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 – Final report

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

Contributor(s): Arthur van der Wees, Arthur's Legal; Marina Bregou, CSA

Date: 31 Dec, 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 degree of trust a user can put on Cloud Service Providers (CSP) to consequently leverage the higher uptake of cloud services. As the linkage across the CSP and the user typically transpires 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 in what to trust.

To this end, SLA-Ready has created a Common Reference Model (CRM) that helps towards the common understanding of SLAs for cloud services. The CRM integrates guidelines, standards and best practices to create a component based reference model to define SLAs with a common terminology, SLA attributes and Service Level Objectives.

The CRM was introduced in D2.3 by evaluating the requirements elicited in D2.1 and D2.2. An initial evaluation of the CRM was also conducted in D2.3 by evaluating the pertinent standards, best practices and also four representative use cases from real CSPs.

D2.4 conducts an in-depth validation and establishes the practical usefulness of the CRM. More specifically, D2.4 progresses beyond D2.3 in the following aspects:

- The update of the evaluation of the CRM with respect to the standardization bodies and agencies for best practices.
- A comprehensive evaluation of the CRM from the industrial perspective with the analysis of 23 use cases. The analysis is based on an extended template that has been modified to include aspects related to the expertise levels of the company.
- A novel recommendation methodology that provides the level of importance of every element of the CRM to SMEs that wants to provide cloud services.
- The computation of a SLA readiness index based on the CRM that compares across the CSPs using the CRM as a comparison criteria.

Table of Contents

Table of Tables

Table of Figures

Document information

Deliverable number	D2.4
Deliverable title	A Common Reference Model to describe, promote and support the uptake of SLAs – Final report
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	Dec 2016
Actual delivery date	Dec 2016
Author(s)	Rubén Trapero, Neeraj Suri, TUDA
Contributor(s)	Arthur van der Wees, Arthur's Legal; Marina Bregou CSA
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	141

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 that 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)	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
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 validates the final version of the SLA-Ready Common Reference Model (CRM), an integrated set of SLA components (i.e., attributes and SLOs), including the guidelines/state of practice and standard terminology. A high-level view of the process followed to develop and validate the CRM 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.

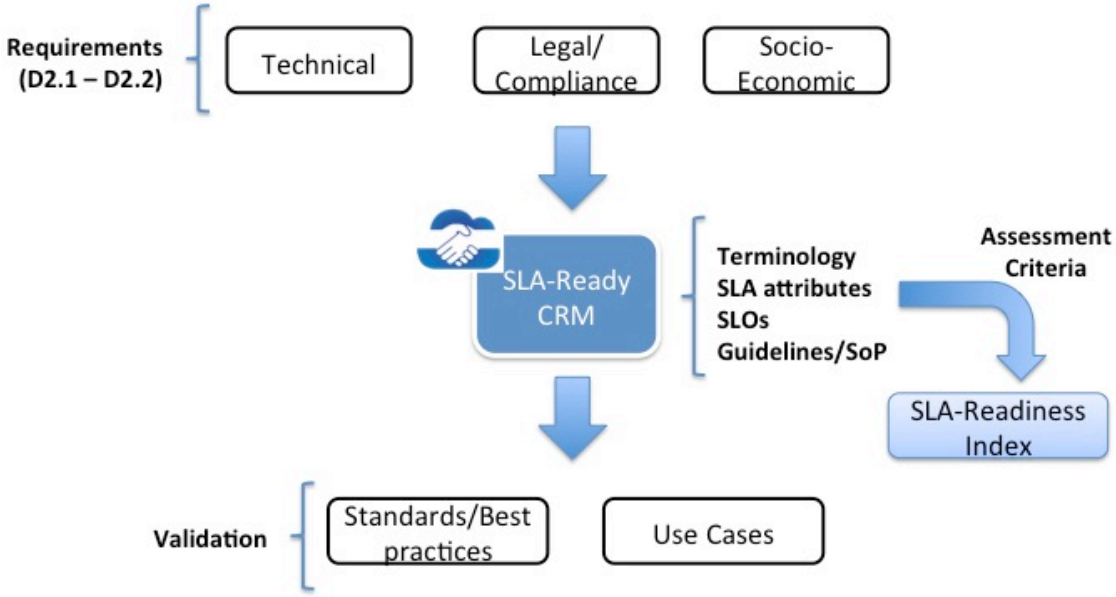

Figure 1. Developing and validating the SLA-Ready CRM.

Taking as a starting point the initial version of the CRM from deliverable D2.3, this deliverable consolidates the elements of the CRM and further validate it (beyond the initial validation done in D2.3) with the latest state of practice and relevant standards and with more sector-specific use cases.

This deliverable also provides a recommendation methodology to leverage the adoption of the CRM, by providing with the level of importance of the CRM elements adapted to the characteristics of new business cases.

Finally, this deliverable extends the "SLA-Readiness Index" introduced in D2.3. The SLA-Readiness Index complements the evaluation of the CRM against multiple CSPs.

1.1. Positioning D2.4 within SLA-Ready

This deliverable (D2.4), is the final iteration for the creation of the Common Reference Model (CRM) to define cloud SLAs. D2.4 builds upon D2.3 that provided an initial CRM along with an initial validation of the CRM, which is subsequently used in D2.4 to conduct a comprehensive validation with respect to the current market status.

Figure 2 shows the relationship between D2.4 and the rest of the WP2 deliverables. The CRM was created with the inputs received from: (i) WP3 (International cooperation, consensus and standardisation), (ii) the analysis of the state of practice carried out in D2.2, and (iii) the feedback received from the SLA-Ready's Advisory Board.

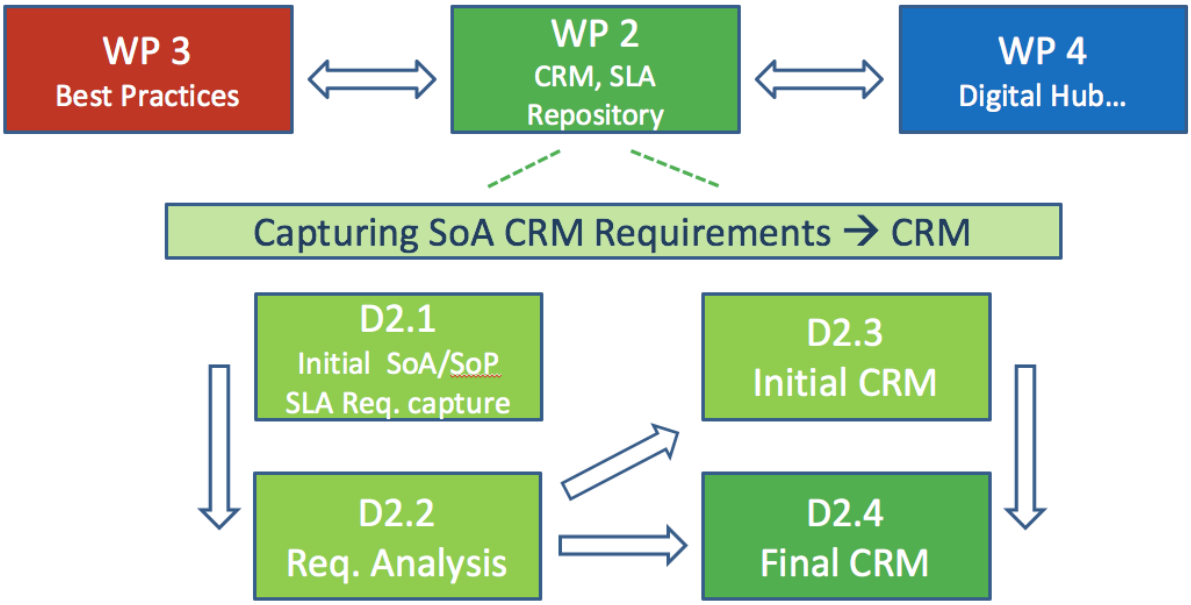

Figure 2. D2.3 within SLA-Ready

1.2. Structure of this report

The D2.4 report is organized as follows:

- Section 2 describes the process behind the validation of the CRM.
- Section 3 describes the actual CRM.
- Section 4 compares 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 the standards.
- Section 5 describes the analysis of several use cases with respect to the CRM.
- Section 6 describes the recommendation methodology based on the CRM and on the analysed use cases.
- Section 7 includes the comparison between different CSPs by using the CRM and based on cloud assessment techniques.
- Section 8 concludes the deliverable.

Please note that the listing of the considered use cases and the CRM questionnaire for the CSPs appears in Annexes A, B and C.

2. *Improving the validation of the CRM*

This section presents the approach followed in D2.4 to consolidate and validate the CRM. Figure 3 represents the initial process developed in D2.3 to validate the CRM. In D2.3 the process started by conducting a two-step analysis. First, the CRM was compared to the definitions and models proposed by the standardization community and working groups. More specifically, the analysis was done with respect to five references, namely (a) ISO/IEC 19086, (b) the cloud SLA checklist from the European Union, (c) the Cloud Standards Consumer Council, (d) the C-SIG SLA guidelines and (e) ETSI.

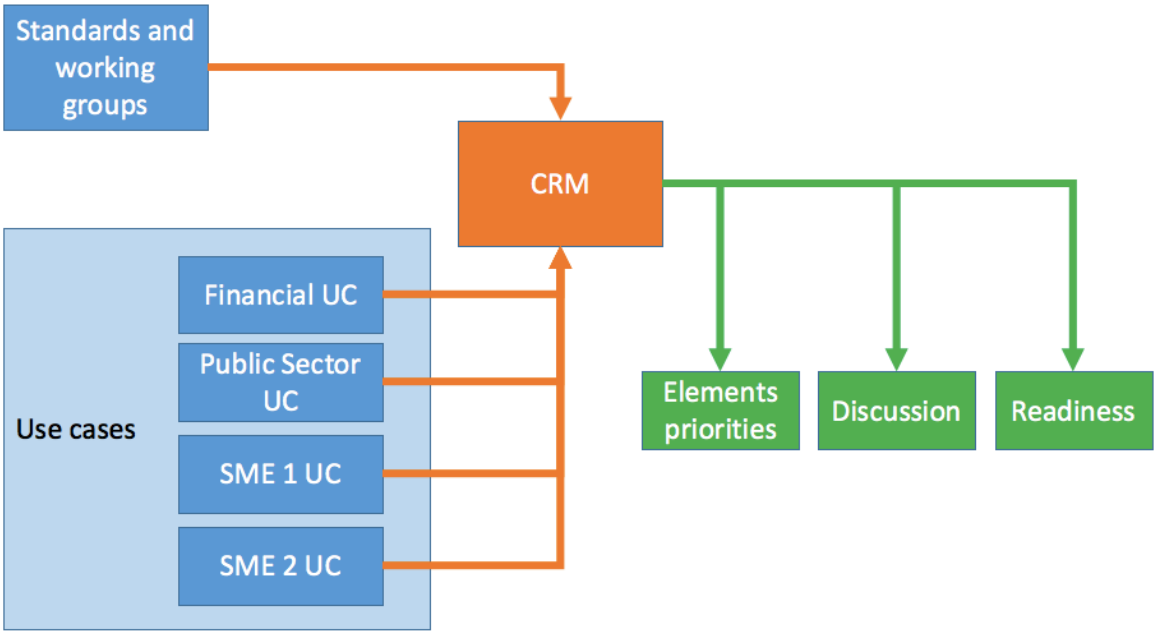

Figure 3. CRM inception and initial validation in D2.3

Secondly, the CRM was compared with respect to four representative use cases obtained from the targeted domains of financial sector, public sector, and from SMEs. The basic purpose of this comparison was to ensure the broad relevance of the elements of the CRM across the diverse use case being analysed.

The result was an overview of the priorities that makes some elements of the CRM more relevant than others across the use cases. D2.4 builds work upon these initial results to provide both a comprehensive analysis of the CRM and also establishing its broad validity by evaluating over an extensive 23 use cases.

Another result obtained from the initial validation of the CRM in D2.3 was a general overview of the techniques to evaluate the readiness of the CRM, including also the initial insights of the SLA marketplace along with D4.2. D2.4 comprehensively extends this with additional validation actions.

Figure 4 depicts the overall process followed in D2.4. In order to improve the analysis of the CRM, D2.4 reports an extended evaluation of the CRM based on the analysis of multiple use cases covering interdisciplinary areas. The CRM has also been updated with respect to the latest developments in ongoing standards and working groups.

As a result, the CRM has been used to carry out a two-fold validation:

- **The analysis of the CRM** with respect to the complete set of use cases has allowed identifying the most representative use cases domains. These domains are used to provide with the recommendation of the most important elements of the CRM for new business cases. The process (as described in Section 6) classifies new business cases into distinct categories. For each category, the recommendation methodology informs about the relevance of every element of the CRM. This information is adapted to the characteristics of the business case being studied.
- **The evaluation of the readiness index of the CRM**. The security assessment techniques introduced in D2.3 has allowed us to compare different real world CSPs according to their offered SLA and based on the CRM. The results can be organized in a ranking that provides CSPs with both feedback and recommendations.

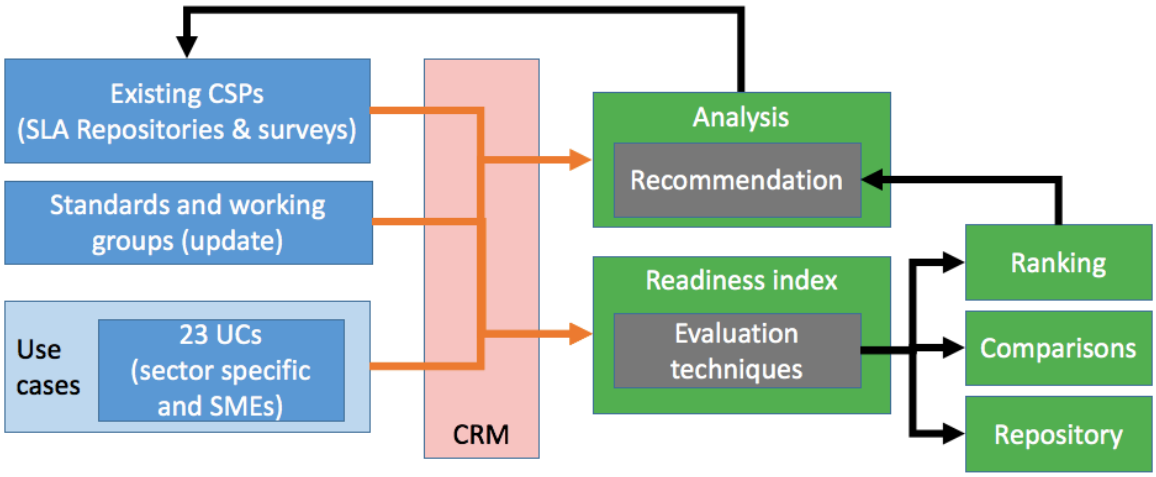

Figure 4. Final CRM and extended validation in D2.4

3. The Common Reference Model (CRM)

This section overviews the SLA-Ready's proposed CRM. Section 3.1 summarizes the requirements elicited from D2.2, while Section 3.2 outlines the initial version of the CRM.

D2.2 conducted a comprehensive analysis of four significant domains in order to identify the common characteristics of the cloud service provisioning. Figure 5 represents the analysed domains and also highlights the varied perspectives (i.e., economic, sociological and legal and governance) that were considered in the analysis by considering customers and stakeholders associated to the SLA-Ready partners. The technical perspective analysed both research projects (ongoing and finished) and the pertinent standards.

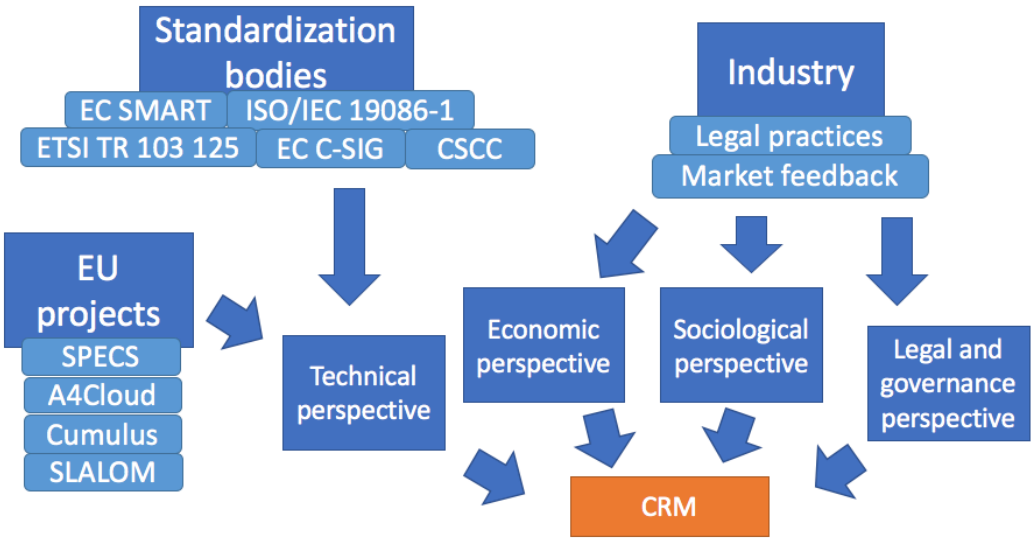

Figure 5. Requirements elicitation

The result of this analysis derives a list of requirements that represent the expected information to be included in an SLA. We have used these requirements to transcend from the information "expected" in an SLA to deriving the proposed specific elements of the Common Reference Model.

The process, to identify the elements of the CRM, starts by grouping the list of requirements elicited in D2.2. This identification process results into four initial requirements groups as depicted in Figure 6:

- The *general requirements* contain the information or characteristics of the SLAs that describe the general terms of the service provisioning, such as the language of the SLA or the length of the SLA.
- The *responsibility* related elements are the requirements that have to do with the parties involved in the SLA.

- The *economic* related requirements have to do with information related to the billing and cost associated to the service provided.
- The *technical* SLOs group the requirements related to the definition of technical aspects of the service provisioning.

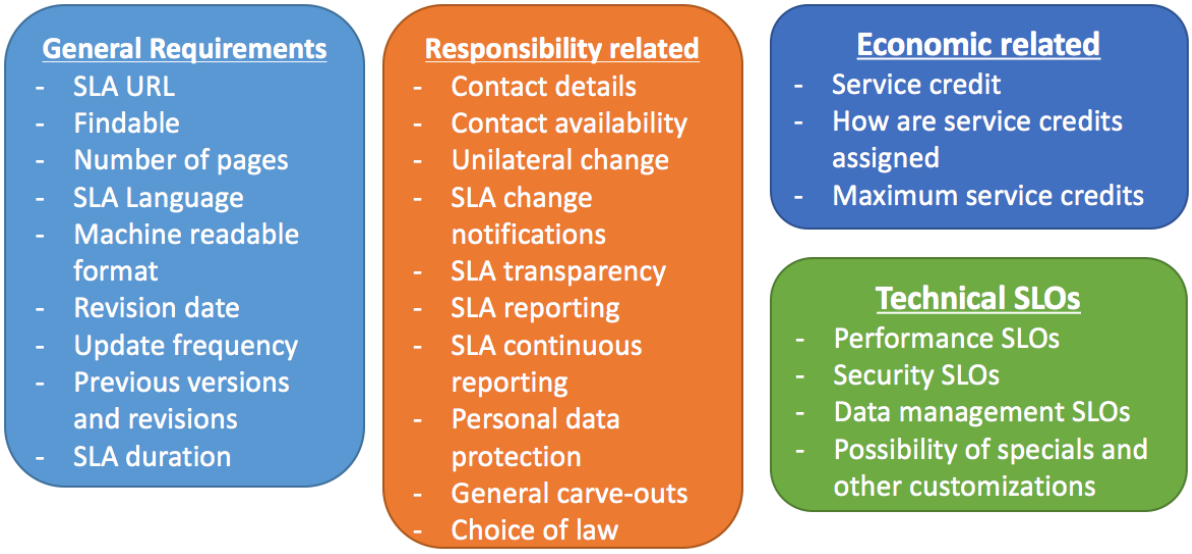

Figure 6. Grouped requirements

This initial set of groups has been used to fine tune the specification of the elements that comprises the CRM. Overall, 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.

