested in these requirements, than the more technical and in-depth requirements which they are unable to assess due to a lack of knowledge.

The **Gov cloud use case** (please refer to Section 4.2.2) is a clear representative of the importance related to functional and non-functional requirements of Public Administrations (PA), where a clear definition of SLOs is expected from the CSP. Besides SLOs, Gov cloud customers may also expect clarity in aspects related to roles & responsibilities, along with a clear understanding of the definitions stated in the SLA.

Furthermore, PAs also expect an SLA where the CSP contact point's data is explicitly stated in order to streamline the resolution of potential technical and non-technical issues related to the cloud service/SLAs being agreed upon. Also considered as important (although with slightly less criticality than the CRM elements mentioned before), sections related to reporting/monitoring of service levels, credits, and documented exceptions/specials. In all these cases, the PA will also expect transparency although the relative importance of these elements may be perceived as lower than in the case of the SLO-related specifications.

Finally, in the case of the PAs our analysis found that some CRM elements may be taken for granted by the Gov cloud customer (e.g., choice of law, and language), or are expected to be provided under request by the CSP while procuring the cloud service (e.g., SLA URL and

findability). CRM elements like machine-readable versions of the SLA may not be considered as essential nowadays by PAs, although the mid-term adoption of new cloud features (e.g., automation and brokering) may disrupt such perceptions[9].

The SME view of the cloud SLA is slightly different (cf., Section 4.2.3 and 4.2.4).

In the case of **ConsultLess** (cf., Section 4.2.3), while the definition of relevant functional/non-functional SLOs is critical, other aspects related to definitions/changes/notifications are more of a priority. It is clear that more cloud transparency is a must for SMEs. This can be achieved through a clear specification of service levels and vocabularies.

CRM elements related to credits/CSP contact data/SLA revision are perceived as more critical for SMEs than for PAs, probably due to the different mechanisms both will use to procure cloud services (i.e., PAs may be procuring cloud services using brokers in the near future, therefore getting more negotiation potential than SMEs). Finally, a last group of non-so-critical CRM elements (ranked 21 – 30 in Table 9) is quite similar for both SMEs and PAs with the potential exception of SLA notification mechanisms and General SLOs. In such cases, SMEs still may not have the requirement of continuous SLA reporting/monitoring as PAs have.

Finally, for the **SMEs migrating from one SaaS CSP to the other** (Section 4.2.4), the CSC is at an experienced level from a practical point of view, even though the experience comes from previous procurement and usage carried out "on the job" and without any formal training. However, this CSC now understands that it is mission critical for the business. Therefore, as set above in Section 4.2.4 as well, this CSC finds the CRM Requirements 'Previous Versions and Revisions, 'Findable', 'Revision Date' and 'Contact Availability' as its top four most vital elements, as this CSC needs to find one of the previous versions in order to assess its rights & obligations. Without this, it cannot even start assessing the other CRM Requirements. Furthermore, in this use case this CSC is for obvious reasons particularly interested in 'Unilateral Change', 'SLA Change Notifications' and 'SLA Duration' as per the experience with its previous CSP. As this CSC is at a more experienced level, it is interested in and able to some extent assess the more technical and in-depth requirements being the SLOs (in particular 'Personal Data Protection', 'Security', Data Management' and General SLOs'.

[9] Please refer to EU FP7 Cloud for Europe Project. Online: http://www.cloudforeurope.eu/

Table 9. CRM - Use Cases Coverage

		CRM element importance for every use case (red: highest, yellow: medium, green: lowest)			
Item	**Name of CRM element**	**Financial sector**	**Small Public Administration using Governmental Cloud**	**ConsultLess, SME for using SaaS**	**SMEs migrating from one SaaS CSP to the other**
1	SLA URL				
2	Findable				
3	Choice of law				
4	Roles and responsibilities				
5	Cloud SLA definitions				
6	Revision date				
7	Update Frequency				
8	Previous versions and revisions				
9	SLA duration				
10	SLA language				
11	Machine-readable format				

		CRM element importance for every use case (red: highest, yellow: medium, green: lowest)			
Item	**Name of CRM element**	**Financial sector**	**Small Public Administration using Governmental Cloud**	**ConsultLess, SME for using SaaS**	**SMEs migrating from one SaaS CSP to the other**
12	Nr. of pages				
13	Contact details				
14	Contact availability				
15	Service Credit				
16	Service credits assignment				
17	Maximum service credits (Euro amount) provided by the CSP				
18	SLA change notifications				
19	Unilateral change				
20	Service Levels reporting				
21	Service Levels continuous reporting				
22	Feasibility of specials & customizations				
23	General Carveouts				

		CRM element importance for every use case (red: highest, yellow: medium, green: lowest)			
Item	**Name of CRM element**	**Financial sector**	**Small Public Administration using Governmental Cloud**	**ConsultLess, SME for using SaaS**	**SMEs migrating from one SaaS CSP to the other**
24	Specified SLO metrics				
25	General SLOs				
26	Cloud Service Performance SLOs				
27	Service Reliability SLOs				
28	Data Management SLOs				
29	Security SLOs				
30	Personal Data Protection SLOs				

5. *Progress on developing the SLA-Readiness Index*

The concept of the SLA-Readiness Index i.e., a high-level metric designed to assess a CSP alignment to the CRM, was first introduced in Deliverable 4.2 within the context of the envisioned SLA Marketplace. The rest of this section reports the progress related to the development of the SLA-Readiness Index, with a particular focus on the assessment criteria and the quantitative techniques that can be used to perform the computation of this metric.

5.1. Overview

During the early phase of the project and while designing the SLA-Repository (cf., Deliverables 2.1 and 2.2), the consortium realised that in order to provide comprehensive cloud SLA information to (prospective) cloud customers it was necessary to go beyond just offering a "raw" collection of SLAs. Therefore, the SLA-Repository has evolved to become a collection of cloud SLAs *analysed* according to the elements defined by the CRM (cf. Section 2). However, even in this case the resulting information could have become too granular for SMEs just willing to have a quick understanding of the offered CSP SLA before going into all involved details. For this reason, the project has proposed the SLA-Readiness Index: a high level metric that could be used by cloud customers to assess (at a glance) the CSP SLA.

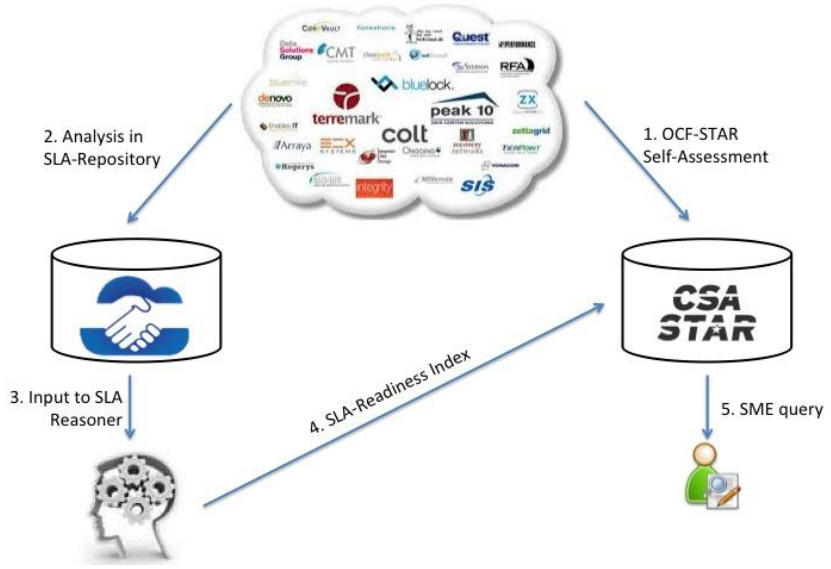


Figure 5. Computing the SLA-Readiness Index.

Figure 5 shows a high-level view of the proposed set of steps needed to compute and make publicly available the SLA-Readiness Index. The following sections presents in more details each one of the steps depicted in Figure 5.

5.1.1. Step 1: CSP SLA self-assessment

During this first stage the CSP is asked to perform the self-assessment of its SLA(s) based on the developed CRM. This initial step has two main goals:

1. Validate the usefulness of the CRM from the CSP perspective
2. Collect real-world SLA data for the SLA-Repository (along with the CSP approval for publishing that information).

In order for the CSP to analyse the CRM in such a way that the resulting information can be used to compute the SLA-Readiness Index (cf., Section 5.4), it is necessary to assign a qualitative/interval scale to each CRM element (e.g., a YES/NO answer). This approach has proved its usefulness in the development of cloud security repositories such as CSA STAR [17], where CSPs self-assess the implementation of security controls based on the Consensus Assessment Initiative Questionnaire (i.e., CSA CAIQ [16]).

The SLA-Ready consortium has developed a questionnaire for allowing CSPs to assess their SLAs based on the developed CRM. This questionnaire is shown in Annex B and will be used to compute the SLA-Readiness Index (to be detailed in D2.4). The results will be published in the SLA-Repository and then the CRM best-practices will be extracted (to be documented in D3.3 and D4.3).

5.1.2. Step 2: SLA-Repository

Once the CSPs have answered the questionnaire shown in Annex B, then it is feasible to store the CSPs data in a machine-readable format i.e., the SLA-Repository. The internal structure of the SLA-Repository will resemble that of the CRM as presented in Section 2 i.e., a hierarchy down to the level of elements which are evaluated based on the answers provided by the CSPs. Each entry can then be made publicly available so (prospective) cloud service customers can have access to it. As documented in D4.2, the SLA-Repository will be part of the SLA Hub[10].

By acknowledging the trade-offs associated with the SLA-Repository's usability and granularity (i.e., detailed information should not be the entry point for SMEs into the SLA-Repository), the consortium proposes the SLA-Readiness Index as presented next.

5.1.3. Step 3: Computing the SLA-Readiness Index

[10] Please refer to http://www.sla-ready.eu/creating-sla-repository

The CSP SLA information collected in the SLA-Repository is structured in a way that allows for its quantitative reasoning; in particular we refer to its *aggregation* as explained next. At the state of the art, there are some well-known methodologies that can be used to aggregate quantitative/qualitative metrics organised in a hierarchical structure in order to obtain a unique measure. These techniques will be reviewed in Section 5.6

By applying the same principle it can be possible to aggregate bottom-up (i.e., from the element to the Group level) the qualitative data compiled from the CSP questionnaires to result in a numeric value that is, the SLA-Readiness Index. This metric is proportional to the amount of positive answers provided by the CSPs to the questionnaire. For example, a CSP replying with more positive (i.e., YES) answers to the CRM will have a higher SLA-Readiness Index than another CSP that replied with more negative answers (i.e., NO). Furthermore, the numeric SLA-Readiness Index can be easily transformed into a qualitative metric where more SME-friendly labels can be associated to the SLAs e.g., Gold/Silver/Bronze. Deliverables D2.4 and D4.3 will further elaborate about the SLA-Readiness Index, by also presenting proof-of-concept computations.

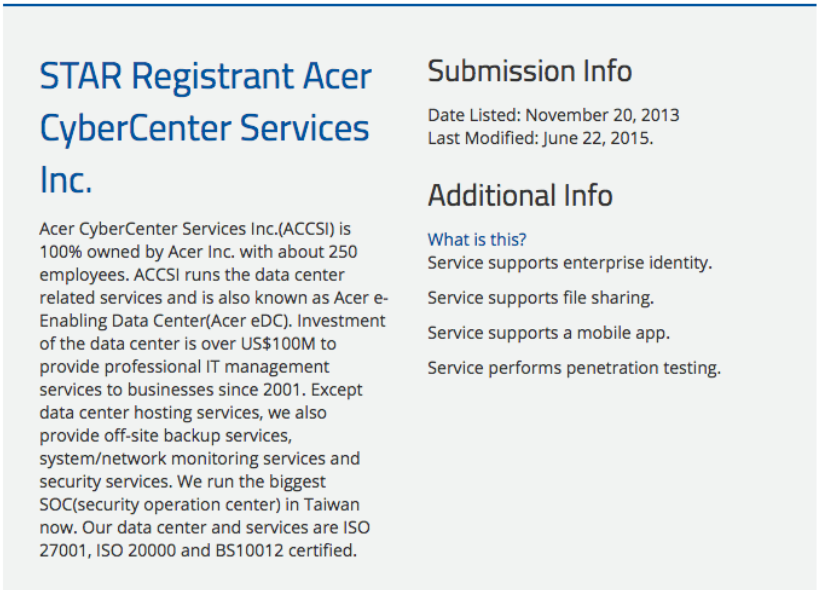


Figure 6 A CSP entry on CSA STAR - Additional Info

5.1.4. Step 4: Using the SLA-Readiness Index

The computed SLA-Readiness Index can be used as the *entry-point* to more detailed self-assessment data from the CSP (i.e., as stored into the SLA-Repository), by making it publicly available in the SLA Hub and the CSA STAR registry webpage. In the latter case, the SLA-Readiness Index information will become part of the CSP entry's Additional Information where the cloud service is further qualified, as seen in Figure 6 A CSP entry

on CSA STAR - Additional Info. More details associated to publishing the SLA-Readiness Index will be provided in D4.3

The following section analyses relevant state of the art related to the SLA-Readiness' computation (cf., Step 3 above).

5.2. SLA Evaluation: Initial context

The evaluation of the SLA-Readiness index depends on the assessment techniques that allow one to ascertain (qualitatively or quantitatively) how good or bad a CSP's SLA is with respect to customers' requirements and with respect to the SLAs of other CSPs.

However, there are only very limited techniques available to provide such an SLA assessment. This is indeed, as reported in D2.2, another impediment that customers encounter when they decide to migrate their key applications to the Cloud. Notwithstanding, several approaches are emerging aiming to evaluate the functionality and security of CSPs. We now briefly outline the state of the art in SLA assessments.

Li et al. [1] focuses on performance indicators to compare different CSPs. This approach is based on the active measurement of elastic computing, persistent storage and network services. To this end a set of metrics are created which are also used to evaluate the impact on the performance of the service.

The QoS of CSPs is evaluated by Garg et al [11] that uses the Analytic Hierarchy Process (AHP) to evaluate performance data and provide with a ranking. The technique is based on the Service Measurement Index (SMI) indicator as defined by the Cloud Service Measurement Index Consortium (CSMIC) [21]. The SMI consists of a set of business-relevant Key Performance Indicators (KPIs) that provide a standardized method for measuring and comparing a business service. This methodology uses these KPIs to create a set of metrics that are used to compare the providers. These KPIs are measured through the corresponding metrics by monitoring directly the system. The evaluation of these measurements is done by applying the Analytical Hierarchy Process (AHP) [19] that provides a ranking of the analysed providers.

Several activities are devoted to evaluate SLAs focused on security. Hegging [12] is probably the first initiative that introduced the term security in SLAs. Hegging defines a set of quantifiable security metrics that can be used to evaluate services

Although the previous references are interesting approaches to deal with the evaluation of SLAs, the following ones provides with a structured methodology based on a quantitative evaluation of the controls that comprise the SLA. Although these methodologies are mainly

focused on security controls, they can be easily translated to any set of controls included in a SLA as long as they can be quantified.

The following figure depicts the three progressive stages driving SLA assessment as:

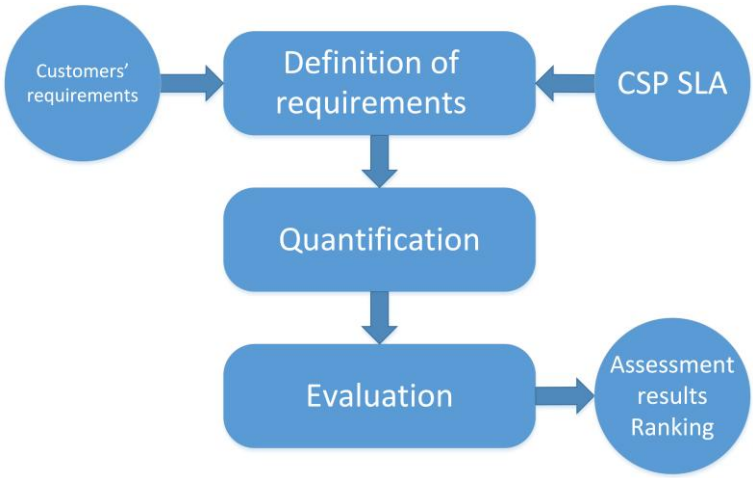


Figure 7. Stages comprising the quantitative SLA assessment

- **Definition of requirements:** In this stage both customers' requirements and CSP SLAs are expressed in a set of common elements (for example using the CSA CCM [13]). The most prominent characteristic of these elements is the hierarchical structure used to organize them. For example, a typical hierarchy used to evaluate SLAs is the one that combines the CSA CCM with the ISO/IEC 19086, which results in a three levels three (*categories, groups and SLOs as depicted in Figure 8*)