In order to facilitate the applicability of the CRM and to increase the granularity of the analyses that will be done using it, we have split these four main groups into several subgroups. This allows us to better adjust the elements of the CRM that will fulfil the requirements identified in D2.2. Furthermore, we have used the recommendations from the ISO/IEC 19086 to identify these groups. Table 1 describes the 8 groups of the CRM.

Table 1. 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 the CSP

CRM Group	Description
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.

Each identified group will contain one or more elements where these elements have been extracted from the CRM requirements. Some of requirements can be directly extrapolated from the CRM requirements while the other more implicit requirements have been divided into more than one element as depicted in Table 2.

Table 2 categorizes the elements identified in each group. As already pointed out, some CRM requirements directly map to the same group. Others, such as "Choice of law" have been moved to the general group, as it describes the scope of applicability of the SLA, which represents a general aspect.

Table 2. Groups and elements of the CRM

Group	Name of CRM element	Description
General	SLA URL	Needed for SMEs to easily reference the SLA.
	Findable	This element represents the difficulty to find the SLA on the CSP´s website.
	Choice of law	Describes if the SLA applies to a particular geographical region, jurisdiction.
	Roles and responsibilities	Describes the responsibilities of the parties involved in the SLA (customer and provider(s)).
	Cloud SLA definitions	A description of the terms used in the SLA.
Freshness	Revision date	The revision date might be important for the user/customer that already created SLAs before with a CSP to easily identify that there may be changes that need to be reviewed.
	Update Frequency	Most of the CSPs will only update the SLA when a new functionality or way to use the services are provided. For public SLA, CSP's will avoid to have to manage multiple applicable SLA. In most of the cases, the last one is the one applicable for all service transactions. In many cases, SLA updates are related to the monthly billing process (a new SLA starts with a new month and a new way to calculate the bill).

	Previous versions and revisions	The CSP should have a repository with the previous versions/revisions of their SLAs.
	SLA duration	The common practice is to have a SLA valid until the next one is released. The CSP will try to have a valid SLA as long as possible to avoid any disagreement with the customer.
Readability	SLA language	Having the SLA available/located in multiple languages facilitates its readability and understanding.
	Machine-readable format	This aspect benefits automation on the SLA management. May prove useful to empower Customers.
	Nr. of pages	The state of practice is to have not so readable SLA and quite often build using many links and redirection. For SME, SLA shall consist of two pages at the maximum.
Support	Contact details	Easy to locate contact details benefit SME trying to solve questions about the SLA during the life cycle of the cloud service.
	Contact availability	Helpdesk availability may benefit the SME perception of assurance on the CSP.
Credits	Service Credit	Credit refers to the amount of money that usually the CSP spares to the Customer for using its services (e.g., pre-payment). After the provided Credit, the Customer will be billed by the CSP. For public cloud, the state of practice is "pay as you go". For most of CSP, this feature is not yet implemented. For some services, this feature could damage the customer (for example: end of the credit, end of the cloud service and uncertainty about customer data if any).
	Service credits assignment	Refers to the stakeholder (CSP or Customer) determining of the credits are provided.
	Maximum service credits (Euro amount) provided by the CSP	Refers to the amount of credits (in Euros) that are provided in order for the Customer to use the services from the CSP.
Changes	SLA change notifications	The common practice is to notify only changes that can impact the service provided to the customer. As common practice, minor changes will not be notified to the customer. The number of change notifications to customer have an impact on the customer perception of quality of the cloud platform, so CSPs will only notify major changes.
	Unilateral change	The common practice is to change the SLA unilaterally. The terms and conditions of the new SLA in most of the case may have been evaluated through a set of "beta testers" chosen among trusted

		customers/partners.
Reporting	Service Levels reporting	Refers to the reporting done by the CSP (either continuous or not) related to the achieved Service Levels in a period of time. This is useful for the Customer to compare with respect to the agreed SLOs. The common practice is to join the SLA reporting with the customer's bill.
	Service Levels continuous reporting	Specifies if the Service Levels reporting is actually continuous.
	Feasibility of specials & customisations	For IaaS CSP, the Customer should expect that all the customisations are feasible on the installed software.
	General Carve outs	Describes the potential exclusions of some provisions of the SLA, according to some kind of condition or assumption.
SLOs & Metrics	Specified SLO metrics	Indicates whether SLO metrics are included in the SLA. Only few CSP describe the mechanism used to measure the SLA attributes. Mainly because it is not an easy task and the customer needs to be mature enough to analyse the rightness of the measurement mechanism.
	General SLOs	SLOs related to general aspects of the SLA, such as Availability.
	Cloud Service Performance SLOs	SLOs describing performance indicators.
	Service Reliability SLOs	SLOs related to the reliability of the service.
	Data Management SLOs	SLOs related to the management of the information handled by the service.
	Security SLOs	SLOs related to security aspects of the service.
	Personal Data Protection SLOs	SLOs related to the management of sensitive personal Data.

Therefore, the CRM follows a hierarchical structure (as depicted in Figure 7). The top level represents the main CRM Groups that organize the rest of the elements of the CRM. The core of the CRM is the CRM Element level that includes the main parts that can be mapped to the different aspects of SLAs.

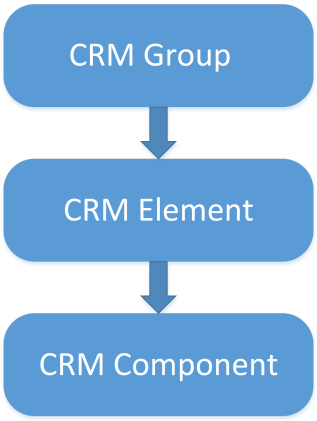

Figure 7. CRM hierarchical specification

The lowest level comprises the CRM Components that could be part of some CRM Elements. Currently just the "SLOs & Metrics" group contains elements that includes components at the lowest level of the hierarchy. Figure 8 depicts the 7 elements that are part of the "SLO & Metrics" group and the components that are included in every element. Those components are compliant with the classification of SLOs as described in the ISO/IEC 19086 specification. Two elements of the "SLO & Metrics group" provide general information:

- 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 ISO/IEC 19086 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/IEC 19086 specification. These components of the CRM are used to check whether those technical aspects are included in SLAs.

Figure 8. Components of the SLO & Metrics element of the CRM

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

- 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).

3.1. Summary takeaways

Summary takeaways

- The CRM is based on requirements gathered from the study of four different domains spanning the technical domains (including standardization bodies and research projects), the economic domain, plus the sociological and legal domains by analysing the current state of practice on SLAs in the industrial sector.
- The compiled requirements were grouped according to four main areas identified in the study of the aforementioned domains as: general aspects of SLAs (related to the sociological analysis), responsibility related aspects (related to the legal analysis), economic aspects (related to the economic analysis) and technical aspects (related to the analysis of the research and standardization domains).
- To create the CRM, we have evaluated the compiled requirements and split the four areas identified in the requirements into eight derived groups compliant with the latest ISO/IEC 19086 specification.
- The CRM is organized as a hierarchy, with 8 Groups at the top containing 30 Elements.

- The Elements of the CRM have been taken either directly from the requirements or from the current relevant standards, when a direct mapping requirement-standard was possible.
- Additionally, the elements of the group SLO & Metrics contain 46 components derived from the technical aspects identified in research projects and standards.
- In total, the CRM is composed of 8 groups, 30 elements and 46 components

4. CRM mapping to standards and best practices

In order to maximize the impact and to facilitate the adoption of the contributed CRM by the 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 have 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 and best practices perspective by using as input the work done by SLA-Ready's WP3 related to 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.

4.1. Initiatives being analysed

Based on the activities performed by WP3, this section focuses on gap analysing the contributed CRM with respect to the following relevant set of standards and best practices:

Table 3. 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 computing services [3]	The proposed Model SLA is the most current EC-sponsored study in this field.
ETSI	TR 103 125	SLAs for Cloud services [4]	The defined SLA template is relevant to the industry.

Organisation	Initiative acronym	Initiative	Relevance to the CRM
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.
EU H2020 SLALOM Project	SLALOM	SLALOM SLA Specification and Reference Model [22]	The EU SLALOM project proposed a cloud SLA model, including related best practices, which are also aligned to the relevant ISO/IEC 19086 family of standards.
EU H2020 SLALOM Project	SLALOM	Model contract for Cloud Computing [23]	This SLALOM deliverable documents he legal model proposed by the project, which is aimed to complement SLALOM's SLA Specification.

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

Table 4 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. From the performed analyses, it may be noted that the contributed 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 and Credits. As already mentioned, the results shown in Table 4 were used to structure SLA-Ready's guidance documents produced by WP3 and WP4. The current versions of the ISO/IEC 19086-1/-4 standards used for the CRM analysis have not been changed since the results shown in the previous deliverable (D2.3).

Table 4. CRM coverage of relevant standards and best practices

CRM element	CRM coverage to relevant standards (Yes/No)						
	ISO/IEC 19086[2] (Part 1 and Part 4)	Cloud SLA checklist[3]	Guide for Evaluating Cloud SLAs[4]	C-SIG SLA Guidelines	ETSI's cloud SLA template[5]	SLALOM SLA Specification and Reference Model[6]	SLALOM Model contract for Cloud Computing[7]
SLA URL	No	No	No	No	No	No	No
Findable	No	No	No	No	No	No	No
Choice of law	No	No	No	No	No	No	Yes
Roles and responsibilities	Yes	Yes	Yes	No	Yes	No	Yes
Cloud SLA definitions	Yes	No	No	Yes	Yes	No	Yes
Revision date	No	No	Yes	No	Yes	No	No
Update Frequency	No	No	Yes	No	Yes	No	No

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

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

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

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

[6] Please refer to http://slalom-project.eu/. Last accessed on Nov 2016.

[7] Please refer to footnote no. 6

CRM element	CRM coverage to relevant standards (Yes/No)						
	ISO/IEC 19086[2] (Part 1 and Part 4)	Cloud SLA checklist[3]	Guide for Evaluating Cloud SLAs[4]	C-SIG SLA Guidelines	ETSI's cloud SLA template[5]	SLALOM SLA Specification and Reference Model[6]	SLALOM Model contract for Cloud Computing[7]
Previous versions and revisions	No	No	Yes	No	Yes	No	No
SLA duration	No	No	Yes	No	Yes	No	Yes
SLA language	No	No	No	No	No	No	Yes
Machine-readable format	No	No	No	Yes	No	No	No
Nr. of pages	No	No	No	No	No	No	No
Contact details	Yes	Yes	Yes	Yes	Yes	No	Yes
Contact availability	No	No	Yes	Yes	Yes	No	No
Service Credit	No	No	Yes	No	No	No	Yes
Service credits assignment	No	No	No	No	No	No	Yes
Maximum service credits (Euro amount) provided by the CSP	No	No	No	No	No	No	Yes
SLA change notifications	Yes	Yes	Yes	Yes	Yes	No	Yes
Unilateral change	No	Yes	Yes	No	No	No	Yes
Service Levels reporting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Levels continuous reporting	No	Yes	Yes	No	Yes	No	Yes
Feasibility of specials & customizations	No	No	Yes	No	No	No	No
General Carveouts	Yes	No	Yes	No	No	No	Yes
Specified SLO metrics	Yes	No	Yes	Yes	Yes	Yes	No

CRM element	CRM coverage to relevant standards (Yes/No)						
	ISO/IEC 19086[2] (Part 1 and Part 4)	Cloud SLA checklist[3]	Guide for Evaluating Cloud SLAs[4]	C-SIG SLA Guidelines	ETSI's cloud SLA template[5]	SLALOM SLA Specification and Reference Model[6]	SLALOM Model contract for Cloud Computing[7]
General SLOs	Yes	Yes	Yes	No	Yes	Yes	No
Cloud Service Performance SLOs	Yes	Yes	Yes	Yes	No	Yes	No
Service Reliability SLOs	Yes	Yes	Yes	Yes	Yes	Yes	No
Data Management SLOs	Yes	Yes	Yes	Yes	Yes	No	No
Security SLOs	Yes	Yes	Yes	Yes	Yes	Yes	No
Personal Data Protection SLOs	Yes	Yes	Yes	Yes	No	No	No

4.2. Summary takeaways

Summary takeaways

- The analysis of the CRM with respect to surveyed standards and best practices shows that there is a 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].
- Most 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. One exception is SLALOM [22], which proposed a machine-readable specification for SLA metrics based on ISO/IEC 19086-2.
- 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]. An exception is SLALOM [23] which considers some of those CRM elements.
- From the analysed-standards/best-practices both the CSCC and SLALOM reports 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. Both SLALOM reports [22] and [23| altogether provide a good coverage of the CRM proposed by SLA-Ready. While [22] is more focused on metrics, the report [23] covers some of the other CRM elements.
- Despite not being cloud-specific, the SLA template defined by ETSI in their "ETSI EG 202 009-3" report also shown a good coverage 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.

5. 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 23 use cases from varied domains. Each of the use cases is analysed by first taking the CRM as a reference, and then assessing which CRM elements are actually applicable to these use cases along with considering their priorities therein.

5.1. 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. Furthermore, the use case template used in the present report has been enhanced to better profile the SME in order to provide a major focus on extracting information required for the following:

- The guidance in "D3.3 - A Business Guide to Service Level Agreements: How to be a well-advised user of cloud services".
- The analysis for the automated recommendation of CRM good practices, which will be introduced in Section 6.

For the analysis of the use cases, we will use the template shown in Table 5 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. As mentioned above, the template also collects information related to the SME’s maturity level in relationship to the use case being documented (i.e., novice, basic or experienced), and target cloud service characteristics (i.e., life-cycle, preconditions and requirements).

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 5. Use Case Template

Identification	**Title**	UC name
	SME Maturity	One or more of the following: • Novice: no knowledge, no experience • Basic: some knowledge, but no practical experience • Experienced: some practical experience (either good or bad)
	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 4 for more information.
	Additional comments	Add comments, remarks, suggestions, as you see fit
Summary	Conclusions related to the use case analysed	

5.2. Use cases and CRM mapping

This section demonstrates the applicability of the proposed template (cf., Table 5) for analysing the developed CRM from the use cases perspective. In particular, we focus on the analysis of 23 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. The results of this section will be used as input for the recommendation methodology detailed in Section 6.

5.2.1. Use case 1: Fintech - Financial sector use case

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 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'.

Table 6. Use case 1: Fintech

Identification	**Title**	Fintech Early Stage Seeking IaaS (Financial sector)
	SME Maturity	• Experienced
	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 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 its own customers which in this use case 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	Before looking for appropriate IaaS CSPs, and finding

	compliance criteria	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, first, 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 and 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. For instance the banks have their own (without an FSI industry) best practice being available regarding cloud services. This is because the bank authorities do not see it as its 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 but 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	

5.2.2. Use case 2: Governmental 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 Governmental Cloud resemble those typically elicited by European SMEs.

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

Table 7. Use case 2: Estonian Governmental Cloud

Identification	**Title**	Governmental Cloud (Small Public Administration using Governmental Cloud)
	SME Maturity	• Experienced
	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 Governmental 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 Governmental Cloud solution. Sufficient flexibility has to be planned in advance. The State Infocommunication Foundation leads the Governmental 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 Governmental Cloud. In some cases, PAs are provisioned with IaaS resources (e.g., virtual machines), but also PAs provision Governmental cloud-based services to citizens. The Governmental Cloud system does not store personal identifiable data.
	Cloud Actors	List of involved actors/stakeholders: • Cloud Service Providers, which provision

		their services to the Governmental 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 Governmental Cloud services This use case defines an additional actor, namely the Governmental Cloud Owner, which relates to the organization that legally owns the Governmental Cloud and defines policies and requirements. The analysis of this use case considers that the Governmental 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	• Operation
	Legal and Data Protection compliance criteria	The Governmental Cloud does not manage any PII data from the citizens. Legal compliance criteria are defined by 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 Governmental 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 Governmental 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.	

5.2.3. Use case 3: ConsultLess, 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., "ConsultLess, SME using SaaS"). The relevance of this use case for SLA-Ready is based on its focus on

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

both security and SLAs for SMEs that are transitioning to the cloud. Table 8 further documents this use case.

Table 8. Use case 3: ConsultLess, SME for using SaaS

Identification	**Title**	ConsultLess, SME for using SaaS
	SME Maturity	• Novice • Basic
	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 office software installed on computers."
	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	• Acquisition
	Legal and Data Protection compliance criteria	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.
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, having some 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.

5.2.4. Use case 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.

Table 9. Use case 4: SME migrating from one SaaS CSP to the other

Identification	**Title**	SME migrating from one SaaS CSP to the other
	SME Maturity	• Basic • Experienced
	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 that mission critical for the SME's business. Upon the plans made to shift the cloud services from the existing SaaS CSP to a new SaaS CSP, the SME founds out that its survival and success depends on the use of the particular SaaS.
	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 and integrated in the organization of the SME.
	Cloud Service life-cycle phase	• 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 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 in this use case the SME has used to the intent to improve his way of procuring cloud services and follow the CRM where important for his 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, this as per 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, for this type of SME customary requirements have 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, for this type of SME customary best practices have 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.	

5.2.5. Use case 5: Cloud Brokering: Chargeback and Showback

The following use case is based on "ISO/IEC SC38 Standing Document 1 - Compendium of Cloud Computing Usage Scenarios and Use Cases". Its relevance to SLA-Ready resides on the use case's focus on interoperability, multi-cloud and brokering where the CRM's usefulness can be easily observed. It is important to highlight that the CRM-analysis for this use case is performed from the CSC perspective (i.e., the Cloud Broker and involved CSP's are "visible" to the CSC).

Table 10. Use case 5: Cloud Brokering: Cloud Chargeback and Showback

Identification	**Title**	Cloud Brokering: Cloud Chargeback and Showback
	SME Maturity	• Basic
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud
	Short description	A CSC uses the services of a Cloud Broker to select the CSP that fulfils its specific requirements. The Broker implements a service catalogue encompassing services from multiple CSPs. In addition, the catalogue clearly outlines charges for the various resources that can be provisioned. The CSC makes a selection and the Cloud Broker seamlessly provisions the requested resource from the appropriate CSP through their API or other interface using their native commands. At the same time, the Broker handles the chargeback to the CSC's organization, if appropriate.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer • Cloud Service Partner
	Cloud Service life-cycle phase	• Acquisition
	Legal and Data Protection compliance criteria	There are not generic legal/data protection criteria applying to this particular use case. However, we acknowledge the fact that in those cases where such criteria exist, then the prospective cloud customer's analysis of the CRM should reflect those.
Preconditions and Requirements	**Security and privacy requirements**	CSCs will be able to track utilization per identity from CSPs and bill the appropriate organization for use of resources.
	Additional preconditions and requirements (e.g. performance)	CSPs will provide necessary accounting information to enable CSC to bill accordingly. CSPs interoperability (including billing systems) is required in this use case, and mostly managed by the Broker.
	Existing SLA standards and best practices to rely on	• C-SIG SLA Guidelines
	Additional comments	None
Summary	This use case is a representative example related to the usefulness of cloud SLAs for decision-making processes. Cloud brokers are becoming more common in the cloud ecosystem, so the analysis/good practices extracted from the CRM are expected to be used as guidelines for prospective cloud customers.	

5.2.6. Use case 6: Distribution of SME Training Material to Mobile Employees

The following use case is based on "ISO/IEC SC38 Standing Document 1 - Compendium of Cloud Computing Usage Scenarios and Use Cases". It considers a scenario which may become familiar to several SMEs, where employees are involved and need to have (cloud-) ubiquitous access to documentation from any place.

Table 11. Use case 6: Distribution of SME Training Material to Mobile Employees

Identification	**Title**	Distribution of SME Training Material to Mobile Employees
	SME Maturity	• Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • DI: Data Integrity • HA: High Availability
	Short description	A SME must deploy the technical processes and considerations to distribute educational material for new products to their agents. Given the potential network traffic to be generated by this process, it is necessary to rely on cloud services. This use case can be considered as one of many use cases that are possible with mobile cloud, which notion is similar to DaaS (Desktop as a Service) except that all services are for mobile devices.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer
	Cloud Service life-cycle phase	• Operation
	Legal and Data Protection compliance criteria	This use case does not involve PII, therefore no particular Data Protection requirement applies. Authentication requirements (see below) are only related to the IAM data contained in e.g., legacy authentication systems.
Preconditions and Requirements	**Security and privacy requirements**	A correct version of the material should be delivered to authorised agents, and with an auditable access control mechanism that enforces the company's security policies. Identity management for access authentication, and authorization is crucial for this use case.
	Additional preconditions and requirements (e.g., performance)	The SME will distribute only static data (e.g., documents, presentations, leaflets digital format), but it is not considering distributing dynamic content. Besides integrity and consistency of distributed content, it is necessary to guarantee communication between CSP and SME's agents.
	Existing SLA standards and best practices to rely on	None
	Additional comments	None
Summary	Mobile and cloud computing are represented in this use case. This scenario can potentially apply to a broad variety of SMEs, therefore its relevance to SLA-Ready. Furthermore, this	

	scenario can be easily extended to comprise the integration of non-static content e.g., streaming video tutorials for the sales representatives.

5.2.7. Use case 7: EasyAgriSelling - SME using IaaS/PaaS

This use case is based on a real life case where a small tech start-up in the EU, developed an online web shop software (as a service) for farmers who would like to start direct-selling their vegetables and other products. Farmers can set up an online shop in a few clicks - customizing their shop with a logo, colours and a description of their farm. EasyAgriSelling is a SaaS provider and they are a cloud services customer building services on a cloud provider who offers them IaaS and PaaS on which to build their product. The relevance of this use case for SLA-Ready is based on its focus on security, and also on SLAs for SMEs that are being built in the cloud.

Table 12. Use case 7: EasyAgriSelling, SME using IaaS/PaaS

Identification	**Title**	EasyAgriSelling, SME using IaaS/PaaS
	SME Maturity	• Experienced
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud • HA: High Availability
	Short description	EasyAgriSelling is a small tech start-up in the EU, which developed an online web shop software (as a service) for farmers who would like to start direct-selling their vegetables and other products. Their slogan is: "Selling your agricultural produce to consumers, made easy". Farmers can set up an online shop in a few clicks - customizing their shop with a logo, colours and a description of their farm. EasyAgriSelling operates a pay-as-you-go model, charging no monthly fee, but only charging their customers when products are sold. EasyAgriSelling is a SaaS provider and they are a cloud services customer building services on a cloud provider who offers them IaaS and PaaS on which to build their product. The SaaS platform runs on top of the IaaS/PaaS platform.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer EasyAgriSelling - SaaS is both a vendor, as it is paid by the farmers when they sell their products and a CSC, as it pays for cloud service from the IaaS/PaaS platform, which it uses for running its web shop software for farmers. The IaaS/PaaS platform is a CSP.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal and Data Protection compliance criteria	Availability is a critical factor in this use case. Furthermore, security and privacy of payment

		data is very important, as well as some of the consumers' personal data. Data leaks could have a severe impact on the reputation/business of the firm. The SME (EasyAgriSelling) is already using cloud services, in this case IaaS/PaaS, and the CSP (IaaS/PaaS platform provider) guarantees end-to-end quality of service as well as guaranteed performance against an abrupt increase of the load. The SME is responsible for the software security of the online web shop software, the web interfaces used by the farmers (customers of EasyAgriSelling) and the personal data and payment data of the consumers buying from the farmers.
Preconditions and Requirements	**Security and privacy requirements**	For the SME (EasyAgriSelling) in this case, software vulnerabilities are a big risk (because the payment and personal data of consumers is at stake). The SME will look closely at how the IaaS/PaaS is patched and updated. Some security tasks are outsourced to the provider, but many security tasks still have to be carried out by the customer/SME (EasyAgriSelling). It is the responsibility of the SME (EasyAgriSelling) to fix software flaws in the deployed web shop software as well as managing the accounts of the farmers using their web shop software, the consumer accounts, including resetting passwords, troubleshooting issues with payments etc. Their responsibility includes managing backups of application software and data. Security considerations in the procurement process really only regard security of the facilities, the operating system and the application servers which are under control of the provider. Security tasks the provider carries out are managing hardware and facilities, including physical security, power, cooling, etc.; managing the server operating systems and the application server, including development, deployment, patching, updating, monitoring, checking logs, and so on. The following security and privacy requirements apply to EasyAgriSelling: • 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 EasyAgriSelling. • The CSP should demonstrate compliance through those certifications required by EasyAgriSelling. • EasyAgriSelling requires a two-factor authentication process • EasyAgriSelling wants to avoid vendor lock-in issues.
	Additional preconditions and requirements (e.g. performance)	Availability is a main concern in this use case. Also for this type of SME customary preconditions and requirements have been taken into account while procuring the subsequent cloud services, e.g. a two-factor authentication process.
	Existing SLA standards and best practices to rely on	Non-applicable, as per this use case. However, for this type of SME customary best practices have been taken into account while procuring the subsequent cloud services. No particulars to mention in this case.
	Additional comments	EasyAgriSelling works with farmers and consumers from several countries. The data and processes are about simple e- commerce and there are no specific legal requirements that could cause issues with foreign jurisdiction.
Summary	This use case considers an SME cloud customer with some background experience on this technology, which is planning to use a new CSP (IaaS/PaaS). This use case validates the CRM from the perspective of an SME familiarised with cloud computing, and with a particular focus on the security/privacy implications of this technology.	

5.2.8. Use case 8: Video storage and streaming from the Cloud

The following use case is based on "Cloud Computing Use Case group - Cloud Computing use cases whitepaper" [32]. It describes a customer experience using cloud computing for streaming and storing video in the cloud while meeting security requirements.

Table 13. Use case 8: Video Storage and streaming from the Cloud

Identification	**Title**	SME video storage and streaming from the Cloud
	SME Maturity	• Novice • Basic
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud • HA: High Availability
	Short description	A financial investment company is launching new investment products to its agents and affiliates. A number of videos have been created to teach the company's agents and affiliates about the benefits and features of the new products. The videos are very large and need to be available on-demand, so storing them in the cloud lessens the demands on the corporate infrastructure. However, access to those

		videos needs to be tightly controlled. For competitive reasons, only certified company agents should be able to view the videos. An even stronger constraint is that regulations require the company to keep product details, including the videos, confidential during the quiet period before the launch of the product. The company's decision is to use a public cloud storage provider to scale the secure hosting and streaming of the videos. The cloud solution must control the videos with an auditable access control mechanism that enforces the company's security policies.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer, which includes the company but also the agents that will be certified to have access to the videos (agents and affiliates). • Cloud Service Partner - auditors will have the right to audit the cloud solution in order to enforce the company's security policies.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal and Data Protection compliance criteria	This use case does not involve PII, therefore no particular Data Protection requirement applies. Authentication requirements (see below) are only related to the IAM data contained in e.g. legacy authentication systems. Confidentiality is also of crucial importance because the product details, including the videos, are highly confidential during the quiet period before the launch of the product.
Preconditions and Requirements	**Security and privacy requirements**	For competitive reasons, only certified company agents should be able to view the videos. An even stronger constraint is that regulations require the company to keep product details, including the videos, confidential during the quiet period before the launch of the product. An auditable access control mechanism that enforces the company's security policies is required. Identity management for access authentication, and authorization is crucial for this use case.
	Additional preconditions and requirements (e.g. performance)	Apart from compliance, confidentiality and security of distributed content, it is necessary to guarantee communication between CSP and SME's agents. Access management is also important.
	Existing SLA standards and best practices to rely on	Governmental regulations.
	Additional comments	None
Summary	Mobile and cloud computing are represented in this use case. This scenario can potentially apply to a broad variety of SMEs that need compliance for non-static content e.g. streaming videos, therefore it is relevant to SLA-Ready.	

5.2.9. Use case 9: Cloud-based Development and Testing

This company chooses a cloud provider to deliver a cloud-based development environment with hosted developer tooling and a source code repository. It also chooses another cloud provider to provide a testing environment so that the new application can interact with many different types of machines and huge workloads. The relevance of this use case for SLA-Ready resides on the use case's focus on cloud federation and service level agreements for this purpose. The use case is based on "Cloud Computing Use Case group - Cloud Computing use cases whitepaper" [32].

Table 14. Use case 9: Cloud-based Development and Testing

Identification	**Title**	Cloud-based Development and Testing
	SME Maturity	• Experienced
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud • DI: Data Integrity • CB: Cloud Bursting • HA: High Availability
	Short description	An online retailer needs to develop a new Web 2.0 storefront application, but does not want to burden its IT staff and existing resources. The company chooses a cloud provider to deliver a cloud-based development environment with hosted developer tooling and a source code repository. Another cloud provider is chosen to provide a testing environment so that the new application can interact with many different types of machines and huge workloads.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer • Cloud Service Partner - auditors will have the right to audit the cloud solution in order to enforce the company's security policies.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal and Data Protection compliance criteria	This use case does not involve PII, therefore no particular Data Protection requirement applies. Authentication requirements (see below) are only related to the data contained.
Preconditions and Requirements	**Security and privacy requirements**	Identity management for access authentication, and authorization is crucial for this use case. Controlled access to source code and test plans is needed therefore Cryptography, Endpoint Security, Identity, Roles, Access Control, and Network Security are crucial.
	Additional preconditions and requirements (e.g. performance)	The SME requires that all traces of the application or data must be deleted when a VM is shut down, controlled access to source code and test plans, service automation and event auditing and reporting.
	Existing SLA standards and best	None

	practices to rely on	
	Additional comments	None
Summary	This use case validates the CRM from the perspective of a company/SME familiarised with cloud computing, and with a particular focus on the security/compliance implications of this technology. This use case is a representative example related to the usefulness of cloud SLAs for cloud-based developing and testing processes.	

5.2.10. Use case 10: Logistics and Project Management in the Cloud

The following use case is based on "Cloud Computing Use Case group - Cloud Computing use cases whitepaper" [32]. It considers a scenario which may become familiar to several SMEs, where the enterprise needs to move their data to the cloud and then it reaches the End User.

Table 15. Use case 10: Logistics and Project Management in the loud

Identification	**Title**	Logistics and Project Management in the Cloud
	SME Maturity	• Novice
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud • DI: Data Integrity
	Short description	A small construction company with approximately 20 administrative employees needed a way to manage their resources, optimize project scheduling and track job costs. The company had very specific requirements that no commonly available system addressed, so they used a combination of Quickbooks and spreadsheets. This system was not elastic and was a huge waste of human resources. The solution to the problem was to build a custom client-side application. All of the business logic resides on the client (company). Data for the application is served from a Google App Engine (GAE) datastore. The datastore does not enforce any sort of schema other than an RDF graph, although it does host an RDF-OWL ontology. The client uses that ontology to validate data before displaying it to the user or sending it back to the GAE.
	Cloud Actors	• Cloud Service Provider – GAE as PaaS • Cloud Service Customer – the company
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal and Data Protection compliance criteria	This use case does not involve PII, therefore no particular Data Protection requirement applies.
Preconditions and Requirements	**Security and privacy requirements**	No particular security needs for this use case. Data operations are communicated with the datastore using an application - specific RESTful protocol over HTTP. The datastore maintains RDF graphs specific to the applications it is serving within silos managed on the server. When Security is needed, it is implemented separately for each silo depending on the requirements of the application using a particular

		silo of data. Using this system, any number of applications can use the datastore.
	Additional preconditions and requirements (e.g. performance)	None. The data moved was reconciled before being uploaded to the GAE datastore.
	Existing SLA standards and best practices to rely on	None
	Additional comments	None
Summary	This use case presents the simple case of SMEs that have very specific needs which no commonly available system addresses. This use case is a representative example related to the acquisition of a simple PaaS implementation that provides database support.	

5.2.11. Use case 11: Local Government Services using a Hybrid Cloud

The following use case is based on "Cloud Computing Use Case group - Cloud Computing use cases whitepaper". It considers a scenario which may become familiar to several local governments that want to use a combination of services at a private and hybrid cloud level. The relevance of this use case for SLA-Ready resides on the use case's focus on federation of applications and data inside the hybrid cloud.

Table 16. Use case 11: Local Government Services in a Hybrid Cloud

Identification	**Title**	Local Government Services in a Hybrid Cloud
	SME Maturity	• Expert
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud • CB: Cloud Bursting
	Short description	There are more than 1800 local governments across Japan, each of which has its own servers and IT staff. A secondary goal of the Kasumigaseki cloud is to provide a hybrid cloud environment. In addition to the Kasumigaseki cloud, the Japanese central government has decided to group local governments at the prefecture level. Each prefecture will have a private cloud and a connection to the Kasumigaseki hybrid cloud. Internal tasks and some data will be hosted in the prefecture's private cloud, while other data will be stored locally. Wherever possible, existing systems will be virtualized and hosted in the Kasumigaseki cloud.
	Cloud Actors	• Cloud Service Provider – Kasumigaseki hybrid cloud • Cloud Service Customer – the prefecture
	Cloud Service life-cycle phase	• Operation
	Legal and Data Protection compliance criteria	Japanese law prevents some types of data from being stored outside the local government's servers, so moving applications and data into the Kasumigaseki cloud is not an option. It is also illegal for many types of personal data to be stored on a server outside of Japan.
Preconditions	**Security and privacy requirements**	Security and privacy requirements are set by the

and Requirements		central government of Japan, which has built a secure, centralized infrastructure for hosting government applications.
	Additional preconditions and requirements (e.g. performance)	Federation of applications and data inside the hybrid cloud is crucial.
	Existing SLA standards and best practices to rely on	None
	Additional comments	None
Summary	This use case presents the case of a government building a private cloud for its centralised applications and using that cloud as hybrid for few decentralised applications in order to reduce costs, energy consumption and IT staff.	

5.2.12. Use case 12: Payroll Processing in the Cloud

The following use case is based on "Cloud Computing Use Case group - Cloud Computing use cases whitepaper" [32]. It considers a scenario which may become familiar to several SMEs, where the enterprise needs to run its payroll process in the cloud. The relevance of this use case for SLA-Ready resides on the use case's focus on virtual machines and cloud storage (IaaS)

Table 17. Use case 12: Payroll processing in the Cloud

Identification	**Title**	Payroll processing in the Cloud
	SME Maturity	• Novice
	Base Use Case (cf. Deliverable 2.2)	• AP: App on a Cloud
	Short description	The organization decided to see how practical it would be to run the payroll process in the cloud. The existing payroll system was architected as a distributed application, so moving it to the cloud was relatively straightforward. The payroll application used an SQL database for processing employee data. Instead of rewriting the application to use a cloud database service, a VM with a database server was deployed. The database server retrieved data from a cloud storage system and constructed relational tables from it. Because of the size of the original (in-house) database, extraction tools were used to select only the information necessary for payroll processing. That extracted information was transferred to a cloud storage service and then used by the database server. The payroll application was deployed to four VMs that run simultaneously; those four VMs work with the VM hosting the database server. The configuration of the payroll application was changed to use the VM hosting the database server; otherwise the application was not changed.
	Cloud Actors	• Cloud Service Provider • Cloud Service Customer – the company
	Cloud Service life-cycle phase	• Acquisition

		• Operation
	Legal and Data Protection compliance criteria	This use case does not involve PII, therefore no particular Data Protection requirement applies.
Preconditions and Requirements	**Security and privacy requirements**	No particular security needs for this use case.
	Additional preconditions and requirements (e.g. performance)	The payroll application runs on Fedora and Java 1.5, so it will run without changes on any cloud provider's platform that supports Fedora. Modifying the application to use a different cloud storage provider could be a problem if the other vendor does not support the specific S3 APIs used in the payroll process.
	Existing SLA standards and best practices to rely on	None
	Additional comments	None
Summary	This use case presents the simple case of SMEs that have very specific needs, as is the processing of payroll. In the cloud-based version of the application, processing time for the payroll task was reduced by 80%. This is an example of SMEs/companies, that the cloud-based version offers them more elasticity, which can be a significant advantage as they expand.	

5.2.13. Use case 13: CSP specifying carve-outs in its cloud service terms

Each CSP provides qualified cloud services, as each has general carve-outs and other limitations and exclusions written in its SLA documentation. Some may be understandable, reasonable and within normal risk allocation boundaries. Some are not. Especially SMEs do not have the knowledge or expertise whether general carve-outs are reasonable and acceptable for their specific application and use of the cloud services, and what the consequences would be if a carve-out is specified.