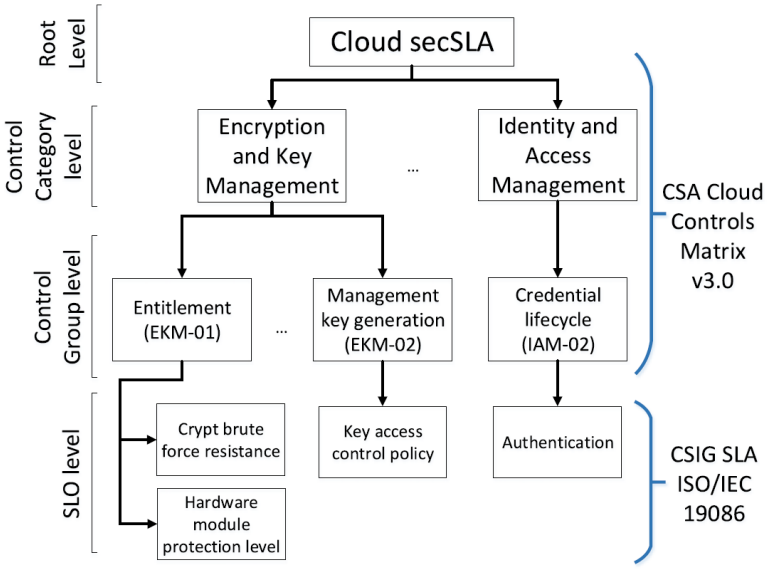


Figure 8. SLA hierarchy combining the CSA CCM and the ISO/IEC 19086

- **Quantification.** Each element of the previous stage is then quantitatively evaluated. The specific way to evaluate each element of the SLA depends on the concrete

methodology but the common denominator for all of them is based on the definition of all the possible service levels for each element. For example, an element of the SLA might be defined in such a way that it can only get two possible values (YES and NO or TRUE and FALSE). In this case the quantification would assign scores to each possible value (i.e., 1 to YES and 0 to NO). In the case of an element with more than one possible value (i.e., the cryptographic key length specified by 128, 256 and 512 bits), the scores would be given in the range of possible values (i.e., {0,1,2,3} for the {128, 256, 512} bits levels of the cryptographic key length example).

- **Evaluation.** This stage comprises the use of algorithms with the quantified elements of the SLA. The algorithms highly depend on the methodology used but all of them are based on the aggregation of the quantified elements of the SLA along with the hierarchy used to organize the elements of the SLA.

A very relevant evaluation methodology is the one presented by Luna et al. in [14]. This methodology (called Quantitative Policy Trees (QPT)) evaluates and compares security SLAs based on the CAIQ [16] structure and taken from the STAR repository [17]. The methodology is based on scores given to the elements of the SLA hierarchy according to the quantified values. The scores are calculated as the distance of the scores for the quantified level of an element for the CSP and for the customer, weighted with respect to the maximum quantification level for that element. The scores are calculated for every node of the tree and are aggregated towards the higher levels of the hierarchy till getting a global score. This methodology allows also to define basic dependencies between the lowest nodes of the hierarchy by using AND/OR rules in the aggregation process.

The QPT methodology is very related to the Reference Evaluation Methodology (REM)[18]. The definition of requirements and the quantification process is very similar to QPT. The main difference is in the evaluation process. In REM the quantification process leads to a set of matrices. The REM uses matrices arithmetic to calculate distances between matrices representing to SLAs of customers' requirements and CSPs.

The newest approach is the Quantitative Hierarchy Process (QHP) presented by Taha et al. in [13]. The proposed framework allows both basic and expert users to express their security requirements according to their expertise and specific needs by using qualitative requirements that can even be expressed in natural language. The quantification process is basically the same as the one used by QPT and REM. The algorithm to evaluate the SLA is based on the AHP for solving Multiple Criteria Decision Making (MCDM) [20] problems. The algorithm is also based on the aggregation of quantified controls all over the hierarchy. The aggregation is done by carrying out a pair-wise comparison between the (quantified)

elements of the SLA provided by all the CSPs that are to be compared. The result is a matrix whose Eigen vector is used to obtain the final score. The relevance of this methodology is that the pair-wise comparison can be done at any level of the hierarchy. Thus, the results can be obtained with different levels of granularity, depending on the depth of the analysis that is required. Such an analysis will be discussed further in D2.4

6. Conclusions

This report presents SLA-Ready's initial Common Reference Model based on the analysis of the requirements elicited in D2.1 and D2.2. Besides the definition of the Common Reference Model, D2.3 has compared it with respect to the current state of practice of different domains, including standards and industry.

From the analysis of the standardization domain we have assessed the CRM with the most dominant standards (ISO/IEC 19086, Cloud SLA checklist (from the SMART 2013/0039 Model SLA), Guide for Evaluating SLAs from the Cloud Standards Consumer Council), C-SIG Guidelines and ETSI's cloud SLA template). The outcome of this preliminary assessment is that most of the standards provide a good coverage of the technical elements of the CRM (namely SLO either for security, privacy and performance). However, the coverage of categories such as general and economic aspects is quite limited.

For the analysis of the industrial domain, we have used four use cases taken directly from real companies using/offering cloud services. In general, we have seen that the CRM is able to fulfil with the main needs of companies in what regards to the different aspects covered by the CRM. However, there is still a paucity of information published by companies in what regards to the elements of the CRM included in their terms of service. In order to improve this aspect, we have identified different priorities for the elements of the CRM, according to the type of use case analysed which, at the same time, has been classified using the five categories that the ETSI has defined for cloud services scenarios.

Finally, we have provided the first insights with respect to the approach to analyse the readiness of the SLAs with respect to the proposed CRM.

References

[1] Cloud Standards Customer Council. Practical Guide to Cloud Service Agreements – Version 2.0. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf, 2015.

[2] CSIG – Cloud Service Level Agreement Standardisation Guidelines. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines, 2014

[3] European Commission, "Standards terms and performance criteria in service level agreements for cloud computing services", [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/study-report-standards-terms-and-performances-criteria-service-level-agreements-cloud-computing, 2015

[4] ETSI, TR. 103 125 V1. 1.1: "CLOUD." *SLAs for Cloud services* (2012).

[5] International Organization for Standardization (ISO/IEC), "ISO/IEC 19086, Information Technology – cloud computing – Service level agreement (SLA) framework and terminology (Draft)," 2014.

[6] ETSI. "Cloud Standards Coordination. Final Report". 2013. [Online]. Available: http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf. 2013.

[7] ENISA. "Security Framework for Governmental Clouds". [Online]. Available: https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds, 2015.

[8] Riigi Infosüsteemi Amet. "Estonian Security System Overview". [Online]. Available: https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf. 2016

[9] ENISA. "Cloud Security Guide for SMEs". [Online]. Available: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes, 2015.

[10] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: Comparing public cloud providers," *IEEE Internet Computing*, vol.15, no. 2, pp. 50-53, March/April 2011, doi:10.1109/MIC.2011.36.

[11] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: A framework for comparing and ranking cloud services," In *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, pp. 210-218. IEEE, 2011.

[12] R. Henning, "Security SLAs: Quantifiable security for the enterprise?" in Proc. ACM Workshop New Security Paradigms, 1999, pp. 54–60.

[13] Cloud Security Alliance. Cloud controls matrix v3. [Online]. Available: https://cloudsecurityalliance.org/research/ccm/, 2015.

[14] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in Proc. IEEE Conference Trust, Security Privacy in Computing Communications, 2014, pp. 284–291.

[15] J. Luna, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in Proc. ACM Cloud Computing Security Workshop,

2012, pp. 103–112.
[16] Cloud Security Alliance, "Consensus Assessments Initiative (CAI) Questionnaire," 2012. [Online]. Available: https://cloudsecurityalliance.org/research/initiatives/ consensus- assessments- initiative/, 2011.
[17] Cloud Security Alliance, "The security, trust & Assurance registry (STAR)". [Online]. Available: https://cloudsecurityal- liance.org/star/, 2012.
[18] V. Casola, R. Preziosi, M. Rak, and L. Troiano, "A reference model for security level evaluation: Policy and fuzzy techniques," J. Universal Computing Science, vol. 11, no. 1, pp. 150–174, 2005.
[19] T. Saaty, "How to make a decision: The analytic hierarchy process," Eur. J. Operational Res., vol. 48, pp. 9–26, 1990.
[20] M. Zeleny, Multiple Criteria Decision Making. New York, NY, USA: McGraw Hill, 1982.
[21] C. S. M. I. C. (CSMIC), "SMI Framework," [Online]. Available: http://betawww.cloudcommons.com/servicemeasurementindex.