Table 18. Use case 13: CSP specifying carve-outs in its cloud service terms

Identification	**Title**	CSP specifying carve-outs in its cloud service terms (General Carve-outs)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud
	Short description	As there is so much to think about while choosing, selecting and procuring cloud services, and the SME is aware that carve-outs are part of the cloud SLA where the CSP further limits or excludes its responsibility and liability, it is not always the highest priority to assess, understand, discuss and negotiate these with the CSP. When an incident happens the CSP has defined the carve-out 'force majeure' very

		broad, in a way that all influences of third parties are excluded, even of those the CSP procures to be able to provide the cloud services. In such a case, if an incident happens, the SME usually expects that it would be within the control of the CSP, but is often unable to claim any resource. The CSP merely referred to the general carve-out in the applicable SLA.
	Cloud Actors	CSP as vendor, and SME as customer.
	Cloud Service life-cycle phase	• Operation
	Legal compliance criteria	Before looking for an appropriate CSP, the SME should assess what kind of general carve-outs the CSP has stated in its SLA, ask questions if it does not understand the carve-outs, ask what it is paying for, and assess potential the consequences in case of an incident that may fall within scope of those general carve-outs.
Preconditions and Requirements	**Security and privacy requirements**	If the security of the data centre is involved for certain carve-outs, those requirements are an absolute necessity to assess within view of general carve-outs as well.
	Additional preconditions and requirements (e.g., performance)	Some basic knowledge about business and other risk allocation, as well as laws and regulations are necessary to assess a cloud SLA.
	Existing SLA standards and best practices to rely on	CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines
	Additional comments	N/A
Summary	The SME always needs to assess whether the general carve-outs are understandable, not described too broad, to what extent the CSP is in control, where that control ends, and what the consequences are in case of an incident that it either the control of the CSP or beyond the reasonable control of CSP.	

5.2.14. Use case 14: CSP changing SLA at operation time

Any change made in contractual arrangements, whether an SLA or otherwise, without the consent of all the parties involved seems impossible and unlawful. However, many CSPs have designated the contractual right to unilaterally change the SLA and the cloud services itself, whether beneficial or detrimental to the CSC. This means the CSP will be able to change its rights and obligations, without the consent of the CSC. Most, although not all, will notify you of a change, but then it may already be too late.

Table 19. Use case 14: CSP changing SLA at operation time

Identification	**Title**	CSP changing SLA at operation time (Change Notifications & Unilateral Change)
	SME Maturity	• Novice • Basic
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • HA: High Availability
	Short description	An SME has built its own SaaS on the PaaS infrastructure of a major CSP. The SME provides its SaaS to its customer under its own Master Service Agreement, Terms and Conditions and SLA. However, the SaaS SME did not notice that the PaaS CSP is contractually entitled right to unilaterally change the PaaS service offerings and conditions in the SLA, since the SME ticked the box while registering online without taking the time to assess the SLA and related terms. The CSP now invoked this right to lower the uptime and level of redundancy. Therefore, the SaaS cloud Services from the SME cannot meet the service level it has granted to its own customers. Migrating the application on a PaaS of another CSP would be a very time consuming and costly task.
	Cloud Actors	Cloud Service Provider as PaaS Provider, SME as Cloud Service Partner and SMEs customer as Cloud Service Customer.
	Cloud Service life-cycle phase	• Operation
	Legal compliance criteria	N/A
Preconditions and Requirements	**Security and privacy requirements**	N/A
	Additional preconditions and requirements (e.g., performance)	N/A
	Existing SLA standards and best practices to rely on	SMART SLA Model CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines ETSI Cloud SLA template
	Additional comments	N/A
Summary	Many CSP have reserved the right to unilaterally change the service conditions and terms, however this could be a serious obstacle for SaaS SME providers who are in a contractual relationship with their own customers.	

5.2.15. Use case 15: CSP providing services under different regulations

Cloud services are often hosted in one country and consumed in others. CSPs may use distributed data centres scattered around the globe, while CSCs using cloud services have the desire and even necessity to know the location of their data. In addition, there may

be issues of legal jurisdiction in the event of dispute and uncertainty about the applicable law. These issues are due to these different national legal frameworks and uncertainties about applicable law, data location and the free flow of data ranks concerns arisen amongst the potential cloud adopters, particularly for large enterprises already using the cloud[9]. This is in particular related to complexities of managing services and usage patterns that span multiple jurisdictions and in relation to trust and security in fields such as data protection, contracts and consumer protection. This could mean there could be a complex value chain with stakeholders and conflicting agreements, especially when the SME is procuring cloud to develop their own SaaS.

Table 20. Use case 15: CSP providing services under different regulations

Identification	**Title**	CSP providing services under different regulations (Choice of Law)
	SME Maturity	• Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data
	Short description	The Choice of law clause is a term of a contract in which parties specify that any dispute arising under the SLA shall be governed by in accordance with the laws of a particular jurisdiction. Since most of the major CSPs have headquarters in the United States of Americas, many of these CSP's have designated the governing law of the state they have their headquarters applicable to the agreement. The SME has done diligence on what CSP would fit its SaaS and business ambitions best with regard to the provided IaaS. However, it did not notice the choice of law the SLA is governed by. As the SME is providing SaaS to end-users being consumers in the EU member state where it is based, it is obliged to provide the services under the laws of that member state, including consumer right provisions. Therefore, the supply chain is not workable for this SME as it cannot hold its IaaS supplier accountable or responsible if certain issues arise. The SME will bear the full liability

[9] Eurostat News Release 9 December 2014 (latest statistics to date).

		towards its end-users without any recourse, which happened several times for this SaaS SME.
	Cloud Actors	Cloud Service Provider as PaaS Provider, SME as Cloud Service Partner and SMEs customer as Cloud Service Customer.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal compliance criteria	Mandatory rules cannot be avoided if the main activity takes place in the country of the SME or its end-users within the EU. Before looking for appropriate CSPs, and finding and assessing the terms and conditions (including SLA) that may be applicable in the relationship between such CSP and SME, the SME should identify the main legal compliance criteria relevant in (1) the local regulation of the SME and the countries in where the SME would like to do business and (2) the laws of the applicable governing law.
Preconditions and Requirements	**Security and privacy requirements**	If Personal data is involved the data protection regulation and legislation of the data-subject is applicable as well.
	Additional preconditions and requirements (e.g., performance)	N/A
	Existing SLA standards and best practices to rely on	List of SLA standards/best practices to rely on: C-SIG SLA Guidelines
	Additional comments	N/A
Summary	All CSP and all CSCs (including SMEs) in every deployment model have to deal with Governing Law Issues, but it is especially a burdensome if the SME wishes to develop and exploit its respective services and products on top of cloud-based services, in particular either IaaS or PaaS. 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'.	

5.2.16. Use case 16: CSP providing data services for the health sector

Back-up, certifications and encryption are important services a CSP offers. In most cases the CSPs have several certifications, back-up programs and encryption possibilities, but

the customer and therefore the SME needs to be aware that those certifications, back-up programs and encryption tools will not necessarily apply to the cloud services they subscribed to.

Table 21. Use case 16: CSP providing data services for the health sector

Identification	**Title**	CSP providing data services for the health sector (Customer Back-Up and Encryption)
	SME Maturity	• Novice • Basic
	Base Use Case (cf., Deliverable 2.2)	• SD: Processing Sensitive Data • DI: Data Integrity
	Short description	An SME in the Health Sector who has built its SaaS application on an IaaS/PaaS from the CSP. Anyone in the health sector has to be compliant to mandatory sectorial standards and needs to have certain certifications. Furthermore, since this SME will process sensitive personal data, it also needs to encrypt the data in light of the applicable personal protection regulations in the EU. Even though many CSPs have such specific certifications, encryption possibilities and back up possibilities, in most cases the layers in the provided IaaS/PaaS where the customer of the SaaS CSP processes its sensitive and other data do not fall under these certifications, or encryption and back-up by default. This SME made the mistake in trusting that the provided certifications were applicable for that use, where it does not.
	Cloud Actors	Cloud Service Provider as IaaS/PaaS Provider, SME as Cloud Service Partner and SME's customer as Cloud Service Customer.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal compliance criteria	Before looking for appropriate IaaS/PaaS CSPs, and finding and assessing its certifications, terms and conditions that may be applicable in the relationship between such IaaS/PaaS CSP and the SME Health Tech company, firstly this SME needs to map the main legal compliance criteria it deems relevant for the Health Tech Sector. Furthermore, as the health sector industry is high-regulated, there are special requirements for vendors and

		their certifications, which include the right of the authority to be able to audit the vendors in the respective supply chain. Personal data is involved of data subjects for which the customer of the SME is primarily responsible as data controller, so the personal protection regulations in the EU is essential as well. These three main legal criteria should be well-known to any Health Tech company. The SaaS SME thereafter needs to make sure it can and will take the appropriate measures in order to fulfil all the sector specific requirements with the help of the CSP they have pre-selected.
Preconditions and Requirements	**Security and privacy requirements**	According to the applicable personal protection regulations in the EU, a data controller needs to make sure they take appropriate security measures which are covered with certifications and encryption measures.
	Additional preconditions and requirements (e.g., performance)	Back-Up
	Existing SLA standards and best practices to rely on	C-SIG SLA Guidelines
	Additional comments	N/A
Summary	Many CSPs have several backup, certifications and encryption offerings, however please note that the SME should make sure their own environment within that IaaS/PaaS is also certified, encrypted and back-ups according to the industry standard and policies. Never just tick the box and think it will all be alright.	

5.2.17. Use case 17: A SME terminating a contract with a CSP

Data deletion, including data retention should be addressed in the SLA, and the SaaS application should have embedded techniques to remove data and ensures that deleted data will not be recovered. It is not always clear how data deletion and data retention is covered by the CSP, unless data deletion and retention are required as per data protection laws and regulations.

Table 22. Use case 17: A SME terminating a contract with a CSP

Identification	**Title**	A SME terminating a contract with a CSP (Data deletion and data retention)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• SD: Processing Sensitive Data • DI: Data Integrity
	Short description	The case is simple, and will happen to all CSCs: an SME wished to terminate the MSA with a CSP, and then starts thinking about whether and to what extent the CSP will delete its data, after the SME has extracted and exported that data as much as possible. This SME, as will others, finds out that nothing is arranged for, and is left in the dark.
	Cloud Actors	CSP as vendor, and SME or end user as customer.
	Cloud Service life-cycle phase	• Operation • Termination
	Legal compliance criteria	In case of termination, there is no need and no purpose to process or store any data of the CSC or related data subjects anymore, so all data related to the specific user should be deleted. Data deletion should be the last data processing a CSP takes care of. However, there are several data retention regulations for different sets of data, and different contexts.
Preconditions and Requirements	**Security and privacy requirements**	Privacy requirements are involved by data deletion as based on the data protection act. Based on the privacy regulation, all personal data should be deleted if there is no lawful interest to store or process any more, but there are exceptions. For instance, for financial data the data retention period is in most EU member states seven years based on the local financial and tax laws and regulations, and even HR data has a different data retention period based on labour law. Furthermore, some CSPs do not have technical capabilities in place to strongly delete the data.
	Additional preconditions and requirements (e.g., performance)	After the internal check of what kind of data the SME process, the SME needs to assess if all the data processing are necessary for using the services. The basic for data storage is data minimisation, where an SME needs to process as less data as possible, to limit the consequences of a data breach, data loss or any unlawful processing.
	Existing SLA standards and best practices to rely on	ISO/IEC 19086 CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines
	Additional comments	N/A
Summary	The requirements for data deletion and data retention based on the different laws and regulations are mostly not the same and contain different periods and	

	requirements. Therefore, the basics for data processing should be data minimisation. Furthermore, the SME should assess before it will look to an appropriate CSP all types of data it processes and the relevant data retention periods, as well as if the CSP has the correct technique to delete the data without the possibility to recover the deleted data. Before entering into an agreement with a CSP, the SME should assess if data deletion is possible if all data will be deleted. Thereafter, the SME should identify and landscape what kind of data its stores, process etc. and the related retention requirements of the different laws and regulations.

5.2.18. Use case 18: CSP migrating data between different jurisdictions

The location(s) where personal data may be stored or otherwise processed by the CSP is relevant for a SME as any CSC, whether it has one or more entities and whether or not it is active different geographical locations, as each country has different regulations regarding personal data and where such personal data may be stored and processed. In this case, the SME has entities in a dozen countries.

Table 23. Use case 18: CSP migrating data between different jurisdictions

Identification	**Title**	CSP migrating data between different jurisdictions (data location)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• SD: Processing Sensitive Data
	Short description	Since both within the European Union and outside the EU each country has different laws and regulations regarding personal data protection, the data location where the SME is active is relevant as well as the data location of the server of the CSP. In this case it concerns an SME active in a dozen countries and wishes to migrate to cloud services its HR data which concerns almost 100% personal data. In some jurisdictions, such HR data is even especially arranged in the law. If an entity of a SME is based in Russia and the headquarter is within the European Union, then it is not allowed by local law to store personal data, including HR data outside of Russia. The server of the CSP should be based in Russia, and in some cases the CSP will cooperate with a local data centre where a back-up copy will be stored on a data location in the European Union. This is not only relevant in Russia, as the same applies for Germany, for example. This SME segmented the data in advance, and together with its legal counsel architected where what data is to be stored, what back-up mechanisms should apply,

		and with success opened the dialogue with the relevant CSP.
	Cloud Actors	CSP as vendor, SME as customer, and its employees as data subjects.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal compliance criteria	Before looking for appropriate CSPs, the data and cloud architecture of the SME should be landscaped on what kind of (personal) data the SME is required to process on which location. Thereafter the SME should identify the local governing laws on data protection who are applicable to the SME and the countries where the SME would like to do business.
Preconditions and Requirements	**Security and privacy requirements**	If personal data is involved the data protection regulation and legislation of the data subject is applicable, and the place where the location of the server is as well.
	Additional preconditions and requirements (e.g., performance)	After the internal check of the SME on the above, the SME can start with landscaping and pre-assessing of which CSP would be able to deliver, and where the data locations of the CSP are.
	Existing SLA standards and best practices to rely on	CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines
	Additional comments	N/A
Summary	Data location is very important to comply with the local laws and regulations, which should always be discussed and agreed between the CSP and the SME. This is not a problem of the SME only; the CSP has similar and parallel problems to solve as it needs to comply with the local laws and legislation as well if it processed data for a CSC. Both CSPs and SMEs each have to deal with local laws and regulations. Especially for SMEs who have more entities and not all of them are based within the European Union a SME needs to assess what kind of laws and regulations are applicable on the different types of data even a SME stores and process. Such assessment could have the result that the SME cannot choose for one data location as the local data protection act does not allow this, and has to choose different locations.	

5.2.19. Use case 19: CSP providing data portability vendor Lock-in of SaaS applications

Vendor lock-in is a situation in which a customer using a product or service cannot easily switch or otherwise migrate (part of) its data to product or service of another vendor. Vendor lock-in is not exclusive to cloud services. Vendor lock-in is usually the result of outdated or just different technologies and methodologies of data formatting and making available data records that are incompatible with those of other vendors. However, it can also be caused by contract constraints, among others. In conjunction with data portability, the concerns of SME's across Europe regarding the risk of vendor lock-in is

one the most common barriers for adoption of cloud. In this case the SME is CSC and found out in a later phase that extracting and exporting its data to another part of the same CSPs SaaS was burdensome, let alone doing the same to another CSP impossible.

Table 24. Use case 19: CSP providing data portability vendor Lock-in of SaaS applications

Identification	**Title**	CSP providing data portability vendor Lock-in of SaaS CRM applications
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • CB: Cloud Bursting • SD: Processing Sensitive Data
	Short description	A European SME who has formally used CRM SaaS to keep track of its customer relationship management and sales cycle would like to switch certain part of its data to another account in the same CRM SaaS, and – when that did not work out – to switch that data to another CSP. This in turn requires the ability to migrate data between different environments or providers. However, the former CRM SaaS did not specify anything on data portability, data format, what data would exactly be possible to migrate, and what not, or whether metadata would be part of that. The SME settled for getting part of its data out in a structured, workable way, where the remainder of its data cannot be extracted or otherwise exported in a suitable way so basically lost the latter data and related analytics.
	Cloud Actors	SaaS CRM Cloud Service Provider, SME Cloud Service Customer.
	Cloud Service life-cycle phase	• Operation • Termination
	Legal compliance criteria	Before looking for appropriate CRM SaaS CSPs, and then finding and assessing the terms and conditions (including SLA) that may be applicable in the relationship between such CRM SaaS CSP and the SME, first, the SME needs to look in to the data formats, data export policies, termination and other data portability related clauses. Furthermore, if personal data is involved, data protection regulation and legislation is applicable as well. Also for the CSP, which is an argument to highlight when having any discussion with a CSP.
Preconditions and Requirements	**Security and privacy requirements**	The General Data Protection Regulation (GDPR) adopted in April 2016 creates a new right to data portability for data subjects with regards to its

		own personal data a CSP as data controller or processor processes in any way. This also means that data subjects have the right to extract their personal data from the SME in this use case.
	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	C-SIG SLA Guidelines
	Additional comments	Other topics cover data portability as well, such as free flow of data. Insuring data portability is a relevant objective of European policies in the context of the Digital Single Market strategy. The DSM strategy identified the lack of data portability as a potential barrier, noticing the shortcomings of cloud contracts in this field.
Summary	Data portability is another very important topic which should always be addressed by everyone who is willing or using the cloud. In case personal data is involved, data protection regulation and legislation is applicable to both CSC as well as the CSP, which is an argument to highlight when having any discussion with a CSP. In case the CSP is not willing to adapt the terms, it is advisable to look further to other alternatives.	

5.2.20. Use case 20: SME looking for Information Security Incident Management

Security incidents are an ongoing topic in the newspapers nowadays, and no one likes to be in the headlines because of a security incident, next to other obvious reasons why to avoid and be prepared for security incidents. However, realistically every organisation, SMEs included will at some point be subject to or otherwise involved in a security incident. Besides and quite important as well, there are several current and upcoming mandatory regulations that both CSPs and CSC need to comply with. So, there are quite some reasons to address information security incident management in the SLA.

Table 25. Use case 20: SME looking for Information Security Incident Management

Identification	**Title**	SME looking for Information Security Incident Management
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data • DI: Data Integrity
	Short description	As per an above-average awareness level as per security breaches in its sector, being the financial services industry, this SME is quite concerned about keeping its data safe while also complying to current and upcoming regulation.

		With all the topics in the newspapers on security incidents, every SME should be keen on the management of those incidents, and this SME actually does. Besides that, new regulations such as the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive with daunting high penalties are a trigger as well. However, it is not easy for the SME to obtain the right in-depth information from the CSP it needs to assess the risks, the way breach notification is taken care of, to what extent and how fast, and how incidents are managed and repeat-incidents avoided.
	Cloud Actors	SME or end user as user.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal compliance criteria	Before entering into an agreement with a CSP, the SME should assess how the CSP will manage and report any information security incidents. Thereafter, the SME should identify and landscape what kind of laws and regulations are applicable; local law, European laws or sectoral regulations. In the Netherlands, and from May 2018 in each member state; if you are a CSC, SME or not, and there is an availability or confidentiality breach of (personal) data which is not encrypted, the SME needs to notify the Data Protection Authority, the sectorial authority (if any), the CERT of the member state and the data subject of such data breach. Such notification requires certain information about the security incident and how the breach will be managed. Besides that, the breach will have consequences for the availability and the trustworthiness of the services.
Preconditions and Requirements	**Security and privacy requirements**	Security and privacy requirements are essential in information security incident management. The CSP should manage and report all the security incidents, note that not all incidents needs to be notified to the authorities.
	Additional preconditions and requirements (e.g., performance)	The SME and CSP should agree on how and when security incidents will be notified, especially the time frame after the discovery of the incident by the CSP and the notification to the SME. Preferably notification to the SME needs to be done at least within 48 hours after discovering of an information security incident.
	Existing SLA standards and best practices to rely on	ISO/IEC 19086 CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines
	Additional comments	N/A

Summary	Related to information security incidents there are several notification acts in case there is a breach with personal data. The SLA needs to assess what kind of proceedings the CSP has for notification, monitoring and management thereof. However, both parties are responsible for the information security management and cooperation to prevent this is a must.

5.2.21. Use case 21: CSP allowing data access for law enforcement

Based on several laws and regulations certain government authorities are allowed to request access to the data centre and other systems CSP. Based on the NSA stories users do not trust the access of the government and quite a few CSPs have insufficient knowledge and processes in place to deal with such request of a government authority, where some CSP in such real-life case tend to more take their own interest in account than fight for their CSC. In the SLA should be stated how the CSP will proceed and deal with such request.

Table 26. Use case 21: CSP allowing data access for law enforcement

Identification	**Title**	CSP allowing data access for law enforcement (Law enforcement access)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • SD: Processing Sensitive Data
	Short description	This use case is from an SME CSP that is quite advanced and knowledgeable about data access requests by authorities, and it is good to consider the do's and don'ts. Most CSPs do not know what to do if access to data is requested from a government authority and may give the government authority the wrong access without assessing such request. Generally, the scope of the formal requests to obtain access is too broad instead of a detailed scope, because the authority does not yet exactly know what kind of data they need to know. However, fishing by the government authorities is not allowed. CSPs needs to check the scope of the request to access and should provide as little information and access as possible, keeping in mind the contractual, ethical and trust relationship they have with their CSC. A CSC expect a CSP to stand up for the rights of the CSC. Furthermore, if a CSP gives access within the scope then it should not affect more data protection infringements than the strictly necessary. Any CSC, SMEs included, should request a detailed data access policy of the CSP itself with the processes and consequences.

	Cloud Actors	CSP as vendor, and SME as customer.
	Cloud Service life-cycle phase	• Operation • Termination
	Legal compliance criteria	Before a CSP gives the government authority access it should assess and identify what the legal ground is on which the government authority request for access and if such authority is authorised to get access within a detailed scope of request. The SME should identify and landscape the related laws and regulations for such request.
Preconditions and Requirements	**Security and privacy requirements**	Security and privacy requirements are involved by law enforcement access. The CSP has the obligation to protect the security and privacy of data subjects even by a request of a government authority, and the privacy should not be breached more than necessary.
	Additional preconditions and requirements (e.g., performance)	The CSP should provide a minimum of information and data within the scope of the request.
	Existing SLA standards and best practices to rely on	ISO/IEC 19086 CSCC Practical Guide to Cloud SLAs C-SIG SLA Guidelines
	Additional comments	N/A
Summary	The requirements for providing access to government authorities are most of the time too broad, as well the request itself. Therefore, a CSP need always to check the legal ground and scope of the request, and provide as less information as possible to prevent of more privacy breaches based on data protection acts. Any CSC, SMEs included should request a detailed data access policy of the CSP to familiarize itself with the processes and consequences.	

5.2.22. Use case 22: SME migrating to IaaS with several duration periods in the agreement

With the use of a SaaS application there are several duration periods and data retention periods applicable, either set forth in the related MSA or SLA or not. Such as the subscription term of the MSA, the access period to the SaaS, the availability of the data in the SaaS, the retention period data needs to be stored/archived by the CSP for legal purposed, and so on. The duration and qualification of each can be totally different. These several duration periods of subscription, access, use and audit of the SaaS should be clearly understood by the CSC, ad documented between CSP and CSC. However, even CSP have not quite thought over these different duration periods, and some are also not easy to recognize.

Table 27. Use case 22: SME migrating to IaaS with several duration periods in the agreement

Identification	**Title**	SME migrating to IaaS with several duration periods in the agreement (duration of different terms of the SaaS application)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • CB: Cloud Bursting
	Short description	This SME is migrating its infrastructure to IaaS of a major CSP. Being a software company itself does not necessarily mean to have the necessary knowledge for migrating to the SaaS. And, to start with, in order to provide a good proposal and business model based on subscription fees this SME needs to know what kind of different duration period are applicable, and what the financial, technical and operational consequences are. In this case for example (i) the MSA is for an indefinite period and the start is at the day of signing, this is the first duration period (ii) the MSA is effective at the moment of signing, but only after implementation of the SaaS in general and then the deployment of a customer a user will be able to access to SaaS, on which date the one-year subscription starts between the SME and its customer. This is the second duration period. Thirdly (iii), the subscription is based on the actual use of content, which means that the duration of use is shorter than the duration of the right to access. Two more for this use case, is (iv) the data retention period during with the CSP is required by law to retain certain data, and (v) the duration the SME and its customers are entitled to extract and export data.
	Cloud Actors	CSP as vendor, the SME as CSC as well as a CSP, and SME customer as the end-user.
	Cloud Service life-cycle phase	Acquisition Operation Termination
	Legal compliance criteria	N/A
Preconditions and Requirements	**Security and privacy requirements**	N/A
	Additional preconditions and requirements (e.g., performance)	N/A
	Existing SLA standards and best practices to rely on	N/A
	Additional comments	N/A

Summary	In order to make a business model based on subscription fees where access and use of the SaaS application depends on payment and the amount of time to use is limited, the SaaS provider should assess all those aspects which are relevant for a subscription business model, in order to have a good proposal and agreement. In short, both the CSP and CSC need to familiarize themselves with the numerous duration periods, landscape and structure those before discussing business and legal terms and conditions.

5.2.23. Use case 23: SME setting up its own hybrid cloud ecosystem

Cloud computing has been a trending topic over the last 10 years but only recently a reasonably matured common definition of cloud computing has been established. However, both CSPs and CSCs tend to define cloud services, service models, deployment models, uptime and other availability differently which leads to confusion and conflicts. Especially when a CSC such as the techno starter SMEs in this use case, would like to set up its own hybrid cloud ecosystem to trust and build its business on, and therefore uses multiple CSPs to build this ecosystem.

Table 28. Use case 23: SME setting up its own hybrid cloud ecosystem

Identification	**Title**	SME setting up its own hybrid cloud ecosystem (Cloud SLA Definitions)
	SME Maturity	• Novice • Basic • Experienced
	Base Use Case (cf., Deliverable 2.2)	• AP: App on a Cloud • CB: Cloud Bursting
	Short description	This SME is a small start-up but is envisioning to be number 1 in its market, globally. It will need cloud service to do so, and as per different technical, business, risk mitigation and risk reasons it is working on architecting a hybrid ecosystem where several major as well as niche CSPs will be involved. However, all CSPs define their definitions and legal terms differently which makes it hard to create a clear landscape of what rights and obligation the SME has towards the respective CSP, and what rights and obligations it can arrange for with its own customers and end-users. Analysing legal documentation from A to Z concerning cloud services such as SLAs is quite cumbersome and time and resources consuming, CSPs even use different quantitative attributes, metrics, measurements and remedies. The SME feels that some CSPs prefer to keep their applicable documentation less transparent than their customers wish for, and the CSPs would be able to. Getting to the bottom of Master Service Agreements, SLAs and other contractual

		arrangements is time-consuming, and a SME, especially a start-up does not have those resources. It will either lead in delay in its business plans, or making the wrong decisions which will be very costly in a later phase.
	Cloud Actors	CSP as vendor. SME as customer.
	Cloud Service life-cycle phase	• Acquisition • Operation
	Legal compliance criteria	It all starts with unambiguous and technology neutral definitions. Keeping the definitions of all relevant documentation well-defined and unambiguous is important to ensure that CSPs and CSCs both have a common understanding and clear communication of that to expect from each other and the services contracted. Currently, the most up to date definitions that have been globally validated, have recently been re-endorsed by the European Commission and are used by many leading companies, government bodies and other organizations. These are contained in the EC Cloud SLA Standardisation Guidelines.
Preconditions and Requirements	**Security and privacy requirements**	N/A
	Additional preconditions and requirements (e.g., performance)	99.95% uptime will not necessarily mean 99.95% uptime since many of the CSP define uptime in multiple ways. For instance, when the measurement starts, what is in or out of scope of such measurement, and so on.
	Existing SLA standards and best practices to rely on	List of SLA standards/best practices to rely on: ISO/IEC 19086 C-SIG SLA Guidelines Cloud Quadrants Report
	Additional comments	N/A
Summary	Without having clear unambiguous definitions, it is impossible to diligently procure cloud services. This goes for generally all procurement but 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 definitions and terms. The same issues arise regarding the various languages.	

5.2.24. 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 tables represent the priorities of the CRM elements for every

use case analysed. 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 important given to one elements of the CRM with respect to others depends on the type of use case analysed (including the type of domain, type of customers, the specific requirements for each use case, etc.).

Table 29. CRM - Use Cases Coverage (part 1)

		CRM element importance for every use case (PART 1) (red: highest, yellow: medium, green: lowest)							
Item	Name of CRM element	Fintech (Financial sector) (UC1)	Estonian Governmental Cloud (UC2)	ConsultLess, SME for using SaaS (UC3)	SMEs migrating from one SaaS CSP to the other (UC4)	Cloud Brokering: Cloud Chargeback and Showback (UC5)	Distribution of SME Training Material to Mobile Employees (UC6)	EasyAgriSelling, SME using IaaS/PaaS (UC7)	Video storage and streaming from the Cloud (UC8)
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								
12	Nr. of pages								

		CRM element importance for every use case (PART 1) (red: highest, yellow: medium, green: lowest)							
Item	Name of CRM element	Fintech (Financial sector) (UC1)	Estonian Governmental Cloud (UC2)	ConsultLess, SME for using SaaS (UC3)	SMEs migrating from one SaaS CSP to the other (UC4)	Cloud Brokering: Cloud Chargeback and Showback (UC5)	Distribution of SME Training Material to Mobile Employees (UC6)	EasyAgriSelling, SME using IaaS/PaaS (UC7)	Video storage and streaming from the Cloud (UC8)
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								

		CRM element importance for every use case (PART 1) (red: highest, yellow: medium, green: lowest)							
Item	Name of CRM element	Fintech (Financial sector) (UC1)	Estonian Governmental Cloud (UC2)	ConsultLess, SME for using SaaS (UC3)	SMEs migrating from one SaaS CSP to the other (UC4)	Cloud Brokering: Cloud Chargeback and Showback (UC5)	Distribution of SME Training Material to Mobile Employees (UC6)	EasyAgriSelling, SME using IaaS/PaaS (UC7)	Video storage and streaming from the Cloud (UC8)
23	General Carveouts								
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								

Table 30. CRM - Use Cases Coverage (part 2)

		CRM element importance for every use case (PART 2) (red: highest, yellow: medium, green: lowest)					
Item	Name of CRM element	Cloud-based Development and Testing (UC9)	Logistics and Project Management (UC10)	Local Government Services in Hybrid Cloud (UC11)	Payroll Processing in the Cloud (UC12)	CSP specifying Carve-outs in its cloud service terms (UC13)	CSP changing SLA at operation time (UC14)
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						
12	Nr. of pages						

		CRM element importance for every use case (PART 2) (red: highest, yellow: medium, green: lowest)					
Item	Name of CRM element	Cloud-based Development and Testing (UC9)	Logistics and Project Management (UC10)	Local Government Services in Hybrid Cloud (UC11)	Payroll Processing in the Cloud (UC12)	CSP specifying Carve-outs in its cloud service terms (UC13)	CSP changing SLA at operation time (UC14)
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						
24	Specified SLO metrics						

		CRM element importance for every use case (PART 2) (red: highest, yellow: medium, green: lowest)					
Item	Name of CRM element	Cloud-based Development and Testing (UC9)	Logistics and Project Management (UC10)	Local Government Services in Hybrid Cloud (UC11)	Payroll Processing in the Cloud (UC12)	CSP specifying Carve-outs in its cloud service terms (UC13)	CSP changing SLA at operation time (UC14)
25	General SLOs						
26	Cloud Service Performance SLOs						
27	Service Reliability SLOs						
28	Data Management SLOs						
29	Security SLOs						
30	Personal Data Protection SLOs						

Table 31. CRM - Use Cases Coverage (part 3)

		CRM element importance for every use case (PART 3) (red: highest, yellow: medium, green: lowest)								
Item	Name of CRM element	CSP providing services under different regulations (UC15)	CSP providing data services for the health sector (UC16)	A SME terminating a contract with a CSP (UC17)	CSP migrating data between different jurisdictions (UC18)	CSP providing data portability vendor Lock-in of SaaS applications (UC19)	ISME looking for Information Security Incident Management (UC20)	CSP allowing data access for law enforcement access (UC21)	SME migrating to IaaS with several duration periods in the agreement (UC22)	SME setting up its own hybrid cloud ecosystem (UC23)
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									
12	Nr. of pages									

		CRM element importance for every use case (PART 3) (red: highest, yellow: medium, green: lowest)								
Item	Name of CRM element	CSP providing services under different regulations (UC15)	CSP providing data services for the health sector (UC16)	A SME terminating a contract with a CSP (UC17)	CSP migrating data between different jurisdictions (UC18)	CSP providing data portability vendor Lock-in of SaaS applications (UC19)	ISME looking for Information Security Incident Management (UC20)	CSP allowing data access for law enforcement access (UC21)	SME migrating to IaaS with several duration periods in the agreement (UC22)	SME setting up its own hybrid cloud ecosystem (UC23)
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									
24	Specified SLO metrics									

		CRM element importance for every use case (PART 3) (red: highest, yellow: medium, green: lowest)								
Item	Name of CRM element	CSP providing services under different regulations (UC15)	CSP providing data services for the health sector (UC16)	A SME terminating a contract with a CSP (UC17)	CSP migrating data between different jurisdictions (UC18)	CSP providing data portability vendor Lock-in of SaaS applications (UC19)	ISME looking for Information Security Incident Management (UC20)	CSP allowing data access for law enforcement access (UC21)	SME migrating to IaaS with several duration periods in the agreement (UC22)	SME setting up its own hybrid cloud ecosystem (UC23)
25	General SLOs									
26	Cloud Service Performance SLOs									
27	Service Reliability SLOs									
28	Data Management SLOs									
29	Security SLOs									
30	Personal Data Protection SLOs									

5.3. Summary takeaways

Summary takeaways

- The CRM has been validated with the analysis of 23 use cases taken from different business domains.
- Such validation has allowed us to identify the importance/applicability of every CRM element for every use case.
- A template is used for a comprehensive analysis of the use cases. The implementation of the template for every use case is used to identify the importance/applicability of every CRM element.
- The importance/applicability of every CRM element depends on aspects such as the actors involved in the use case, the sensitivity of the data managed, the type of cloud services to use or the regulations to implement.
- The template classifies every use case according to the five base use cases defined the ETSI CSC report. It also classifies every use cases according to the Cloud Service Life Cycle created in Deliverable 2.2. This information is used by the recommendation methodology described in the following section.

6. CRM recommendation for new use cases

Very often, companies decide to move their business to the cloud without really knowing what aspects to tackle: Do I have to strengthen performance aspects? How important is security for my business? Do I have to consider potential legal implications when offering my service? This section proposes a methodology that can be used to provide companies with a recommendation based on the CRM that can help them to choose the best possible SLA according to their business target.

As described in previous sections, the CRM provides with a framework that classifies the most relevant aspects that a CSP has to consider when providing cloud services based on SLAs to its customers. The CRM can be used to publish the security levels that a CSP is providing or to know how transparent is a CSP with respect to all the non-functional features associated with the cloud service provision. The CRM can also be used to recommend the most suitable CSPs to customers according to their requirements. This will be demonstrated in Section 7 with the usage of assessment algorithms to evaluate CSPs based on the quantification of the elements of the CRM.

However, the CRM offers greater potential beyond a recommendation means for customers. An additional added value of the CRM consists of recommending to CSPs the most relevant elements of the CRM. In D2.3 an initial validation exercise was done to evaluate use cases from different domains (financial, public and SME sectors) and analyse them with respect to the CRM. The result of the study shows that some elements of the CRM that are more important than others depending on the characteristics of the use case. For instance, the legal aspects of the CRM were more important for the use cases that focused on the public sector rather than the rest of the use cases.

One of the objectives of D2.4 is to go in depth into this direction and to provide a methodology that allows to recommend what elements of the CRM are more important, according to the type of business case analysed. This process is done in two phases (Figure 9):

- **Phase 1 – Clustering use cases**. Use cases that share common characteristics (either due to their domain or business requirements) can be organized in representative domains. These representative domains denote the level of importance of each CRM element for a specific domain. Given a set of m use cases, they can be grouped into n groups, being CRM_i one of these groups, such that:

  $$CRM_i \ (i=1..n), \text{for } n \text{ representative domains}$$

This phase uses clustering algorithms (see Section 6.2) which, for a given input (i.e., the use cases coming from Section 5.2), estimates the level of importance of the CRM element for the identified clusters.

- **Phase 2: Recommendation of a CRM_i for new use cases**. In this phase, new business cases can be assigned to any of the n representative domains identified in phase 1. The corresponding CRM_i is returned which contains a specific report on the level of importance of every element of the CRM.

The following picture depicts this process, being $CRM_{domains}$ the clusters where the use cases are grouped:

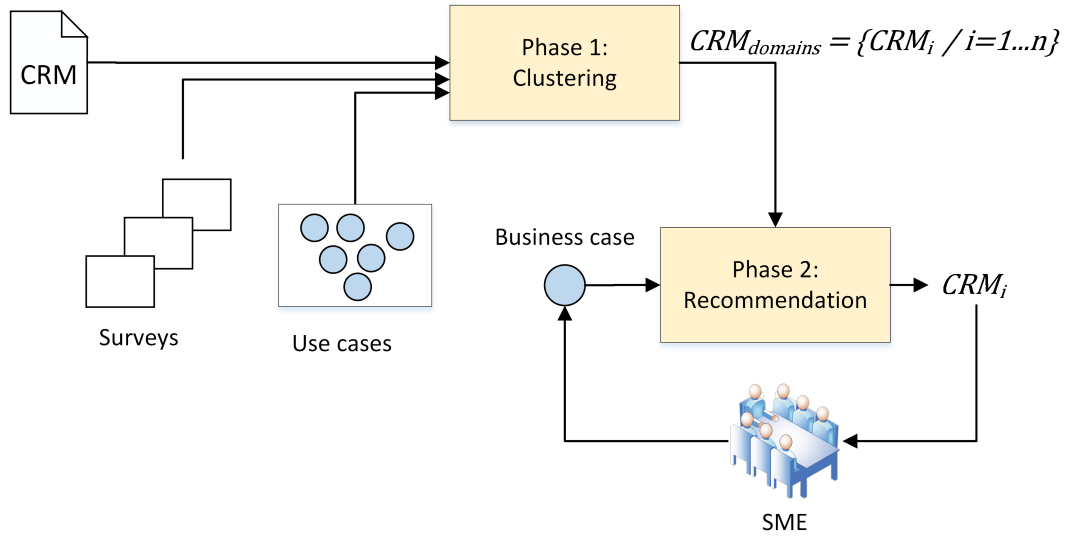

Figure 9. Recommendation process based on the CRM and use cases

The output of this process is a recommendation based on the CRM, CRM_i, that contains the level of importance for every element of the CRM. This will provide SMEs with the information they need to know about what are the aspects of the CRM that need special attention, according to their specific business case.