Annex A. Use Cases list (ETSI CSC)

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Setup Cloud Service	Create Service Template	A cloud service developer creates a template of a service that may later be used to create an instance of a service.	CSP, Cloud Service Partner
Acquisition	Setup Cloud Service	Create Service Offering	The lifecycle of a new service offering is initiated and publicized for potential subsequent: • Advertisement • Contract assignment • Provisioning • Monitoring • Update • Consumption • Deletion	CSP
Acquisition	Setup Cloud Service	Build Application and Package	Developer builds an application and package it for deployment on a cloud	CSP, Cloud Service Partner
Acquisition	Setup Cloud Service	Build Application in Cloud and Optionally Package	Develop an application and optionally package it using an application development environment on the Cloud.	CSP, Cloud Service Partner

[11] One or more of Cloud Service Provider (CSP), Cloud Service Customer (CSC) or Cloud Service Partner.

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Setup Cloud Service	Cloud developer makes application available from cloud infrastructure	ISV or application developer makes their application available as a service, by deploying the application on IaaS infrastructure of a cloud service provider	CSP, Cloud Service Partner
Acquisition	Setup Cloud Service	Deploy application to a PaaS cloud service	Application developer must prepare the application components and associated metadata and enable deployment to the PaaS platform offered by the cloud service provider	CSP, Cloud Service Partner
Acquisition	Setup Cloud Service	Automate deployment of test environments for applications	Application developer requires to test an application to determine the cause of a problem - requires the deployment of the application in an environment that matches the environment in which the problem was experienced	Cloud Service Partner
Acquisition	Setup Cloud Service	IDE driven cloud development, deployment and operation	The IDE driven cloud development, deployment and operation Use Case is based on the creation of new value-added services and how business processes are implemented and adapted to be deployed on the cloud. New services by SMEs have to be easily implemented and adapted for benefiting from the advantages of the Cloud. For developing the Value-Added Service, the Service Developer uses the OPTIMIS Programming Model and IDE for assisting him/her to make an efficient implementation for the Cloud. During this process, the Service Developer implements the service, focusing on the business logic of the service without worrying about the Cloud issues, and as result of this implementation, he/she obtain the Service Manifest and Service Images required for deploying the service in the Cloud. This information is provided to the Service Provider which uses the OPTIMIS toolkit to select the most appropriate Infrastructure Provider to deploy the service. Once the Value-added Service is deployed, the final users of the service can invoke the service, accessing directly to the deployed service VMs as another standard web service.	CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Setup Cloud Service	Okeanos (GRNET)	Okeanos is an open-source IaaS cloud software for the deployment of cloud services. The software is modular, comprising a number of components that can be deployed and exploited independently. Access to the services is through an intuitive user-friendly web interface and command line tools. It is currently being tested with beta release expected in spring 2013. Programmatically, it offers a set of dcoumented proprietary REST APIs and standard APIs like OpenStack Compute (Nova) and OpenStack Object Storage (swift compliant).	CSP, Cloud Service Partner
Acquisition	Setup Cloud Service	Finnish Cloud Software Programme (national cloud strategy)	It creates a new ecosystem that focuses on the most profitable cloud services for sustainable development while ensuring information security. The programme has applied the agile development methods of the software industry in collaboration with companies and research institutions. Client-centered approaches enable the rapid creation of added value services and flexible models of operation . The programme also proposes a set of "standard contract clauses", which can be offered for voluntary adoption for cloud service providers and customers and completed after risk analysis.	CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Setup Cloud Service	EGI Federated Cloud Task Force	Develop a 'blueprint' for EGI resource centres wishing to securely federate and share their local virtualised environments externally with collaborators as part of the production infrastructure. Ongoing efforts are centred around nine core capabilities required of a future EGI federated cloud. Implement interoperability across different cloud platforms. The core capabilities are virtual machine management, storage/data management, information discovery, accounting, monitoring, notification, federated authentication & authorisation infrastructure, virtual machine image sharing, brokering. The capabilities are currently implemented or being tested through resource provider test cases to cover all the necessary functionalities. EGI's Cloud Infrastructure Platform is based on the use of technical standards defining the interfaces and echange points between the services exposed to the public. The following cloud related standards are of key importance: OCCI as the universal and extensible interface description for the provisioning of virtualised computing resources; CDMI for describing the access interface to generic cloud storage resources (both block and object storage resources) and OVF as a declarative language for pre-packaged virtual server images and necessary contextualisation information. Several complementary standards are used to integrate with EGI's Core Infrastructure Platform: X.509v3-based federated authentication is used for safe and secure identification for services and end users; the Usage Resource is extensively used to account for resource usage (virtualised compute resources). The emerging TOSCA language is of interest for extending OVF with a richer deployment language across all cloud deployment levels (IaaS, PaaS, SaaS).	CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	End User to Cloud	Applications running on the cloud and accessed by end users	CSC CSP
Acquisition	Prepare & Procure Service	Enterprise to customer and employee	Applications running in the public cloud and accessed by employees and customers	CSC CSP
Acquisition	Prepare & Procure Service	Enterprise to Cloud	Cloud applications integrated with internal IT capabilities	CSC CSP
Acquisition	Prepare & Procure Service	Enterprise to Cloud to Enterprise	Cloud applications running in the public cloud and interoperating with partner applications (supply chain)	CSC CSP
Acquisition	Prepare & Procure Service	Private Cloud	A cloud hosted by an organization inside that organization's firewall.	CSC CSP
Acquisition	Prepare & Procure Service	Broker coordinated Hybrid Cloud	Multiple clouds work together, coordinated by a cloud broker that federates data, applications, user identity, security and other details.	CSC CSP
Acquisition	Prepare & Procure Service	Desktop as a Service	End users access the enterprise applications and data hosted in virtual desktops which are created within a DaaS server. The sales staff also can view customer information and marketing records on the enterprise website. The DaaS server interacts with traditional enterprise IT facilities to achieve many control tasks, for instance, authentication via AD enterprise server.	CSC CSP Cloud Service Partner
Acquisition	Prepare & Procure Service	Virtual desktop pool	Virtual desktop pool supports the distributed deployment model with the dynamic stretching of resources to consolidate queuing resource and desktop resources. Unified phone call dispatching and delivery and maintenance of the desktop can be achieved in an intensive way.	CSC CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	Mobile Cloud Apps development & deployment	A mobile cloud application can be developed by service partners, or by the cloud provider, or by third-party service provider and can be stored in a marketplace. The mobile cloud application sends processing tasks to the cloud and stores data in the cloud, and receives results generated by the resources from the cloud, including computing resources and storage sources.	CSC CSP Cloud Service Partner
Acquisition	Prepare & Procure Service	Telco uses Cloud for data analytics	Large-scale telecom operators generate a lot of information in the normal course of running their communication networks. Typical data comprises Call Data Records (CDR) and Internet-surfing data records (IDR). In addition the network also generates various signalling data between switches and nodes. We need all the data to complete the telecom services and bill customers. At the same time, we also need them to analyze and predict user behaviour, optimize network QoS, filter spam messages, and so forth. Because of the limitations of the current system, the parallel data inquiry and mining tool, set on the cloud distributed parallel processing systems could be a better solution and achieve massive scalability and high-speed processing .	CSP Cloud Service Partner
Acquisition	Prepare & Procure Service	SLA mapping between ISB (inter-cloud service broker) and CSP	CSP-ISB is the contact point for CSU, and there is SLA (SLA0) between them. CSP-ISB integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are B2B level SLA between CSP-ISB and CSP-1, CSP-2 respectively (SLA1, SLA2). For CSP-ISB, in order to guarantee SLA0 for CSU, it needs to map SLA0 to SLA1 and SLA2, because SLA0 is actually implemented by SLA1 and SLA2.	CSP Cloud Service Partner
Acquisition	Prepare & Procure Service	Contracting guaranteed performance regarding delay	CSP-ISB is the contact point for Cloud Service User (CSU), and there is SLA (SLA0) between them. CSP-ISB integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are B2B level SLA between CSP-ISB and CSP-1, CSP-2	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	Citizen centric one-stop service	The e-application service provided by City A has been pre-arranged to allow interaction with other provider's services (e.g., family registry management service in a municipality cloud, passport management service of the national government, etc.) by negotiating the methods for coordinating ID information and security measures. A citizen in City A applies for his or her passport using the relevant e-application service provided by the municipality A. When he or she has entered required information, such as his or her identity information, the input data is transferred to other cloud system's services (e.g., family registry management service, passport management service, etc.) to authenticate, sharing user ID information entered for application, then information acquisition and inquiry take place. The results of the interacted services are provided to the consumer. Thus, the consumer can receive a one-stop service, which enhances his/her convenience.	CSC CSP
Acquisition	Prepare & Procure Service	Market transactions via brokers	When a consumer wants to uses services provided by cloud systems, he or she needs to compare his or her quality requirements for the services with the SLAs of multiple providers, and to select the most appropriate provider. For this purpose, the consumer provides Broker A with information about his or her quality requirements for services. By receiving information provided by Broker A, that Provider B provides an SLA that best meets the quality requirements of consumer, consumer can use services with best fit to his or her quality requirement. The consumer selects a cloud provider included in the provider list provided by broker, and contracts with Provider B.	CSC CSP Cloud Service Partner
Acquisition	Prepare & Procure Service	Establish Relationship	A potential consumer of a cloud-based service establishes their identity with a cloud service provider for use in future transactions.	CSC CSP

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	Administer Relationship	A potential consumer of a cloud-based service requests administration of a contract. Administration is distinguished from changing a service because administration does not affect the technical delivery of a service. Usually, contract administration involves actions like adding new users or changing user passwords that are associated with an umbrella contract (usually called the "relationship"), not a contract for a specific service.	CSC CSP
Acquisition	Prepare & Procure Service	Establish Service Contract	A potential consumer of a cloud-based service requests a service contract for a cloud-based service.	CSC CSP
Acquisition	Prepare & Procure Service	Update Service Contract	A consumer of a cloud service contract and a provider of a cloud service contract agree to update the contract.	CSC CSP
Acquisition	Prepare & Procure Service	Add Subscriber	The consumer enters into a business relationship with the provider to enable it to use an agreed to set a cloud service.	
Acquisition	Prepare & Procure Service	Create cloud application with components that run on multiple clouds	An organization chooses to develop a cloud application with components that run on multiple clouds simultaneously.	CSP, Cloud Service Partner
Acquisition	Prepare & Procure Service	Customers can "shop around" for cloud services	Customers and developers shop across hosted or public cloud searching for services offering adequate price and the desired level of non-functional properties like performance, security, availability, expressed via Service Level Agreements (SLAs)/certificates.	CSC
Acquisition	Prepare & Procure Service	Material Distribution to Agents	A global insurance company named "ABC" uses manuals and videos to teach the company's agents and affiliates about their new life insurance product. The company distributes the educational materials through the company's PDAs assigned to every agent considering mobile characteristics of their work. The use case describes technical processes	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
			and considerations to distribute company's educational material for new product to their agents. A correct version of the material among three different versions should be delivered to agents in a qualified VO group with an auditable access control mechanism that enforces the company's security policies.	
Acquisition	Prepare & Procure Service	cloud storage as a service	Customer uses public cloud storage as a service offering to store ever-increasing volumes of data as an alternative to adding to on-premise storage infrastructure	CSC
Acquisition	Prepare & Procure Service	Provision of Database capabilities as a cloud service	Customer wants to use a Database as a Service capabilities with ability to upload database images containing data and configuration information.	CSC
Acquisition	Prepare & Procure Service	Provision of big data analytics platform	Cloud service provider provides a dedicated Hadoop cluster as a service platform for big data analytics	CSP
Acquisition	Prepare & Procure Service	Cloud Brokerage	The Cloud broker offers *cloud service intermediation* for services to add value-addition and *cloud service aggregation* bringing two or more cloud based services. The Cloud Brokerage use case brings out the following innovations/value to the Cloud ecosystem. A) provide support for multi-cloud deployment B) provide standards-based SLA negotiation and agreement mechanisms to allow the broker to perform a match between the requirements of the C) Allows the broker to make SP-IP matches based on the Trust, risk, eco-efficiency and cost. D) The service deployment takes into account the legal bounderies as contraints in the service manifest. E) The cloud broker provides a framework to provide variety of value added services to the SP. Some the existing valued added sevices implemented as a supoort for the service includes, VPN overlay, Intelligent Protection system and Secure data storage. F) The cloud broker	CSC, CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
			allows deployment of service in the non-optimis IP, providing interoperability support.	
Acquisition	Prepare & Procure Service	goBerlin	The focus of goBerlin is the provisioning of a service marketplace combining commercial services and public governmental services to state-of-the-art applications with personalised SaaS for administrative matters (e.g. birth, marriage, children). The architecture is a loosely coupled combination of functional and security related aspects, e.g. access control, privacy, multi-tenancy. It can be applied to other cloud services running in similar cloud infrastructures, operated by public data centres.	CSC, CSP, Cloud Service Partner
Acquisition	Prepare & Procure Service	Bioinformatics - BLAST and BLAT tools for sequence mapping	Provide a framework for the seamless execution of widely used bioinformatics tools in the VENUS-C cloud (IaaS, PaaS), easing migration across target platforms (commercial and non-commercial providers). The aim of the VENUS-C user scenari on on bioinformatics (Technical University of Valencia) was to address the challenges faced by biomedical researchers in coping with the exponential growth of annotated databases and increases in the throughput of sequencing. The overall objective was to wrap different processing tools (e.g. for alignment and phylogeny) in a user-friendly framework running in the cloud. Migration across target platforms is ensured by implementation of standards, e.g. OGF-BES, OCCI, OVF, CDMI. Cost-effectiveness, flexibility and scalability over grid infrastructures have been demonstrated.	CSC, CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	Wildfire: Fire Risk Estimation and Fire Propagation	Provide a framework to execute fire risk estimations and fire propagation models, enabling end-user actors (e.g. fire-fighters, emergency crews and civil protection authorities) to run the models in the cloud using a user-friendly web-based graphical user interface. The aim of the VENUS-C user scenario, Wildfire (University of the Aegean) was to provide a tool for calculating fire risk indexes (hourly and over 5 days) and the expected propagation, using weather forecasts (including the direction of the wind), topography, vegetation and socio-economic parameters. It uses a hybrid cloud approach (MS Azure and OpenNebula via the Engineering Group) and has been tested and used by fire-fighting crews in Greece, who can respond to different workload situations; e.g. unpredictable and/or predictable bursting of CPU needs during the summer period.	CSC, CSP, Cloud Service Partner
Acquisition	Prepare & Procure Service	Radiotherapy planning (CloudERT pilot deployment in Spain)	Provide an eIMRT platform with remote tools to facilitate physicians in defining cancer treatment plans and verification using Monte Carlo simulations. Generate a single virtual cluster for each request to move the computing back-end to the cloud, which ensures independent processing for each request. The VENUS-C pilot, CloudERT, is led by the Centre of Supercomputing of Galicia (CESGA). It is aimed at improving hospital planning for cancer treatment with a pilot deployment in Spain, which currently involves 65 users from 47 hospitals. The eIRMT platform has been analysed from the point of view of SaaS, which must scale to thousands of users and service requests every day. It leverages the cloud to overcome the limitations of local clusters, which increase time-to-solution and decrease QoS, and of the grid, due to task grouping and the movement of large files.	CSC, CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Acquisition	Prepare & Procure Service	Drug Discovery service by Molplex (SME)	Provide a framework to calculate molecular virtual profiles that include shape/docking characteristics and QSAR biological activity predictions. The shape/docking calculation offers an embarrassingly parallel execution model, and has been parallelised with the use of OpenMP threads. Molplex requires regular access to computer resources to calculate the virtual profiles of molecules. The aim of the Molplex pilot (Cloud Against Diseases) in VENUS-C is to boost the performance of the comany's systems and reduce costs by allocating computing resources as needed. The virtual profiles are calculated using two techniques: shape/docking profile and QSAR profile. The deployment of former is supported by the Barcelona Supercomputing Center via the COMPSS interface, while part of the QSAR application is deployed on Azure using a legacy system from Newcastle University. Being able to solve a higher number of scientific problems (virtual profiling) gives the SME better market exposure and opportunities, as well as increase staff productivity.	CSC, CSP, Cloud Service Partner
Acquisition	Prepare & Procure Service	Cloud4SOA (FP7 project)	Interconnect public and private platform vendors for developers to help compare, manage and migrate between vendors by offering an open-source added value feature set for PaaS customers (developers and SaaS providers). Cloud4SOA interconnects platforms for added-value capabilities such as multi-platform management, comparative monitoring and application portability across collaborating or competing offerings. It prepares for the wider potential as the PaaS segment of cloud computing evolves, pointing towards concepts such as federation of multiple platforms and management between hybrid use cases of public and private PaaS. It leverages existing PaaS APIs and brings a harmonised layer and adapters to support its advanced features. Standardisation focuses on basic management protocols to enable platforms to focus on innovative	CSC, CSP, Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
			concepts and ecosystem-empowered capabilities.	
Operation	Operate Service - Manage	Guaranteeing performance against an abrupt increase of the load	• A CSP guarantees its service performance, even when an unexpected surge of access to the service arises, by using cloud resources provided by other CSPs on a temporary basis. • Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user ID, user data, and application data are transferred from the original CSP to the CSP that is leasing the resources. • Access from CSUs is appropriately changed to the interworking CSPs so as to achieve load distribution, and thus mitigate the overload of the original CSP.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Guaranteeing availability in the event of a disaster or a large-scale failure	• CSPs continue their service offering by the resources leased from each other, even when systems in one CSP are damaged due to natural disasters or large-scale failures. • Available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. • The services with a high priority are only recovered if available resources are not enough to recover all services. In examining the availability of the resources given from other CSPs, the guaranteed level	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
			of quality of the resources is taken into account. • The services requiring early recovery are recovered using available resources on a best-effort basis even if their quality requirements are partly satisfied. • Network connections among interworking CSPs are instantaneously established or reconfigured. The lead CSP, which is preconfigured and governs the recovery procedure, manages the roles of available CSPs and instructs service continuation based on the original CSP data. • Access from CSUs is appropriately distributed to the interworking CSPs so as to achieve the disaster recovery, and thus mitigate the service discontinuity.	
Operation	Operate Service - Manage	Service continuity	• A CSP continues its service offering by the collaboration with other CSPs, even when the original CSP terminates its business. • Available resources in CSPs other than the service-terminating CSP are discovered and reserved in advance. • Network connections among interworking CSPs are established or reconfigured. Then service-related data including user ID, user data and, application data are transferred from the original CSP to new CSPs. • Access from CSUs is appropriately changed to the interworking CSPs so that the same service is continuously offered. • If the capabilities (VM and applications) at the original CSP migrate to other CSPs, the CSU, who keeps the same user ID, can continuously access the service at the same level of performances as before.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Market transactions via brokers	• The CSP with an ISB role (CSP-ISB) mediates between CSPs meeting the CSU's quality requirements and provides the list of selected CSPs to the CSU. • The CSP-ISB coordinates multiple services offered by other CSPs	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Manage	Guaranteed end-to-end quality of service Guaranteed performance	Use case of guaranteeing performance against a abrupt increase of the load	CSP Cloud Service Partner
Operation	Operate Service - Manage	Guaranteed end-to-end quality of service Guaranteed availability	Use case of guaranteeing availability in the event of a disaster or a large-scale failure	CSP Cloud Service Partner
Operation	Operate Service - Manage	Service continuity by pre-configuration of alternative services	Normally, if the business of Provider A is suspended, the consumers need to re-register with similar services that are provided by different providers. To avoid a situation above, resources, applications, and consumer's ID data for the services provided by Provider A are transferred to the cloud systems of Providers B and C in advance. Then, in the situation of the business suspension of Provider A, its consumers can continue to use similar services provided by Providers B and C. This arrangement can also be applied when a service consumer requests a transfer of his or her service to another provider.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Contract Billing	A cloud service provider issues an invoice for contracted or consumed services.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Change Resource Capacity	A cloud service consumer adds or changes the capacity or resources associated with a service instance, which is an instance of a service template. This can include adding or removing whole resources, or expanding or contracting resource limits associated with the service.	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Manage	Hibernate/Resume	Puts a running application into hibernation. Resume a hibernating application.	CSC
Operation	Operate Service - Manage	Stop/Restart	Stop a running application and create a “snapshot”. Resume from a snapshot.	CSC
Operation	Operate Service - Manage	Patch	Patch (update) one or more components in an application template.	CSC
Operation	Operate Service - Manage	Create Network	The cloud consumer wishes to create a new instance of a “network”. A network is an abstraction of a layer 2 broadcast domain. Any two nodes (machines, volumes, etc.) attached to the same network can connect to one another. To connect to a node on another network a route must be created between the source network and the destination network. A common reason for creating networks is to isolate machines and volumes into protected sub-domains for security and administration purposes.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Cloud application workload requires use of multiple clouds (cloudburst)	Sometimes referred to as a cloudburst scenario, the application normally running onpremises or in a private cloud needs to elastically run on other clouds in the cases of short-term, significant increase in user demand load. Cloud tenants can use both their own private clouds as well as hosted/public clouds as the workload may require. VMs and applications can migrate between private cloud and public/hosted clouds and can seamlessly be managed from either side regardless of their location.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Document release towards an administration	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. The use case describes how a	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
			public administration requests a document from a citizen in the course of an administrative process.	
Operation	Operate Service - Manage	Burst Capacity	A system or service runs in a defined "source" location, and bursts into an alternate location or cloud environment such as a shared or public cloud (target) to obtain additional resources to accommodate business peak processing requirements. Requires license flexibility, and sufficient network and security controls.	CSP Cloud Service Partner
Operation	Operate Service - Manage	Integration of on-premise resources with public cloud resources	Cloud service customer makes use of public cloud IaaS resources for some workloads but still has other workloads retained on-premise, with the need to link the on-premise workloads and the public cloud workloads	CSC
Operation	Operate Service - Provision/Configure/Administer	Provision Resources (from a contracted pool)	Within the context of an existing contract, an administrator allocates resources from the contracted pool. The resources could be of a wide variety, such as virtual system platforms or a preconfigured mini data center that contains virtual systems and virtual storage, connected via a virtual network.	CSC
Operation	Operate Service - Provision/Configure/Administer	Deploy Service Template	A cloud service consumer deploys a parameterized service template in the context of a service offering.	CSC
Operation	Operate Service - Provision/Configure/Administer	Provision New Administration Domain (or Provision New Tenant)	Subscriber administrator is provisioned with a new administration domain.	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Provision/Configure/Administer	Add/Change/Delete User	A cloud consumer administrator adds or removed user, or changes their privileges.	CSC
Operation	Operate Service - Provision/Configure/Administer	Install Application Component	A new application component is uploaded and installed to the cloud.	CSC
Operation	Operate Service - Provision/Configure/Administer	Deploy Application (also Undeploy)	To deploy a package comprising all the required application components to an execution domain.	CSC
Operation	Operate Service - Provision/Configure/Administer	Start an application	To start executing an application such that end-user may start interacting with the hosted applications.	CSC
Operation	Operate Service - Provision/Configure/Administer	Upload Machine Image	The cloud user or third party software provider has a local copy of a "machine image" (a snapshot of a stack of software which may include operating systems, virtual machine runtimes, database servers, application servers, applications, etc.) that they wish to make available for deployment on an IaaS cloud.	CSC
Operation	Operate Service - Provision/Configure/Administer	Deploy Machine Image	The cloud consumer wishes to create a new instance of a "machine" (a logical instance of one or more CPUs connected to local memory and, optionally, local data storage) with software loaded from a machine image.	CSC
Operation	Operate Service - Provision/Configure/Administer	Capture Existing Machine Instance	The cloud consumer wishes to create a new machine image that captures the state of an existing virtual machine instance.	CSC
Operation	Operate Service - Provision/Configure/Administer	Create Persistent Storage Volume	The cloud consumer wishes to create a new storage volume image that captures the information stored on an existing volume instance.	CSC
Operation	Operate Service - Provision/Configure/Administer	Load Image onto Storage Volume	The cloud consumer wishes to load a "volume image" (e.g. an ISO image) onto an existing persistent storage volume.	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Provision/Configure/Administer	Attach Storage Volume to Machine	The cloud consumer wishes to attach a persistent storage volume to a machine instance. Once attached, the volume is accessible by processes resident on that machine instance, usually as a local device (e.g. /dev/sd2).	CSC
Operation	Operate Service - Provision/Configure/Administer	Capture Storage Image	The cloud consumer wishes to create a new storage image that captures the information stored on an existing storage image.	CSC
Operation	Operate Service - Provision/Configure/Administer	Detach Storage Volume from Machine	The Cloud User wishes to detach a persistent storage volume from a machine instance. Once detached, the volume is no longer accessible by the processes resident on that machine.	CSC
Operation	Operate Service - Provision/Configure/Administer	Attach Machine to Network	The cloud consumer wishes to attach a machine to a network. The higher level goal is to allow this machine to connect to one or more of the other machines or volumes on the target network and/or to allow one or more machines on the target network to connect to this machine.	CSC
Operation	Operate Service - Provision/Configure/Administer	Detach Machine from Network	The Cloud User wishes to detach a machine from a network. This is usually a step in a higher-level network management process such as “attach this machine to the back-end, database network and detach it from the default network”.	CSC
Operation	Operate Service - Provision/Configure/Administer	Attach Storage Volume to Network	The Cloud User wishes to attach a volume to a network. The higher level goal is to allow this volume to be attached to one or more of the machines on the target network (see Attach Storage Volume to Machine).	CSC
Operation	Operate Service - Provision/Configure/Administer	Detach Storage Volume from Network	The cloud consumer wishes to detach a volume from a network. This is usually a step in a higher-level network management process such as “attach this volume to the back-end, database network and detach it from the default network”.	CSC
Operation	Operate Service - Provision/Configure/Administer	Onboarding for VEM	Onboarding of a customers applications to IaaS service	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Monitor	SLA Reporting	A cloud service consumer requests and receives a report about an established service contract.	CSC CSP Cloud Service Partner
Operation	Operate Service - Monitor	Monitor Service Resources	A cloud consumer configures a monitor for a deployed service instance and resources that support the service instance. A monitor may collect data (for example, resource consumption, throughput, response times, or availability) or establish an exception threshold.	CSC CSP Cloud Service Partner
Operation	Operate Service - Monitor	Notification of Service Condition or Event	A service has been configured and is in operation. Certain conditions or runtime operational events have been identified or detected that are significant enough to demand immediate notification of the condition or event to the service customer. An example is the detection of an intrusion or an unexpected configuration change.	CSC CSP Cloud Service Partner
Operation	Operate Service - Monitor	Monitoring & management of deployed software	Monitor the health of infrastructure & perform capacity planning for future needs	CSC CSP Cloud Service Partner
Operation	Operate Service - Migrate	Changing Cloud Vendors	An organization using cloud services decides to switch cloud providers or work with additional providers.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Move three-tier application from on-premises to cloud	An organization moves a three-tier application (front-end web server, back-end database, and middle-tier business logic) from an on-premises data center to a cloud infrastructure provider that will run the application off-premises. Platform services for data, identity and access are considered available for source and target clouds but not addressed in this case. This use case represents the most common type of web-based application deployed both in enterprises and mid-sized companies	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Migrate	Move three-tier cloud application to another cloud	An organization moves a three-tier application from one cloud infrastructure provider to another.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Move part of on-premises application to cloud to create "hybrid" application	An organization moves one or more parts – or tiers – of an on-premises application to the cloud, in order to separate data storage from processing, for example. This creates a cloud that is a hybrid of both public (off-premises) and private (on-premises) clouds.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Hybrid cloud application that uses platform services	An organization moves one or more parts – or tiers – of an on-premises application to the cloud and chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider, such as structured or unstructured cloud storage or identity and access control services.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Port cloud application that uses platform services to another cloud	Porting an application that uses services provided by the cloud platform to another cloud platform implies these requirements: 1) bulk import/export of customer data, and 2) Semantic cloud application management protocol.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Capture Aggregate Assembly	The cloud consumer wishes to capture an aggregate assembly consisting of zero or more machine instances, zero or more volume instances, zero or more network instances, and the attachments/connections between these entities. The artifacts generated by this capture operation (the "assembly package") can be used to deploy "a copy" of the assembly onto this or some other cloud.	CSC

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Migrate	Upload Aggregate Assembly	The cloud consumer or third party software provider has a local copy of an assembly package which includes zero or more machine images along with metadata that describes the machines on which these images must be deployed, zero or more volume images along with metadata that describes the volumes on which these images must be deployed, zero or more descriptions of network instances, and a map of the attachments/connections between these entities. The Cloud consumer or third party software provider wishes to make this assembly available for deployment on an IaaS cloud.	CSC
Operation	Operate Service - Migrate	Deploy Aggregate Assembly	The cloud consumer wishes to deploy an aggregate assembly consisting of zero or more machine instances, zero or more volume instances, zero or more network instances, and the attachments/connections between these entities for the purposes of re-creating the system that was captured in IR01.25 (Capture Aggregate Assembly).	CSC
Operation	Operate Service - Migrate	Move three-tier application from on-premises to cloud	An organization (customer) moves a three-tier application from an on-premises datacenter to a cloud infrastructure provider that will run the application off-premises. The data associated with the application is sensitive and confidential and it is necessary to assure its integrity. Issues to be considered include: • suitable SLA/certificate, • responsibility for the provision and application of encryption, • key management processes • data validation • etc…	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Operation	Operate Service - Migrate	Move three-tier cloud application to another cloud	An organization (customer) moves a three-tier application from one cloud infrastructure provider 1 to another provider 2.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Move part of on-premises application to cloud to create “hybrid” application	An organization (customer) moves one or more parts – or tiers – of an on-premises application to the cloud, in order to separate data storage from processing, for example. This creates a cloud that is a hybrid of both public (off-premises) and private (on-premises) clouds.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Hybrid application with shared user ID and access services	This use case is the same as the use case "Move part of on-premises application to cloud to create 'hybrid' application" with the added condition that user ID and access are shared between on-premises and cloud components. This requires a common user ID and access control methodology between components based on either on-premises directory access or identity federation.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Move hybrid application to another cloud with common infrastructures	An organization (customer) moves the cloud portions of a hybrid application from cloud A to cloud B, both of which support common infrastructures and VM packages.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Hybrid cloud application that uses platform services	This use case is similar to the use case "Move part of on-premises application to cloud to create 'hybrid' application" except the cloud application developer in this case chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider, such as structured or unstructured cloud storage or identity and access control services.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Port cloud application that uses platform	Porting an application that uses services provided by the cloud platform to another cloud platform implies the same requirements as for the use case "Hybrid cloud application that uses platform services".	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
		services to another cloud		
Operation	Operate Service - Migrate	Cloud Burst	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. To reduce its own operational costs, the EDS provider decides to accept an IaaS offer from another Cloud provider and use its virtualized resourced to provide the EDS service.	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Document Migration	An Electronic Document Storage (EDS) is a secure storage for official documents provided as SaaS. Governmental institutions or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedures. The use case describes how a public administration requests a document from a citizen in the course of an administrative process. The use case describes the migration process of documents from one EDS (EDS 1) hosted by EDS space provider A into another one (EDS 2) (hosted by provider B):	CSP Cloud Service Partner
Operation	Operate Service - Migrate	Project Capacity	Temporary capacity from an alternate cloud (public or shared private) to support short term initiatives	CSP Cloud Service Partner
Termination	Operate Service - Terminate	Terminate Service Contract	A consumer of a cloud service contract and a provider of a cloud service contract agree to terminate a cloud service contract.	CSC CSP

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[11]
Termination	Operate Service - Terminate	Terminating cloud contract	An organization (cloud service customer) obtaining a cloud service from a cloud service provider directly or via a cloud service partner (a broker) would like to terminate its contract. There can be many reasons for doing so, for example the organization would like to changing cloud service provider of partner or wants exiting the cloud and move to a non-cloud environment. The use case is focusing on the terms and conditions that should be in a SLA, and the enforceability of those terms and conditions to do so.	CSC CSP Cloud Service Partner
Operation	Assure Quality - Audit Service	Independent third party assurance	Establishing an independent third party assurance (a regulator) to build trust whereby European SME's and other organizations (cloud service customers) will use cloud computing services more An independent third party assurance can contribute to building trust whereby European SME's and other organizations will use cloud computing services more. The idea is to establish a kind of active and pro active escrow service (a regulator role) by a third party in such a way that this party can assure a seamless takeover of the cloud operations that provider A executes for a user to cloud provider B. This should therefore include the (functionality of the) software, the users' data and the current state of transactions.	Cloud Service Partner

Annex B. CRM questionnaire for CSPs

Do you need to sign a Cloud SLA & you want to find everything you need, in the one place to make sure what you sign has the right: vocabularies, SLO metrics/measurements, and compliance with standards/best practices? Well this **May 2016**, the European project SLA-Ready[12] has developed precisely all of these features in its **Common Reference Model *(aka CRM)***. This CRM hopes to make European SMEs' life easier in sifting through time-consuming legal contracts for the uptake of cloud computing.

In order to validate the developed CRM[13] from your perspective, we kindly ask you to answer the following set of questions.

1. Information about the participant's profile:
   a) Which one of the following roles best describes your Cloud computing activity? *(Please tick just one answer)*
      [ ] Cloud Service Provider or CSP (e.g. CxO, R&D, etc).
      [ ] Cloud Service Partner (e.g. security auditor, Cloud broker, developer)

   b) Which industrial sector is your main cloud service customer?
      [ ] Small and Medium-sized Enterprise (SME, private sector)
      [ ] Non-SME (private sector)
      [ ] Public sector

[12] Please refer to http://www.sla-ready.eu/

[13] CRM follows a 3-level hierarchical structure: the top level contains eight (8) *groups*, organize thirty (30) *elements* that include the main notions that can be mapped to the different aspects of cloud SLAs. Following the ISO/IEC terminology, the lowest level comprises the *components* that are part of the service level objectives (SLO) related elements of the CRM.

c) Which market vertical best describes your cloud service customer base? *(Please tick just one answer)*

[ ] Education

[ ] Financial Services

[ ] Government

[ ] Information Technology (IT) & Telecommunications

[ ] Other (please specify): _____

d) How well the following high-level use cases[14] describe the interests of your cloud service customers? *(Please rank from 1 (better) to 5 (worst))*

[ ] Application on a Cloud. An Enterprise develops an App on a Cloud Service for their end users.

[ ] Cloud bursting. Describes the scenario where workloads are migrated on-demand to a public CSP as needed by the cloud customer.

[ ] Processing sensitive data. An enterprise wants to use an online cloud application (SaaS) to process sensitive data, including Personally Identifiable Information (PII).

[ ] Data integrity. A customer moves a three-tier application from an on-premises data center to an IaaS CSP that will run the application off-premises.

[ ] High availability. Through the use of one of more CSPs an organization provides high availability in the event of a disaster or a large-scale failure.

e) In which aspects of the Cloud service life cycle are your cloud service customers interested? *(Please rank from 1 (high interest) to 3 (low interest))*

[ ] They are interested on how to acquire Cloud services (e.g., choosing a CSP).

[ ] They are interested on the actual operational stage of the Cloud service (e.g., monitoring)

[ ] They are interested on the termination process of the Cloud service (e.g.,

[14] Categorization based on ETSI's "Cloud Standards Coordination – Final Report". Available online: http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf

understanding data retention clauses)

2. Based on your offered Service Level Agreement, please perform its self-assessment based on the criteria presented on the *attached* spreadsheet (see below)

3. From your point of view, is the CRM missing critical groups/elements/components that could contribute to improve the way SMEs deal with cloud services?

4. Do you agree to make publicly available in the SLA-Ready website the provided self-assessment?
   - ☐ Yes, I agree
   - ☐ No, I don't agree. Please specify a reason:

5. Would you be willing to participate in a follow-up discussion on this subject? If yes please provide your name and a contact email address:

CSP name:
Webpage:
Covered SLA service:

Group	Name of CRM element	Explanation/Assessment Question	CSP Self-assessment	Comments
General	SLA URL	Is there a publicly (online) available version of your cloud SLA?	0 = No , 1= Yes (please provide URL)	
	Findable	How can customers find the SLA on your website?	0 = n/a , 1 = External search engine, 2 = Internal search engine , 3 = Homepage link	
	Choice of law	Is the SLA specific to a particular jurisdiction or geographical area?	0 = n/a or No, 1 = Yes	
	Roles and responsibilities	Does your SLA contain a clear definition of roles and responsibilities?	0 = n/a or No, 1 = Yes	
	Cloud SLA definitions	Does your SLA contain relevant definitions used in the text?	0 = n/a or No, 1 = Yes	
Freshness	Revision date	Does your SLA specify the date of its last revision?	0 = n/a or No, 1 = Yes	
	Update Frequency	Does your SLA specify the frequency of performed updates based on a reported "Last Update" value?	0 = n/a or No, 1 = Yes	
	Previous versions and	Are the public available the previous versions of the SLA?	0 = n/a or No, 1 = Yes	

	revisions			
	SLA duration	Does your SLA contain a clear specification of its validity period?	0 = n/a or No, 1 = Yes	
Readability	SLA language	Is your SLA specified in more than one language?	0 = n/a or No, 1 = Yes	
	Machine-readable format	Is your SLA available in machine-readable format?	0 = n/a or No, 1 = Yes	
	Nr. of pages	What is the number of pages on your SLA? Only applies to SLAs in PDF/document format.	0 = n/a or No, 1 = Please specify the number of SLA pages	
Support	Contact details	Does your SLA contain a reference to the helpdesk number or other details to contact support?	0 = n/a or No, 1 = Yes	
	Contact availability	Does your SLA contain information about contact availability, specifying days of the week and working hours?	0 = n/a or No, 1 = Yes	
Credits	Service Credit	Does your SLA has a clear specification of the service credits provided to the CSC?	0 = n/a or No, 1 = Yes	
	Service credits assignment	Does your SLA specify the conditions whether a service credit shall be provided or not to the customer?	0 = n/a or No, 1 = Yes	
	Maximum service credits (Euro amount) provided by	Does your SLA describe how much does the can CSP credit (Euros) to the customer?	0 = n/a or No, 1 = Yes	

	the CSP			
Changes	SLA change notifications	Does your SLA specify of how the CSP notifies customers about SLA changes?	0 = n/a or No, 1 = Yes	
	Unilateral change	Does your SLA describe if the CSP is entitled to unilaterally change it?	0 = n/a or No, 1 = Yes	
Reporting	Service Levels reporting	Does your SLA describe if reports about achieved Service Levels are provided to the customer?	0 = n/a or No, 1 = Yes	
	Service Levels continuous reporting	Does your SLA explain if/how the service level reports are continuously updated?	0 = n/a or No, 1 = Yes	
	Feasibility of specials & customisations	Does your SLA clearly define any "specials"/exceptions and other possible customisations?	0 = n/a or No, 1 = Yes	
	General Carveouts	Does your SLA clearly define CSP assumptions, exclusions, scope of force majeure, and other carve outs to the negotiated cloud services, SLOs and SLA?	0 = n/a or No, 1 = Yes	
SLOs & Metrics	Specified SLO metrics	Does your SLA clearly and unambiguously specifies metrics related to the SLOs defined in the SLA?	0 = n/a or No, 1 = Yes	
	General SLOs	Does your SLA specify SLOs related to aspects like service monitoring, accessibility, availability, termination	0 = n/a or No, 1 = Yes	

		of service, applicable certifications, and governance?		
	Cloud Service Performance SLOs	Does your SLA specify SLOs related to aspects like response time, capacity, and elasticity?	0 = n/a or No, 1 = Yes	
	Service Reliability SLOs	Does your SLA specify SLOs related to aspects like service resilience, disaster recovery, and customer's data backup/restore?	0 = n/a or No, 1 = Yes	
	Data Management SLOs	Does your SLA specify SLOs related to aspects like IPR, CSC/CSP data, derived data, account data, portability, data deletion/location/examination, and law enforcement access to CSC data?	0 = n/a or No, 1 = Yes	
	Security SLOs	Does your SLA specify SLOs related to aspects like cryptography, physical/operational/communication security, incident management, compliance, and business continuity?	0 = n/a or No, 1 = Yes	
	Personal Data Protection SLOs	Does your SLA specify SLOs related to aspects like consent and choice, limitation, accountability, PII collection/use/retention/disclosure limitation, and privacy compliance?	0 = n/a or No, 1 = Yes	

Annex C. Document Log

DOCUMENT ITERATIONS		
V1.0	Table of Content, template for data collection and instructions to contributing authors	Ruben Trapero, TU Darmstadt
V2.0	First round of contributions on Introduction, CRM and Readiness	Ruben Trapero, TU Darmstadt
V3.0	Second round of contributions: Starndard analysis, use case analysis, readiness roadmap	Jesus Luna, CSA
V4.0	Third round of contributions: More use cases analysis, conclusions.	Ruben Trapero, TU Darmstadt, Jesus Luna, CSA, Arthur van der Wees, Arthur's
V5.0	Contributors review and final edits	Neeraj Suri, Ruben Trapero TU Darmstadt, Jesus Luna, CSA, Arthur van der Wees, Arthur's
V6.0	Internal Review	Silvana Muscella, Roberto Cascella; Trust-IT
V6.1	First round of revisions: comments and refutations addressed	Neeraj Suri, Ruben Trapero TU Darmstadt, Jesus Luna, CSA, Arthur van der Wees, Arthur's
VFinal	Final Version for submission	Nick Ferguson Trust-IT