The following subsections detail the phases involved in the recommendation process.

6.1. Input data: use cases analysis

We have used as input a total of 23 use cases: 4 use cases analysed in D2.3 (which have been extended to be included in D2.4) and 19 new use cases added to Section 5 of this deliverable. For every use case (from now on, we will refer to the new use case as "sample") the information used as input for the recommendation process is:

- **The *base use cases*** that corresponds to every sample. A *base use case* is one of the five types identified in the ETSI CSC report: Application to the Cloud (AP),

Cloud Bursting (CB), processing sensitive data (SD), high availability (HA), Data integrity (DI).

- ***The stage of the life cycle*** where the use case operates (acquisition, operation or termination).
- ***A level of importance for every element of the CRM***, as high, medium or low.

As a result, we have represented every sample as a vector of 38 elements (5 elements correspond to the base use case, 3 elements to the stage of the life cycle and 30 for the elements of the CRM). These elements are quantified using a common scale (from 0 to 2). The quantified values are used as input for the clustering method used.

6.2. Phase 1: Applying clustering methodologies to the input data

The next step entails the classification of the input data in order to find the n most representative domains. To do so we have used clustering techniques that allow to group information according to similarities in the different dimensions that are part of the data analysed. Clustering techniques are widely used in machine learning and data mining. They represent an efficient and an accurate way to identify patterns and predict results and behaviours. Clustering techniques group data (apparently uncorrelated) into groups where the elements belonging to each group are more similar to each other than to those in the other groups. These groups, called clusters, are composed of a variable number of elements. Figure 10 represents a typical clustering representation of two-dimensional samples. Three clusters are clearly identified while there are still some samples (black dots) that cannot be assigned to any cluster (referred as "noise").

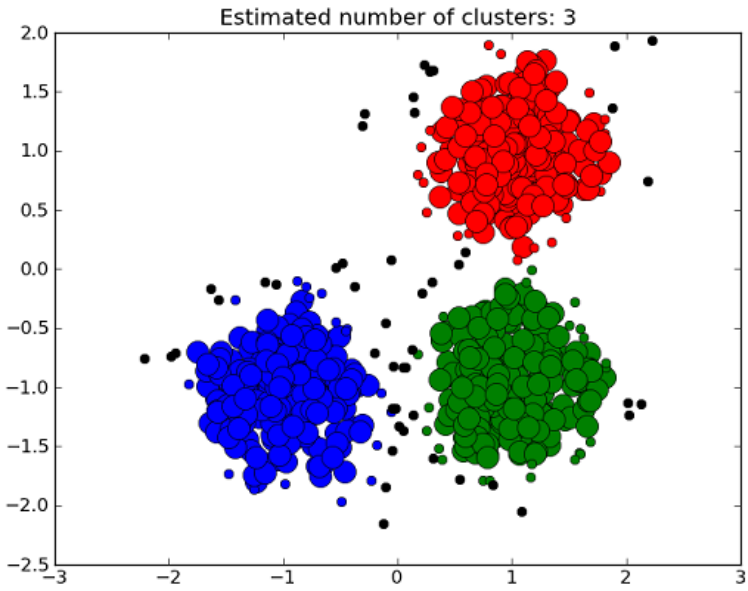

Figure 10. Example of clustering representation[10]

The rules to map elements to clusters depends on the clustering methodology used. There are several clustering techniques in the state of the art:

- Partitioning Method (i.e., K-means [11]). For a set of x elements, these methods build y clusters and assign every element to some of the y clusters, typically using Euclidean distances.
- Hierarchical Methods [12]. Decomposes the input data into a hierarchy which is classified according to the decomposition of the hierarchy. The clusters are identified according to the density (number of elements) of the classifications.
- Density-based Method (i.e., DBSCAN [10]). Unlike the partitioning methods, density based methods do not need to set the number of clusters in advance. Density-based methods dynamically create them according to a predefined expected density of elements in a certain area.
- Grid-Based Method (i.e., STING [13]). Clusters are organized in a grid and samples are assigned to each cell of the grid. Only cells with a minimum density (minimum number of elements) are considered as a cluster. Adjacent cells might be merged to get the expected density to create a cluster.

[10] https://cssanalytics.wordpress.com/2013/11/26/fast-threshold-clustering-algorithm-ftca/

- Model-Based Method (i.e., MCLUST [14]). Uses Gaussian statistical models to calculate the density of a finite collection of elements.
- Constraint-based Method (CBM [15]). This technique is used when the clusters are conditioned by some constraints that the elements have to match.

In SLA-Ready, the elements to classify (i.e., the samples) are not correlated and we do not know in advance how many clusters we will have. As we do not have any constraints for the elements that are part of any clusters, consequently we have chosen a density-based method to classify the elements that are part of our sample set.

While there are many techniques to deal with density-based clustering, we have used the DBSCAN approach for its simplicity and efficiency. DBSCAN calculates distances between the elements of the sample set to find out clusters. The algorithm is configured with two parameters:

- The minimum number of elements in a cluster, represented as m.
- The maximum distance between the elements of a cluster, represented as k.

Figure 11 depicts an example for the DBSCAN algorithm. One cluster is identified in red. The elements of this cluster are at a distance equal or less than the distance k. Elements C, B and N are not considered part of the red cluster as their distance to any element of the red cluster is greater than k. They might be part of a cluster if at least m other elements appear at a distance equal or less to k.

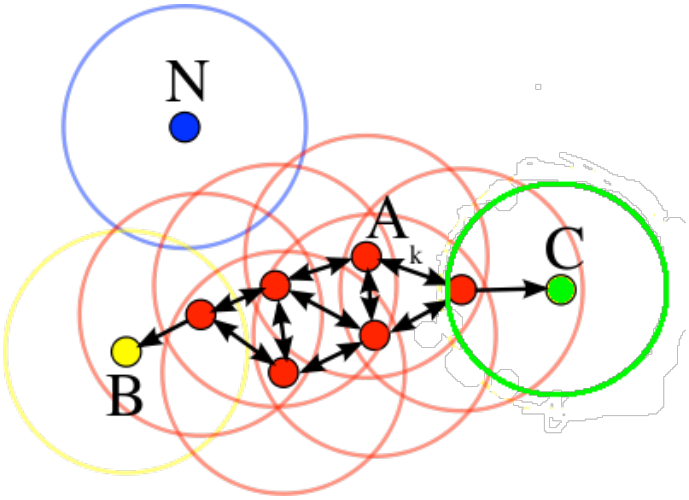

Figure 11. DBSCAN approach

One of the problems that clustering methodologies face when they are used is that very often the number of samples is fewer than the number of dimensions of every sample. This is exactly what happens in SLA-Ready, as we have 23 samples and every sample is

composed of 38 elements. This is a problem when applying clustering techniques as it makes difficult to find clusters where samples are at a distance k (as the number of samples is limited and the number of dimension per sample is big). To solve this problem, machine learning techniques use dimensionality reduction to decrease (without losing too much information) the number of elements of the sample. As an example, in SLA-Ready we have reduced the dimensions from 38 to 3 with a minimum loss of information, which will facilitate discovering clusters. While several algorithms can be found for dimensionality reduction [11], we have used a very well-known technique: PCA (Principal Component Analysis) [17].

PCA relies on the projection of information into a space with reduced dimensions. For example, if we have information defined on a space of three dimensions and we want to reduce it in one dimension, PCA will project the three dimension samples into a plane, which is used as new coordinates system. The projection is done trying to lose the minimum amount of information when projecting the samples to the new coordinates system. To do so, the distance between the samples and the new coordinate's axis is minimized.

In summary, the process that we have followed to cluster elements comprises three steps as depicted in the following picture:

Figure 12. Clustering process

- Step 1: Dimensionality reduction reduces the dimensions of the samples by using the PCA algorithm.
- Step 2: Clusters discovering finds clusters with the samples used as input by using DBSCAN.
- Step 3: Calculates the most representative sample for the clusters identified. To do so we have calculated the mean vector for all the samples that are part of the identified clusters.

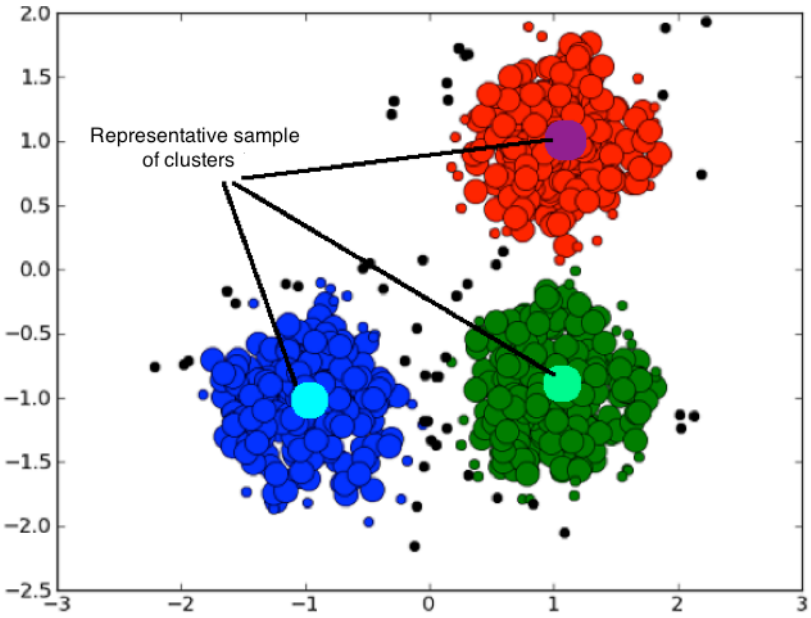

Figure 13. Example of representative vector for clusters

We have applied the clustering methodology to the samples available in SLA-Ready:

- In step 1 we have reduced the dimensionality of the samples from 38 to 3.
- In step 2 we have used DBSCAN to find the potential clusters for the samples. We have configured the DBSCAN algorithm with $k=2$ and $m=3$. This results in the identification of 3 clusters. As we have reduced the dimension of samples to three we can depict a 3D representation of the samples and clearly see the three clusters identified. Figure 14 depicts the results of the clustering. Red crosses samples are part of *cluster #1*. Green squares are grouped into *cluster #2* while blue diamonds are grouped in *cluster #3*. There is a sample (black circle) that is considered as noise and will not take part in the recommendation methodology.

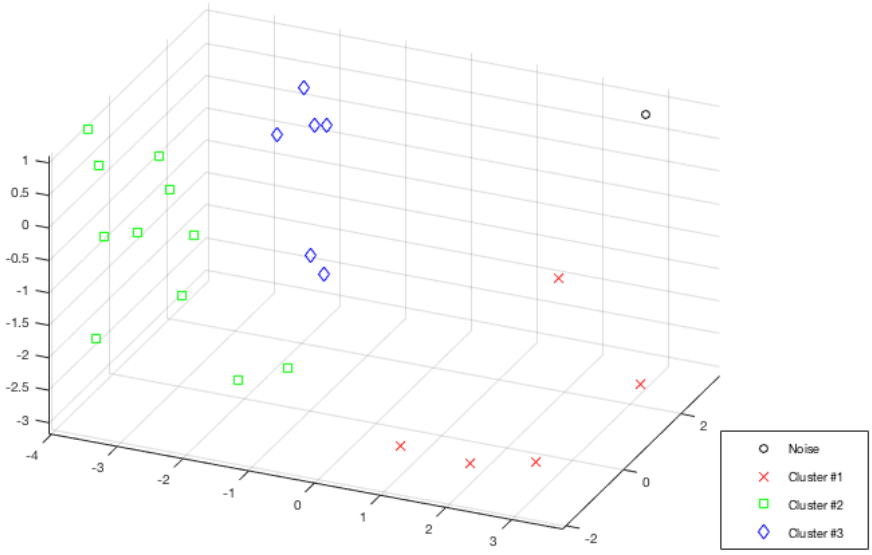

Figure 14. Clusters discovered for the SLA-Ready samples

- In step 3 the representative samples of each cluster are identified by calculating the mean among all the vectors that belong to the same cluster. Figure 15 represents these samples added to the samples of every cluster.

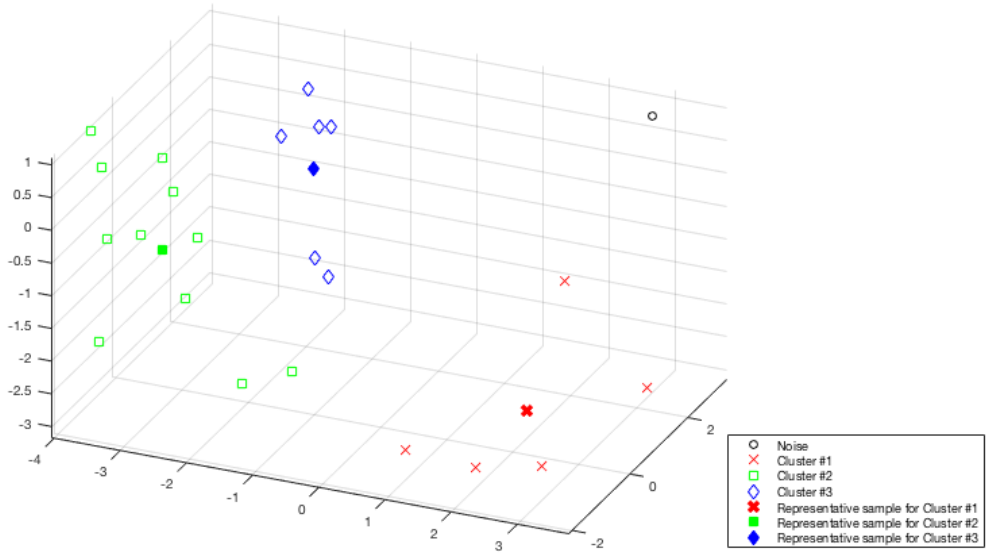

Figure 15. Clusters and representative samples for the SLA-Ready samples

Although Figure 15 depicts the representative samples after reducing their dimensions (otherwise it would not be possible to be represented), in practice the mean value is calculated using the non-reduced samples, as this representative vector will contain the recommendation data of all the CRM elements.

6.3. Phase 2: Assigning new use cases to clusters

The second phase of the methodology provides with the recommended level of importance for every element of the CRM, depending on the characteristics of the business case to evaluate. This is especially useful for SMEs that want to move applications to the cloud or simply want to explore new opportunities by providing their own cloud services. Very often these SMEs are not actually aware of how to manage the relationships to their customers in terms of SLAs, for example considering security or law enforcement aspects.

In this phase the recommendation methodology uses a subset of characteristics (non-technical) that describe the business case that the SME wants to evaluate. We have used only the fields included in the template of Table 5 that gives a high-level view of the service:

- **The base use case**, as one or more of the base use cases defined by the ETSI CSC.
- **The stage of the cloud service lifecycle** where the use case operates.

No further detail on any element of the CRM is required, since this is precisely the information that this recommendation methodology is providing.

The process starts by obtaining the nearest cluster to the business case to evaluate, and then return the representative sample calculated in phase 1. This is done by calculating the distance between the vector that represents the new use case (which contains 8 elements: 5 for the base use case and 3 for the life cycle stage) and the partial vectors of the representative samples. The representative sample with the minimum distance is the best possible recommendation, which is returned to the SME. Figure 16 depicts this process where a new sample (this is, a new business case) is compared with the clusters identified. The distance to each representative sample is then calculated (*d1*, *d2* and *d3* for clusters *#1*, *#2* and *#3* respectively). As *d3* is the minimum distance, we choose the *representative sample of cluster #3 as the recommendation result*.

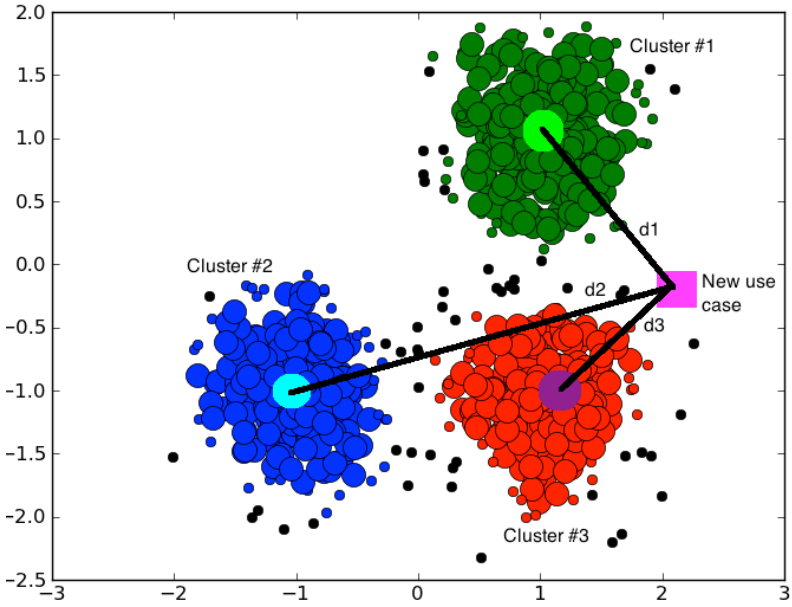

Figure 16. Example of recommendation based on distances between samples

This methodology is extensible. New business cases can provide with new samples that can change the representative sample of clusters, the number of clusters or the members of the clusters. In fact, machine learning techniques are indeed designed to dynamically adapt themselves to non-correlated samples coming into the system at any moment.

6.4. Recommendation methodology validation: Example 1

In this section we present the example of a company that is starting a new business and wants to be recommended about the SLA that should be provided to its customers:

> *This company provides IT services for hospitals and is moving towards providing computational resources for research activities required by hospitals. More specifically, this company provides computational resources for processing genetic based information from patients. The new service is designed in such a way that, depending on the workload, the data is moved between different clouds (public or private), in order to maximize efficiency. The service is also based on previous services that the company has moved to the cloud to save costs and increase performance. The company needs to change the service terms provided to their customers. As a result, a new SLA will have to be offered to its customers. In order to deal with the features of the new service this company is asking for a recommendation on the terms of the SLA to which they should pay more attention.*

Following the recommendation methodology described previously, the new service is analysed according to the requested parameters:

- **Base use case (according to ETSI CSC classification)**. The company is moving applications to the cloud (base use case: AP). It is also moving computational resources between different clouds depending on the workload (base use case CB). Finally, it is also processing sensitive data, as it deals with genetic information from patients of hospitals (base use case: SD). Therefore, we can classify the service as AP, CB and SD.
- **Stage of the life cycle**. The cloud is used during the operation of the service offered. As a result, we can classify the service in the *operation* stage.

Therefore, the sample to process will be the following:

Table 32. Classification of the use case of the example 1

Base use case					Life cycle stage		
AP	**CB**	**SD**	**DI**	**HA**	**Acq.**	**Op.**	**Term.**
YES	YES	YES	NO	NO	NO	YES	NO

After applying Phase 2 of the recommendation methodology, and having the clusters and representative samples described in Section 6.2 (and depicted in Figure 15), we can assign this business case to *cluster #2*. The recommendation on the CRM elements is based on the representative sample for *cluster #2*, which gives the following result.

CRM element	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Recommendation															

CRM element	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Recommendation															

Red: high importance. Yellow: medium importance. Green: Low importance

Figure 17. Recommendation results for the use case analysed in example 1

We can see from the results obtained that for the given use case the elements 28, 29 and 30 of the CRM are labelled as highly important. This is quite consistent with the characteristics of the use case analysed, as elements 28, 29 and 30 are related to data protection. This is consistent with the results obtained as the service to evaluate is focused on the management of sensitive data (genetics information from patients).

6.5. Recommendation methodology validation: Example 2

The following is the example of company that wants to move critical operations to the cloud:

> *A company wants to support the activities of a rail transport operator with cloud services (for example for incident response management). The target customer is a critical infrastructure provider (the rail transport operator), thus the cloud service must be reliable and with high availability.*

Following the recommendation methodology described in Section 6, the new service is analysed according to the requested parameters:

- **Base use case (according to ETSI CSC classification)**. The target of the service is to move the current operations carried by rail transport companies to the cloud. Therefore, we can initially classify it as AP (moving application to the cloud). Furthermore, in this use case there are strict requirements in regard to availability. The cloud services will be used upon a critical infrastructure that requires a high availability in order to properly and quick manage incidents. As a result, we can classify this service also as HA (High availability).
- **Stage of the life cycle**: The new service will be used at operation time. However, in this service it is paramount to consider also critical requirements, such as the expected availability or the response time. These considerations make us classify the use case also in the acquisition stage of the life cycle.

Therefore, the sample to process will be the following:

Table 33. Classification of the use case of the example 2

Base use case					Life cycle stage		
AP	**CB**	**SD**	**DI**	**HA**	**Acq.**	**Op.**	**Term.**
YES	NO	NO	NO	YES	YES	YES	NO

Applying Phase 2 of the recommendation methodology, and having the clusters and representative samples described in Section 6.2 (and depicted in Figure 18), we end up assigning this business case to *cluster #1*. The recommendation on the CRM elements is based on the representative sample for *cluster #1*, which gives the following result.

CRM element	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Recommendation															

CRM element	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Recommendation															

Red: high importance. Yellow: medium importance. Green: Low importance

Figure 18. Recommendation results for the use case analysed in example 2

Looking at the results we can see that for the given business case the elements 26, 27 and 28 of the CRM are labelled as highly important. This is quite consistent with the type of business case. Elements 26, 27 and 28 are "Cloud Service Performance SLOs", "Service Reliability SLOs" and "Data Management SLOs" which are indeed very important aspects for a cloud service built for a critical infrastructure as the one in this example 2.

6.6. Summary takeaways

Summary takeaways

- A novel recommendation methodology based on the CRM has been created to help potential new cloud customers/providers to identify the CRM Elements that are most relevant for their business case.
- The recommendation methodology uses the 23 use cases evaluated in Section 5. It utilizes clustering techniques to find the correlation among the given use cases.
- The result of the clustering technique is a set of use cases grouped in clusters. Every identified cluster has a representative CRM, which includes a specific level of importance (high, medium, low) for every CRM Element.
- The information used to group the use cases is: the base use cases (as defined by the ETSI CSC), the stage of the Cloud Service Life Cycle where the use case operates, and the level of importance identified for every CRM element.
- A high-level description of SME's business cases is used to identify the base use case (as defined by the ETSI CSC) and the stage of the Cloud Service Life Cycle where the SME's business case operates. With that information, the recommendation methodology maps every use case to the clusters discovered during the analysis and provides with the correspondent level of importance for every CRM element.

7. 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 development of the SLA-Readiness Index, mostly focused on the CSP assessment criteria designed by the consortium, the quantitative techniques used to perform the computation of the SLA-Readiness Index, and some developed proof of concept examples with real CSP data.

7.1. Motivation for the SLA-Readiness Index

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, as reported in D4.3 the SLA-Repository became a collection of cloud SLAs *analysed* according to the elements defined by the CRM (cf. Section 3). From the feedback received from stakeholders and Advisory Board (cf., D4.4), we concluded that the entries in the SLA-Repository 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 quantitative metric that could be used by cloud customers, mainly SMEs, to assess at a glance the CSP SLA.

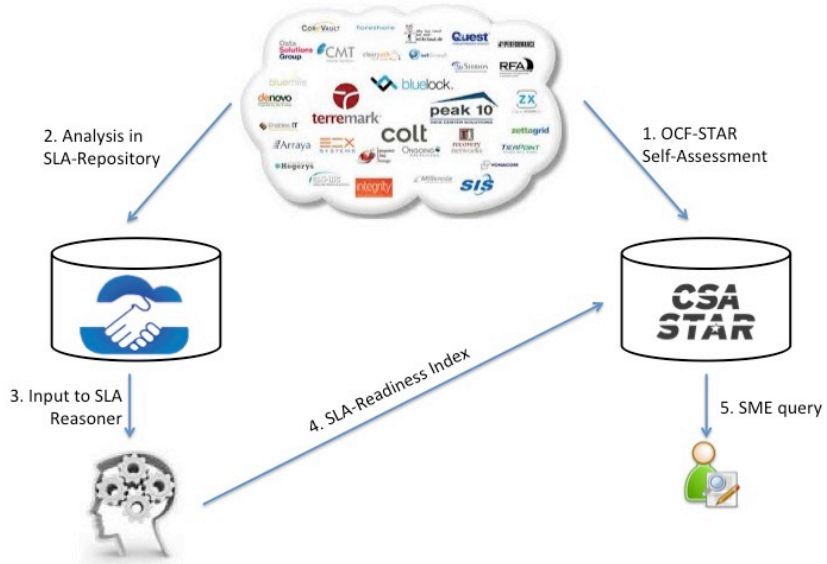

Figure 19. Computing the SLA-Readiness Index.

Figure 19 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 19.

7.1.1. 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, 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 [25], where CSPs self-assess the implementation of security controls based on the Consensus Assessment Initiative Questionnaire (i.e., CSA CAIQ [24]).

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 was used to develop the SLA-Readiness Index. Further details related to the SLA-Ready Index, including the analysis of received CSP answers to the questionnaire, are presented in D4.3.

7.1.2. Step 2: SLA-Repository

Once the CSPs have answered the questionnaire shown in Annex B, then it is feasible to store the received answers in the SLA-Repository for further exploitation. The current version of the repository is a collection of the received CSP questionnaires, although some initial efforts to develop a machine-readable version of the repository have already started by collaborating with projects like H2020 MUSA[11]. In order to support transparency in the cloud market, all CSPs answering the questionnaire have been asked to provide their consent for making their answers publicly available (cf., Annex C). More details related to the SLA-Ready Repository are presented in D4.3

7.1.3. Step 3: Computing the SLA-Readiness Index

The CSP SLA information collected into the SLA-Repository is structured in a way that allows for its quantitative reasoning; in particular, we refer to its *aggregation into a unique quantitative/qualitative level i.e., the SLA-Readiness Index*. At the state of the art,

[11] Please refer to http://www.musa-project.eu/. Last accessed on November 2016.

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.

An adequate aggregation technique can be applied to the qualitative data compiled from the CSP questionnaires to result in a numeric SLA-Readiness Index value. The latter 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. Section 7.3 further elaborates about the computation of the SLA-Readiness Index, and also presents some proof of concept examples based on real-world information from the SLA-Ready Repository.

7.1.4. Step 4: Using the SLA-Readiness Index

For each CSP entry on the SLA-Ready Repository it can be computed a unique SLA-Readiness Index, which can be then used as *entry-point* to provide more detailed information about the CSP SLA. The SLA-Readiness Index can be deployed (for public access) on the SLA-Ready website[12] and also on the CSA STAR webpage (e.g., Figure 20).

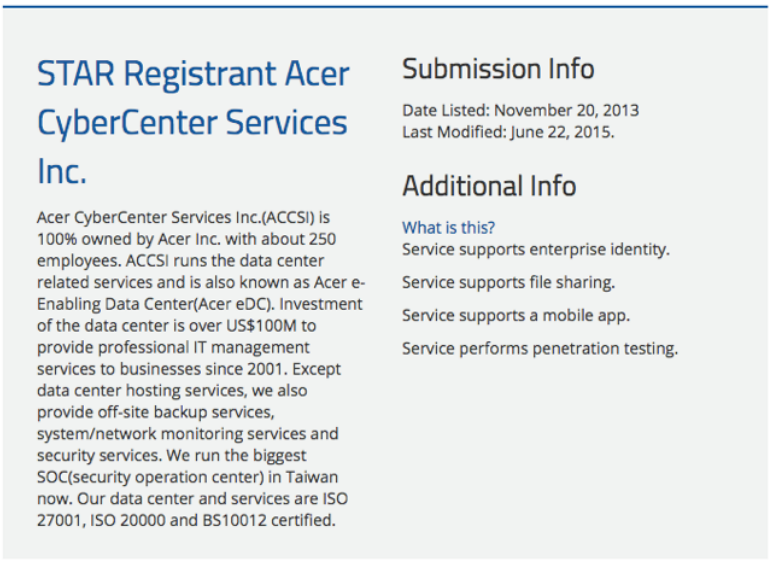

Figure 20. A CSP entry on CSA STAR - Additional Info

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

More details associated with publishing and using the SLA-Readiness Index are discussed in D4.3.

7.2. Techniques for the assessment of CSPs

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 briefly outline the state of the art in SLA assessments.

Li et al. [18] 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 [19] 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) [29]. 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) [27] that provides a ranking of the analysed providers.

Several activities are devoted to evaluating SLAs focused on security. Hegging [20] 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 provide with a structured methodology based on a quantitative evaluation of the controls that comprise the SLA. Although the aforementioned methodologies for cloud assessment are mainly focused on security controls, they can be easily translated to any set of controls included in a SLA as long as they are quantifiable.

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

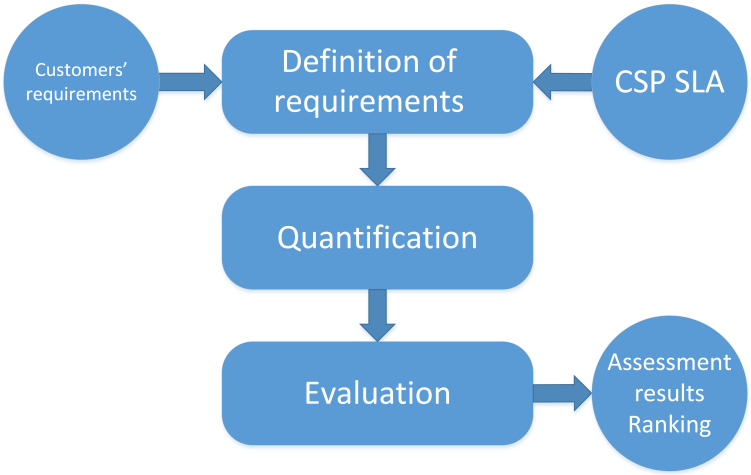

Figure 21. Stages comprising the quantitative SLA assessment

- **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 [21]). 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 tree (*categories, groups and SLOs as depicted in Figure 22*)

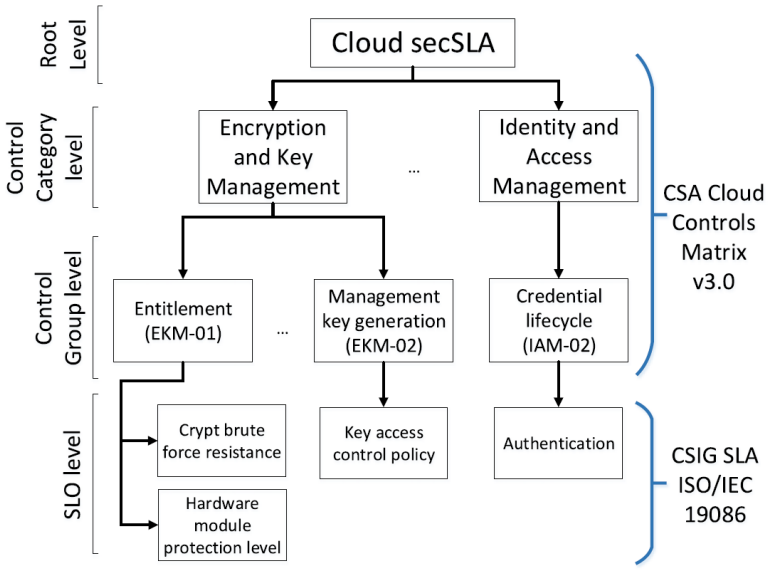

Figure 22. SLA hierarchy combining the CSA CCM and the ISO/IEC 19086

- **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 [22]. This methodology (called Quantitative Policy Trees (QPT)) evaluates and compares security SLAs based on the CAIQ [24] structure and taken from the STAR repository [25]. 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)[26]. 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 the SLAs of customers' requirements and CSPs.

The newest approach is the Quantitative Hierarchy Process (QHP) presented by Taha et al. in [21]. 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) [28] 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

7.3. Comparative assessment of representative CSPs

This section presents the calculation of the readiness index for several providers with respect to the CRM. The QHP approach was used as the assessment technique to compare CSPs. QHP has been developed in TUDA by the DEEDS group and allows to evaluate the level of security provided by CSPs. With QHP we can compare across the CSPs and also compare against a set of security requirements specified by, for example, a customer. QHP takes as input the security SLA of CSPs, which is then organized in a hierarchical structure. QHP has also been chosen as it allows to evaluate the CSPs at different levels of granularity: partial scores can be obtained at different levels of the CRM hierarchy. We have adapted QHP to use the CRM as input. Figure 23 depicts the levels used for the analysis when using the CRM.

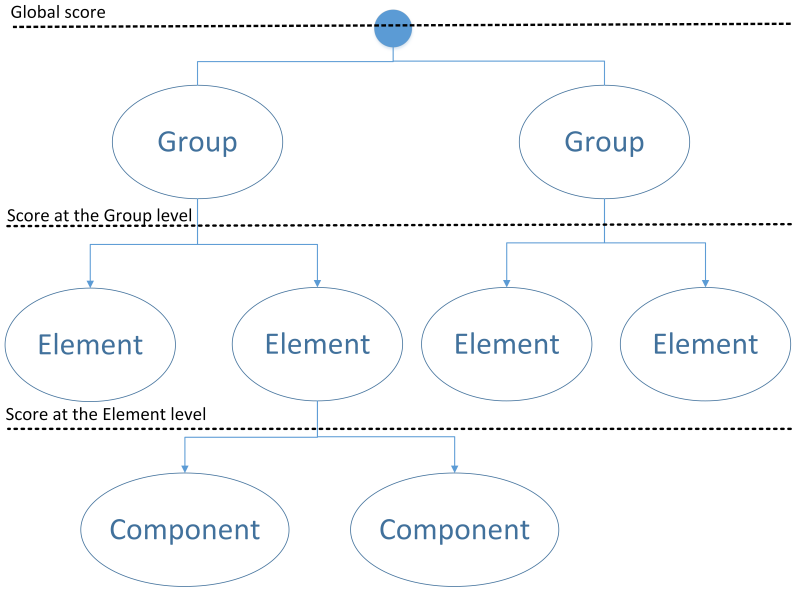

Figure 23. Evaluation done to get the readiness index at different levels in the CRM hierarchy

We have performed two evaluations. Each evaluation uses different information to calculate the readiness index:

- **Evaluation of surveyed CSPs**. In this case, the input has been taken from the answers given by several CSPs to the survey included in Annex B. This survey allows to know the compliance of every CSP with respect to every element of the CRM. We have used a simplified version of the CRM where the element level is the lowest layer of the CRM hierarchy. We have done it to make CSPs' life easier when answering to the survey, answering to 30 questions (30 elements of the CRM as

listed in Table 2) instead of answering to 70 questions (elements and technical components).

- **Evaluation of self-assessed CSPs**. We have compared the CRM with respect to the information from CSPs that is publicly available (for example published in their respective web sites) and information taken from SLA repositories (such as the CSA STAR repository [25]). In this case, we have used the complete hierarchy, considering also the components that are under the SLO & Metric element.

7.3.1. Evaluation of surveyed CSPs based on the CRM

Table 34 shows the answers of five CSPs for the survey shown in Annex B. The values of the answers are taken from the column "CSP self-assessment" of the survey. For example, a number "2" in the CRM element "Findable" means that the SLA is findable using an internal search engine while a "0" means that the SLA is not available in the website of the CSP. We have used that information to apply the QHP methodology to compare them.

Table 34. Answers of the surveyed CSPs

Group	Name of CRM element	*CSP1*	*CSP2*	*CSP3*	*CSP4*	*CSP5*
General (GR)	SLA URL	0	0	0	1	0
	Findable	2	0	0	0	1
	Choice of law	1	0	1	1	0
	Roles and responsibilities	1	1	1	0	1
	Cloud SLA definitions	1	1	1	1	1
Freshness (FR)	Revision date	1	1	0	1	1
	Update Frequency	1	1	0	1	0
	Previous versions and revisions	0	0	0	1	0
	SLA duration	1	0	1	0	1
Readability (RE)	SLA language	1	0	0	0	0
	Machine-readable format	1	0	0	0	0
	Nr. of pages	0	>1	>1	>1	1
Support (SU)	Contact details	1	1	1	0	1
	Contact availability	1	1	1	0	1
Credits (CR)	Service Credit	1	1	1	0	1
	Service credits assignment	1	1	0	0	1
	Maximum service credits (Euro amount) provided by the CSP	1	1	0	0	1
Changes (CH)	SLA change notifications	1	1	0	0	0
	Unilateral change	1	0	1	0	0
Reporting (REP)	Service Levels reporting	0	1	1	1	1
	Service Levels continuous reporting	0	1	0	0	0
	Feasibility of specials & customisations	1	1	0	0	1

	General Carveouts	1	1	0	1	1
SLOs & Metrics (SL)	Specified SLO metrics	0	1	1	1	1
	General SLOs	1	1	1	1	1
	Cloud Service Performance SLOs	1	1	1	1	1
	Service Reliability SLOs	1	1	1	0	0
	Data Management SLOs	0	0	0	0	0
	Security SLOs	0	1	0	0	0
	Personal Data Protection SLOs	1	0	0	0	0

The results are shown in Figure 24 and Figure 25. Figure 24 represents the comparison of the five surveyed CSPs at the higher level of the CRM hierarchy. This is the global score of every CSP with respect to the complete CRM. We can see that, compared with the rest of the evaluated CSPs, *CSP1* is the best one, followed by *CSP2* and *CSP5*. Of course, this is an aggregated evaluation and does not mean that CSP1 is better than the rest of the providers with regard to every element of the CRM. To be able to get a detailed analysis we have to go lower in the CRM hierarchy and evaluate the CSPs at the group level. QHP allows us to do such deeper analysis.

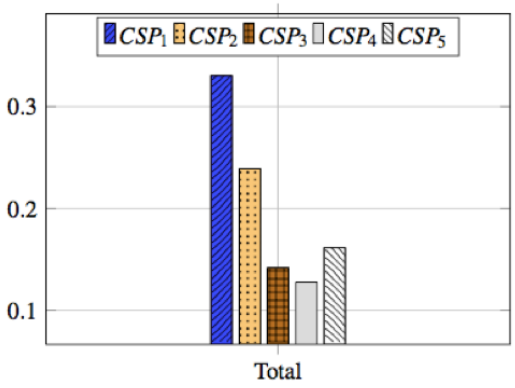

Figure 24. Comparison of surveyed CSPs: readiness index global score

Figure 25 represents the comparison of the surveyed CSPs at the group level of the CRM. As we can see *CSP1* is especially good in the "Readability" (RE) and in the "Changes" (CH) groups. *CSP4* provides detailed information about general aspects of the SLA and especially in what regards to the "Freshness" (FR) group (which is the specification of changes and updates of the SLA). Finally, it is worth mentioning how *CSP2* stands out in "Reporting" (REP) features.

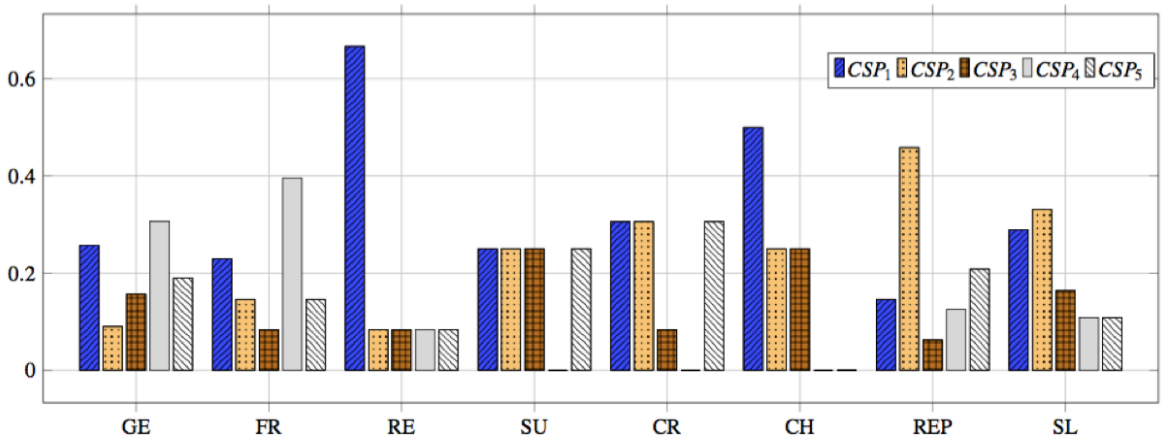

Figure 25. Comparison of surveyed CSPs at group level

As it has been already pointed out, these results are comparisons between the providers used in the evaluation. The results obtained are not absolute but relative with respect to the rest of the providers evaluated.

7.3.2. Evaluation of self-assessed CSPs based on the CRM

Table 35 shows the information for the CRM extracted for four self-assessed CSPs (as based on the information taken from the STAR repository and their respective websites). Additionally, this evaluation includes values for the components that are part of the SLO & Metrics group, being "1" when the component appears in the SLA of the CSP and "0" when it does not.

Table 35. Answers of the self-assessed CSPs

Group	Item	Name of CRM element/components	*CSP6*	*CSP7*	*CSP8*	*CSP9*
General (GE)	1	SLA URL	2	1	2	0
	2	Findable	1	1	1	0
	3	Choice of law	0	0	0	0
	4	Roles and responsibilities	0	0	0	0
	5	Cloud SLA definitions	1	1	1	0
Freshness (FE)	6	Revision date	1	1	1	1
	7	Update Frequency	2	1	2	2
	8	Previous versions and revisions	0	0	0	0
	9	SLA duration	1	0	0	1
Readability (RE)	10	SLA language	1	1	1	0
	11	Machine-readable format	0	0	0	0
	12	Nr. of pages	1	1	1	0
Support (SU)	13	Contact details	1	1	1	1
	14	Contact availability	0	0	0	0
Credits (CR)	15	Service Credit	0	0	0	0
	16	Service credits assignment	0	0	0	0
	17	Maximum service credits (Euro amount) provided by the CSP	0	0	0	0

Changes (CH)	18	SLA change notifications		0	0	0	0
	19	Unilateral change		0	0	0	0
Reporting (REP)	20	Service Levels reporting		0	0	0	0
	21	Service Levels continuous reporting		0	0	0	0
	22	Feasibility of specials & customisations		0	0	0	0
	23	General Carveouts		1	1	1	1
SLOs & Metrics (SL)	24	Specified SLO metrics (SM)		0	0	0	0
	25	General SLOs (GR)	Service monitoring	0	0	0	0
	26		Accessibility	0	1	0	1
	27		Availability	0	1	0	1
	28		Termination of service	0	1	0	1
	29		Cloud Service Support	0	1	0	0
	30		Governance	0	1	0	0
	31		Attestations, certifications and audits	0	1	0	0
	32	Cloud Service Performance SLOs (CP)	Response time	0	0	0	0
	33		Capacity	0	0	0	0
	34		Elasticity	0	0	0	0
	35	Service Reliability SLOs (SR)	Service Resilience	0	0	0	0
	36		Customer data backup/restore	0	1	0	0
	37		Disaster Recovery	0	0	0	0
	38	Data Management SLOs (DM)	IPR	0	1	0	0
	39		Cloud Service Customer Data	0	0	0	0
	40		Cloud Service Provider Data	0	0	0	0
	41		Account Data	0	0	0	0
	42		Derived Data	0	0	0	0
	43		Data portability	0	0	0	0
	44		Data deletion	0	1	0	0
	45		Data location	0	0	0	0
	46		Data examination	0	0	0	0
	47		Law Enforcement Access	0	0	0	1
	48	Security SLOs (Sec)	Organization of Information Security	0	0	0	0
	49		Human Resources Security	0	0	0	0
	50		Asset Management	0	1	0	0
	51		Access Control	0	1	1	1
	52		Cryptography	0	1	1	0
	53		Physical and Environmental Security	0	1	0	0
	54		Operations Security	0	1	0	0
	55		Communications Security	0	1	1	0

	56		Systems Acquisition, Development and Maintenance	0	1	0	0
	57		Supplier Relationships	0	0	0	0
	58		Information Security Incident Management	0	1	1	0
	59		Business Continuity Management	0	1	0	0
	60		Compliance	0	1	0	0
	61	Personal Data Protection SLOs (PDP)	Consent and choice	0	0	0	0
	62		Purpose legitimacy and specification	0	0	0	0
	63		Collection limitation	0	0	0	0
	64		Data minimization	0	0	0	0
	65		Use, retention and disclosure limitation	0	0	0	0
	66		Accuracy and quality	0	0	0	0
	67		Openness, transparency and notice	0	0	0	0
	68		Individual participation and access	0	1	0	0
	69		Accountability	0	0	0	0
	70		Privacy compliance	0	1	0	0

Figure 26 represents the readiness index of the SLAs for the four self-assessed CSPs given the global score at the highest level of the CRM. As we can see, this time it is *CSP7* that stands out over *CSP8* and *CSP6* in this order. Far behind them it is *CSP9*. Again, this provides just a global score and does not allow us to know how well or bad these providers behave for every group of the CRM.

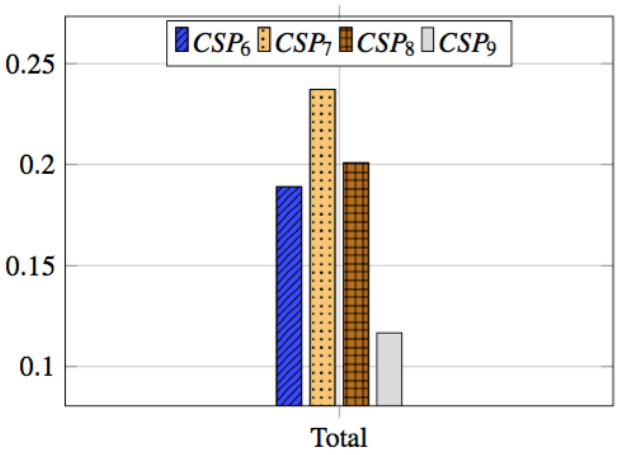

Figure 26. Comparison of self-assessed CSPs: readiness index given the global score

To obtain a more detailed comparison we have carried out a comparison of these four providers at the group level. The results are depicted in Figure 27. In general, the four

CSPs behave quite similar in most of the groups. Just *CSP7* stands out in the specification of SLOs and Metrics (SL). We can also see in Figure 27 the reason for the low global score of *CSP9* as it does not provide information about 4 out of the 8 groups evaluated. Furthermore, it is worth noticing that the groups "Credits" (CR) and "Changes" (CH) are giving a score of 0 for all the CSPs. The reason is that they are not detailing such information in the self-assessment report stored in the STAR repository and no further details are given in the public information that can be extracted from their web sites (or at least we have not been able to find it).

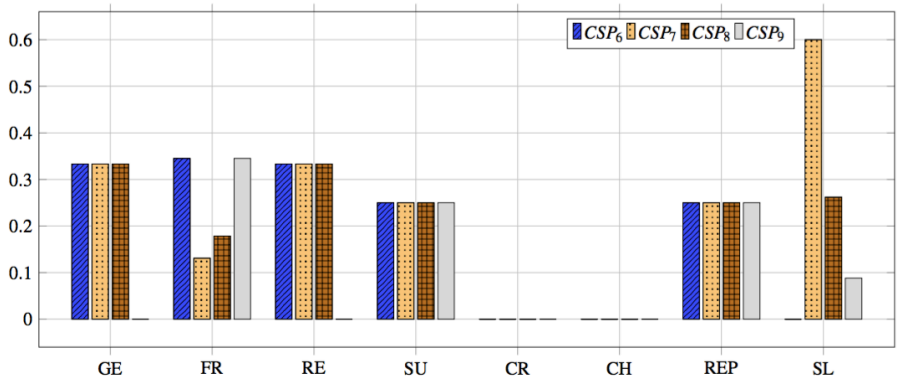

Figure 27. Comparison of self-assessed CSPs at the group level

A deeper analysis of the SLA & Metric group explains the high score of *CSP7* and the low score of *CSP6* for that group. Figure 28 represents the scores of the four providers in the SLO & Metric group. This analysis takes into consideration the values of every component at the lowest level of the hierarchy. We can see that, only *CSP7* details information about 5 out of the 7 elements of the SLO & Metrics group. This explains the high score that *CSP7* has for this group in Figure 27. We can also see that *CSP8* is only providing values for Security SLOs (as it can be seen in Table 35).

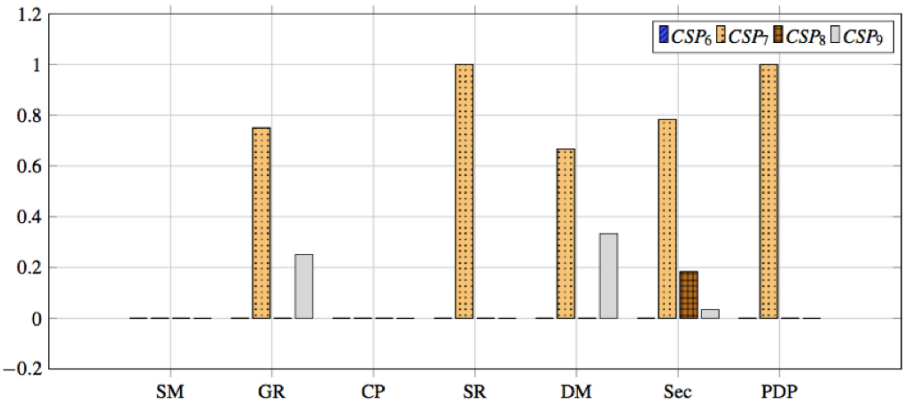

Figure 28. Comparison of self-assessed CSPs at the "SLO & Metrics" group level

As a result, the evaluation methodologies, such as QHP, combined with the SLA-Ready CRM provides with a powerful tool not only to evaluate and compare CSPs, but also to discover the aspects in which the respective CSPs are stronger or weaker than others. For example, this offers an opportunity for CSPs to know in what aspects to improve.

7.4. Summary takeaways

Summary takeaways

- The CRM, as added value, can additionally be used to compare across the CSPs or comparing the CSPs against customers' requirements. This can be done by calculating the SLA-Readiness index.
- The SLA-Readiness index can be obtained by using different types of input. In SLA-Ready we have used: (i) information taken from CSPs that answered to a survey based on the CRM (see Annex B) or (ii) public information (available in Web sites or SLA repositories) that has been mapped to the CRM.
- The SLA-Readiness index is obtained by applying an assessment methodology developed by TUDA: The Quantitative Hierarchy Process (QHP).
- QHP allows to perform comparisons at any level of the CRM hierarchy, depending on the level of granularity requested.

8. Conclusions

This report describes and validates the SLA-Ready's Common Reference Model based on the analysis of the requirements elicited in D2.1 and D2.2 and on the initial analysis done in D2.3. D2.4 reports a comprehensive analysis of different domains (standards, industry) with respect to the CRM.

From the analysis of the standardization domain we have updated the evaluation of the standards and best practices analysed in D2.3. Furthermore, we have extended the evaluation by adding to additional best practices taken from the SLALOM project. The outcome of this 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. Only the ETSI Cloud SLA template has a better coverage of non-technical aspects. The SLALOM specification for SLAs is also mainly focused on technical aspects. On the contrary, the SLALOM specification for contracts is mainly focused on legal and administrative aspects, while technical aspects are avoided.

For the analysis of the industrial domain, we have extended the evaluation of the CRM with additional 19 use cases from different domains and extended the 4 use cases studied in D2.3. We have also extended the template to evaluate use cases with information about the level of expertise required by the CSPs to implement such use case and the stage of the life cycle where the use cases are applied.

We have used this additional information to propose a recommendation methodology based on the CRM that uses machine learning techniques. The recommendation methodology receives as input a high-level description of a business case (such as the type of cloud service provided and the stage of the life cycle) and returns information about the level of importance of every CRM element, which will be the most suitable one for the characteristics of the business case.

Finally, we have also proposed a technique to obtain the readiness index of SLAs by evaluating the SLAs of several CSPs with respect to the CRM. On the one side, we have analysed more than 100 CSPs with the information that is publicity available. On the other side, we have received surveys from several CSPs which have self-assessed their SLAs with respect to the CRM. We have used that information to compare (by using cloud assessment methodologies) several CSPs in terms of the CRM.

The outcomes of the validation of the CRM carried out in D2.4 can be used to leverage the creation of tools that integrate the calculation of the readiness index and the recommendation methodology.

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] Ester, Martin, Hans-Peter Kriegel, Jörg Sander, and Xiaowei Xu. "A density-based algorithm for discovering clusters in large spatial databases with noise." In Kdd, vol. 96, no. 34, pp. 226-231. 1996.

[11] MacQueen, James. "Some methods for classification and analysis of multivariate observations." In Proceedings of the fifth Berkeley symposium on mathematical statistics and probability, vol. 1, no. 14, pp. 281-297. 1967.

[12] Johnson, Stephen C. "Hierarchical clustering schemes." Psychometrika 32, no. 3, 241-254. 1967

[13] Wang, Wei, Jiong Yang, and Richard Muntz. "STING: A statistical information grid approach to spatial data mining." In VLDB, vol. 97, pp. 186-195. 1997.

[14] Fraley, Chris, and Adrian E. Raftery. "MCLUST: Software for model-based cluster analysis. "Journal of Classification 16, no. 2: 297-306. 1999

[15] Tung, Anthony KH, Jiawei Han, Laks VS Lakshmanan, and Raymond T. Ng. "Constraint-based clustering in large databases." In International Conference on Database Theory, pp. 405-419. Springer Berlin Heidelberg, 2001.

[16] Saul, Lawrence K., Kilian Q. Weinberger, Jihun H. Ham, Fei Sha, and Daniel D. Lee. "Spectral methods for dimensionality reduction," Semisupervised learning: 293-308. 2006

[17] Jolliffe, Ian. Principal component analysis. John Wiley & Sons, Ltd, 2002.

[18] 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.

[19] 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.

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

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

[22] 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.

[23] 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.

[24] Cloud Security Alliance, "Consensus Assessments Initiative (CAI) Questionnaire," 2012. [Online]. Available: https://cloudsecurityalliance.org/research/initiatives/ consensus- assessments- initiative/, 2011.

[25] Cloud Security Alliance, "The security, trust & Assurance registry (STAR)". [Online]. Available: https://cloudsecurityal- liance.org/star/, 2012.

[26] 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.

[27] T. Saaty, "How to make a decision: The analytic hierarchy process," Eur. J. Operational Res., vol. 48, pp. 9–26, 1990.

[28] M. Zeleny, Multiple Criteria Decision Making. New York, NY, USA: McGraw Hill, 1982.

[29] C. S. M. I. C. (CSMIC), "SMI Framework," [Online]. Available: http://betawww.cloudcommons.com/servicemeasurementindex.

[30] EU H2020 SLALOM, "SLA Specification and Reference Model". Online: http://www.slalom-project.eu 2016

[31] EU H2020 SLALOM, "Model contract for Cloud Computing". Online: http://www.slalom-project.eu 2016

[32] Cloud Computing Use Case Discussion Group. “Cloud Computing Use Cases White Paper”. [Online]. Available: http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf

Annex A. Use Cases list (ETSI CSC)

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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

[13] 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[13]
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[13]
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 documented 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-centric 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[13]
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 exchange 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[13]
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[13]
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 analyse 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[13]
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[13]
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 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.	CSC
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-premises 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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 boundaries as constraints 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 services implemented as a support for the service includes, VPN overlay, Intelligent Protection system and Secure data storage. F) The cloud broker allows deployment of service in the non-optimis IP, providing interoperability support.	CSC, CSP, Cloud Service Partner
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 scenario 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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 concepts and ecosystem-empowered capabilities.	CSC, CSP, Cloud Service Partner
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 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.	CSP Cloud Service Partner

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 on-premises 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 procedure. The use case describes how a public administration requests a document from a citizen in the course of an administrative process.	CSC
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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-premises, with the need to link the on-premises 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 centre 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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 customer's applications to IaaS service	CSC
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 centre 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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 artefacts 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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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
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

Cloud Service life-cycle phase (D2.2)	High-level Use Cases	UC Title	UC Short Description	Actors[13]
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 services to another cloud	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[13]
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 procedure. 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 procedure. 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[13]
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 proactive 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: CRM assessment

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 revisions	Are the public available the previous versions of the SLA?	0 = n/a or No, 1 = Yes	
	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 the CSP	Does your SLA describe how much does the can CSP credit (Euros) to the customer?	0 = n/a or No, 1 = Yes	
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 of service, applicable certifications, and governance?	0 = n/a or No, 1 = Yes	
	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. CRM questionnaire for CSPs: Consent and General Data

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[14] 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[15] 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

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

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

[15] 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.

[ ] Education

[ ] Financial Services

[ ] Government

[ ] Information Technology (IT) & Telecommunications

[ ] Other (please specify): _____

d) How well the following high-level use cases[16] 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., understanding data retention clauses)

2. Based on your offered Service Level Agreement, please perform its self-assessment

[16] 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

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: