www.sla-ready.eu

Title: Requirements emerging from the state-of-the-art analysis

Author(s): Neeraj Suri (TUD), Arthur van der Wees (Arthur)

Contributor(s): Jesus Luna (CSA), Silvana Muscella & Stephanie Parker (Trust-IT), Thierry Floriani (Numergy).

Reviewer(s): Daniele Catteddu (CSA), Nick Ferguson (Trust-IT)

Date: 29 June 2015

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

Executive Overview

SLA-Ready aims to provide common understanding of Service Level Agreements (SLAs) for Cloud services with greater standardisation and transparency so firms can make an informed decision on what services to use, what to expect and what to trust. SLA-Ready services will support SMEs[1] with practical guides, and a social marketplace, encouraging them to carefully plan their journey and make it strategic through an informed, stepping-stone approach, so the Cloud and applications grow with their business.

The SLA-Ready Common Reference Model (CRM) will benefit the industry by integrating a set of SLA components, e.g. common vocabularies, Service Level Objectives (SLO) service metrics and measurements, as well as best practices and relevant standards to fill identified gaps in the current SLA landscape.

In order to systematically develop the CRM, the deliverables in WP2 will take a two-fold approach with an initial data compilation and requirements elicitation phase (D2.1) to outline the SLA landscape followed by a fuller gap analysis on the requirements (D2.2) to guide the CRM development. Thus, the current deliverable presents the initial compilation and elicitation of SLA requirements developing the following components of:

- Requirements compiled from a state-of-the-art/practice analysis
- Initial gap analysis on missing requirements – D2.2 will specifically develop this.
- Preliminary design of the Cloud Service Provider (CSP) SLA repository

The terms used herein are consistent with those in Chapter 2 of the current EC Cloud SLA Standardisation Guidelines[2] ('EC Standardisation Guidelines'), the SLA Vocabulary, which for easy reference is part of this Deliverable and detailed within the requisite sections.

The next version of this deliverable (D2.2 at M12) will provide the refined version of the initial SLA state of the art/practice (SoA) reported in D2.1, in order to form the basis of composing the CRM.

[1] When 'SME' is referred to, the implication is of small and medium-sized enterprises having between 2-250 Full Time Employees. This terminology is consistent as used by the DG Connect and DG Justice, whereby the threshold is meant to make a split between consumers and enterprises.

[2] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Table of Contents

Table of Tables

Table of Figures

Document information

Deliverable number	D2.1
Deliverable title	Requirements emerging from the state-of-the-art analysis
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	June 2015 (M6)
Actual delivery date	29 June 2015
Author(s)	Neeraj Suri (TUD), Arthur van der Wees (Arthur)
Contributor(s)	Jesus Luna (CSA), Silvana Muscella & Stephanie Parker (Trust-IT), Thierry Floriani (Numergy)
Reviewer(s)	Daniele Catteddu (CSA), Nick Ferguson (Trust-IT)
Task(s) contributing to the deliverable	Task 2.1 – SLA challenges and requirements in the Cloud landscape and Task 2.2 – SLA-Ready Common Reference Model
Target audience(s)	Project partners, members of the SLA-Ready Advisory Board and other external experts, European Commission, project reviewers
Total number of pages	60

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.

1. Introduction

The goal of WP2 (Definition of a Common Reference Model) is to increase the uptake of Cloud services, especially in the private SME sector, through the definition of a SLA[3] Common Reference Model (CRM).

The CRM includes an integrated set of SLA components (e.g., common vocabularies, service level metrics, a Service Level Agreement (SLA) repository, quantitative and qualitative assessment techniques) and best practices. Moreover, the CRM defines the relationship with relevant standards with the objective of filling potential gaps in the current Cloud SLA landscape.

WP2 builds on top of relevant best-practice works (reports, projects, standards…) and recommendations (in particular the EC report on Cloud SLA and the Cloud Select Industry Group (CSIG) SLA "Cloud SLA Standardisation Guidelines"). This deliverable also utilizes SLAs gathered from a representative set of worldwide public Cloud Service Providers (CSPs).

This deliverable D2.1 spans the first-phase of requirements analysis and compiles the results of Tasks 2.1 (SLA challenges and requirements in cloud landscape) and 2.2 (Legal, privacy and data governance issues), to provide a comprehensive compilation of the requirements identified in the community, both from the technical perspective (both in the industrial and academic domains as part of the Task 2.1), and from the legal perspective (as part of the Task 2.2). This deliverable also reports the preliminary design of the repository of SLAs, to become part of the 'social marketplace for Cloud SLA' built on WP4.

D2.1 relates to Objective 1 and Objective 2 of SLA-Ready through the following process:

- Compiling a set of SLA-related information spanning the state-of-the-art/practice (SoA), to elicit the key SLA requirements: technical (performance, security, privacy), legal and socio-economic.
- Defining the foundations of the CRM based on the analysis of elicited requirements
- Initial design of a public repository of SLAs

3 An SLA (Service Level Agreement) is a contract that outlines (qualitatively, quantitatively etc) the various services that will be provided and the contractual conditions for their full or deficient provisioning.

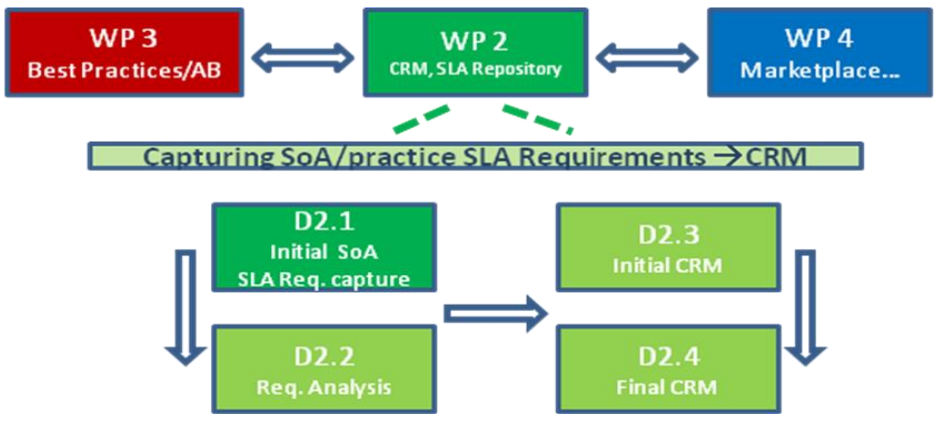
1.1. Positioning D2.1 within SLA-Ready

This deliverable (D2.1) is the first of two iterations of an analysis of requirements emerging from a state-of-the-art analysis. D2.1 is an initial compilation of the SoA of SLA attributes covering the areas of security, personal data protection, legal and socio-economic aspects with a particular focus on metrics. The second iteration (D2.2) will be published in December 2015 (M12 of the project) and will provide an analysis of the collected requirements. Relevant findings from both D2.1 and D2.2 will feed into D2.3 (a Common Reference Model (CRM)). Although a public deliverable, this document is primarily for internal project purposes, and as mentioned above, is part of a two stage analysis of requirements. Content from this deliverable will be used for awareness raising activities that are part of WP4 (Communications, impact and exploitation).

Figure 1 gives an overview of the role of D2.1 and, more in general of WP2 in the context of SLA-Ready. As is shown in Figure 1, the definition of the CRM also depends on WP3 (International cooperation, consensus and standardisation) in providing input on relevant standardization efforts and initiatives, and user and provider requirements through interaction with the SLA-Ready Advisory Board (AB). Furthermore, WP2 also inputs relevant CRM information to WP3, in particular we refer to the results of the gap analysis that will provide guidance to develop the best practices.

The SLA-Repository (preliminary described in this report) will be also used as an input to WP4's Social Marketplace. The Social Marketplace (T4.1 SLA-Ready digital hub and social marketplace) will provide a set of tools and practical guides to help the European private sector navigate its way through the Cloud SLA lifecycle. A core activity thus is making the CRM more useful and practical. Moreover, WP4 will engage with key stakeholders, collecting and analyzing feedback on specific information needs including from a socio-economic perspective.

Figure 1 D3.1 within SLA-Ready



1.2. Scope and Methodology

The following three disclaimers will help put the report in context.

Firstly, there is a very wide variety of CSPs, business models and Cloud customers' needs. Hence a one-size-fits-all SLA CRM is not feasible to develop. SLA-READY develops a pragmatic approach of formulating a 'generic' Common Reference Model where the distinctive aspects of SLA attributes across varied requirements (security, personal data protection, legal, and socio-economic) and life cycles can be presented and assessed in a conformal manner.

Secondly, the intent is not to project a "golden" SLA but rather to provide "information and guidelines" to support the customer to assess and implement their Cloud strategy. The intent is to help the customer in obtaining and managing good enough" SLA. The "information and guidelines" shall help customers to understand the elements of performance, security, personal data protection, liability or socio-economic factors that may be important to them.

Thirdly, this report is developed from the viewpoint of SME's. It is important to note that CSPs and SME's have differing degrees of technical awareness. The SME may or may not be fully technology savvy nor may have the inclination to interpret the fine nuances of terminology and concepts. Consequently, a "useful" CRM is designed to facilitate bridging this gap across the CSP and the customer. Hence this report documents the State of the Art/Practice (SoA) aspects of SLAs, in order to develop a common reference model for Cloud SLAs.

1.3. The Importance of Stakeholders

The internet is a global communications channel and it is built on standards that are respected worldwide. Likewise, cloud services have a global audience of governments, small and midsized businesses, enterprises, non-government organisations (NGO) and individuals. Agreements that govern Cloud services must account for regional, national and local laws, regulations and policies but everyone benefits from globally common concepts, vocabulary and globally accessible technology.

As per the characteristics of Cloud computing, Cloud services can be obtained and utilized by one Cloud customer but also by many at the same time, either through the Cloud customer or through platforms or other user ecosystems. So, a multi Cloud customer environment is to be taken into account, both by Cloud service providers as well as other stakeholders. These ecosystem or platform environments trigger several challenges, technical, legal and otherwise.

This not only applies for the Cloud customer and user side, but also from the Cloud service provider side. As per the characteristics set forth above, most Cloud service providers have, use and contract with many Cloud and other vendors, suppliers and licensees, in order to be able to provide its Cloud services to its Cloud customers. These multi-vendor environments trigger several challenges, technical, legal and otherwise.

Therefore, a number of stakeholders can and need to be identified, in order to understand SLOs/Attributes, and to be able to understand Cloud SLAs.

1.4. SLA Value Chain

When identifying the supply chain and value chain of Cloud services, as set forth in the previous paragraph, there are many stakeholders involved, each with one or more SLA relationships both on the vendor side as well as the Cloud customer side.

1.5. Structure of this report

On this background of the proposed scope and methodology, this report is organized as follows.

- Section 2 outlines the SLA-READY advocated use of the SLA lifecycle to capture the SLA requirements. Section 2 also defines the template SLA-READY proposes for the capture of SLA requirements, in particular the associated metrics.
- Using the proposed template Section 3 systematically details the SLA requirements of security, personal data protection, legal and socio-economic aspects.
- Section 4 performs an initial review of the requirements that will lead to a metrics-based analysis approach in subsequent deliverables.
- Section 5 outlines the initial steps towards developing the repository of SLA, to become part of SLA-Ready's Social Marketplace.

2. The Cloud SLA management life cycle

There are multiple ways to capture and analyze the requirements that will drive the development of the CRM. An SLA is not a static entity; rather it evolves through a set of phases that consequently have to be managed on a dynamic manner. Based on the latest ISO/IEC CD 19086-1 draft, the Cloud SLA management life cycle covers the stages of design, evaluation and acceptance, implementation and execution, changes and termination. In order to elicit the CRM requirements (cf., Section 3), SLA-Ready advocates the stages associated to the Cloud SLA management life cycle by mapping them to the Cloud Service management life cycle as follows:

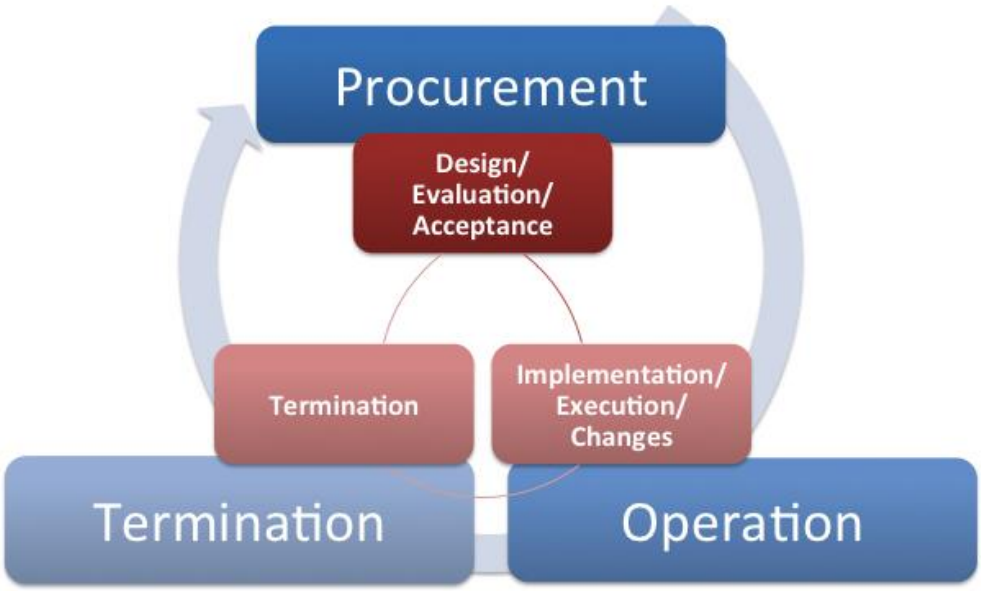
Phase 1 – Procurement (comprehending SLA design, and evaluation and acceptance): A prospective Cloud Customer can use service offerings published by the CSP to check whether it meets its requirements (security, personal data protection, performance, economic, etc.) and how one CSP's service offering compares with another in the market. This phase of the Cloud service life cycle is crucial for establishing a SLA between the Cloud Customer and the CSP.

Phase 2 – Operational (comprehending SLA implementation, execution and changes): This determines whether Cloud services meet the committed SLOs during the provisioning of the Cloud service, and might imply CSPs taking corrective actions to avoid SLA violations. This phase is important as SLAs can be used to monitor the CSP in order to assess the correct fulfilment of the negotiated Cloud service (or detect potential violations in which case remediation action may take place).

Phase 3 – Termination (comprehending SLA termination): This last phase, SLA termination and consequences of termination, should preferably already be thought about and addressed in phase 1, as a SLA can be used to arrange the conditions under which the Cloud customer's data (including but not limited to for instance Personal Identifiable Information or PII) will be exported and returned to the Cloud customer, and not retained by the CSP (to the extent mandatorily possible).

A graphical presentation of the intersection between the SLA life cycle and the Cloud Service management life cycle can be seen in Figure 2.

Figure 2 The SLA Management and the Cloud Service Management life cycles.



2.1. Capturing the CRM requirements

In order to build the foreseen CRM, it is essential to capture the basic measurable attributes of the surveyed SLA elements based on the life cycles depicted in Figure 2. A template comprehending the following elements is proposed and used throughout this document:

1. Name of SLO/attribute requirement (Type: Academic, Industry-use, Standards recommendation)
2. Summary description of key SLO/Attribute/SLA requirements
3. Name the phase of the Cloud Service life-cycle where this is typically used (cf., Figure 2)
4. Name of source supporting the SLO/attribute: e.g. CSIG-WG, EC Cloud Study, Web pointers.
5. Description of the SLO's/Attribute purpose and value advocacy in the SLA
6. Is this SLO actually used as a practice? For example, is this SLO/Attribute used because one is required to use it or because it is a useful SLO/Attribute?
7. Is this a recommended best-practice SLA?
8. Prominent use-case(s) that apply for this SLO/Attribute.

These eight elements will provide the basis for the analysis in D2.2. Furthermore, the proposed elements can be represented as in Table 1 to facilitate their gathering and usage in other WPs (in particular WP3 for standardization purposes).

Table 1 Template for reporting Cloud SLA elements

Name:	Unique name of the Cloud SLA element
Type:	Academic/Industry/Standards or recommendation
Cloud Service life-cycle phase:	Procurement, Operation, Termination
Source:	EU FP7/H2020, standardisation body, other.
Description:	Brief information related to the element (e.g., objective).
State of practice:	Yes/No
Recommended best-practice:	Yes/No
Use case:	Reference Use Cases as taken from the ETSI CSC report: **AP**: App on a Cloud **CB**: Cloud Bursting **SD**: Processing Sensitive Data **DI**: Data Integrity **HA**: High Availability

The designed template contains information that is useful to SLA-Ready, in particular the relationship of the reported Cloud SLA element (i.e., attributes/SLOs and metrics) to the life-cycle and the actual use case where the reported element could be applied. On one hand, the life-cycle perspective allows WP2 to classify these elements according to the Cloud service management stage(s) where customers should identify them in their CSP's SLAs. This is useful for the SLA-Ready CRM in order to provide further customer guidance and focus (e.g., to better understand how to elicit customer's requirements).

On the other hand, the use case perspective is useful to provide a general idea with respect to the actual SLOs/attributes and metrics that are typically considered in real world application scenarios. The foreseen SLA-Ready framework will allow customers to select the SLA elements that are adequate or "good enough" for his/her own organizational context, by further analyzing or composing the initial set of ETSI CSC-based use cases.

The information provided by the template will be further analyzed in WP2 to develop the basis of the planned CRM.

2.2. Legal and sociological analysis

From a legal and sociological point of view, the SLA mainly covers non-technical requirements and business customer perspectives. An analysis of the situation today, especially from a demand perspective, calls for an approach aligned with the following point from the C-SIG SLA included in its *Cloud Service Level Standardisation Guidelines*:

"From case to case reviewing less quantitative or qualitative SLOs and comparing different services may provide extra insights for making an informed decision".

Using the framework below, the analysis will cover supply side behaviour (CSPs), demand side behaviour (Cloud customers) and varying levels of comprehension across both (e.g. consistency of terminology, comprehension of terminology and vocabulary). Legal and sociological analysis will use data from CSPs and on the business community and may also consider partners in the Numergy value chain.

2.2.1. Elements specific to SMEs

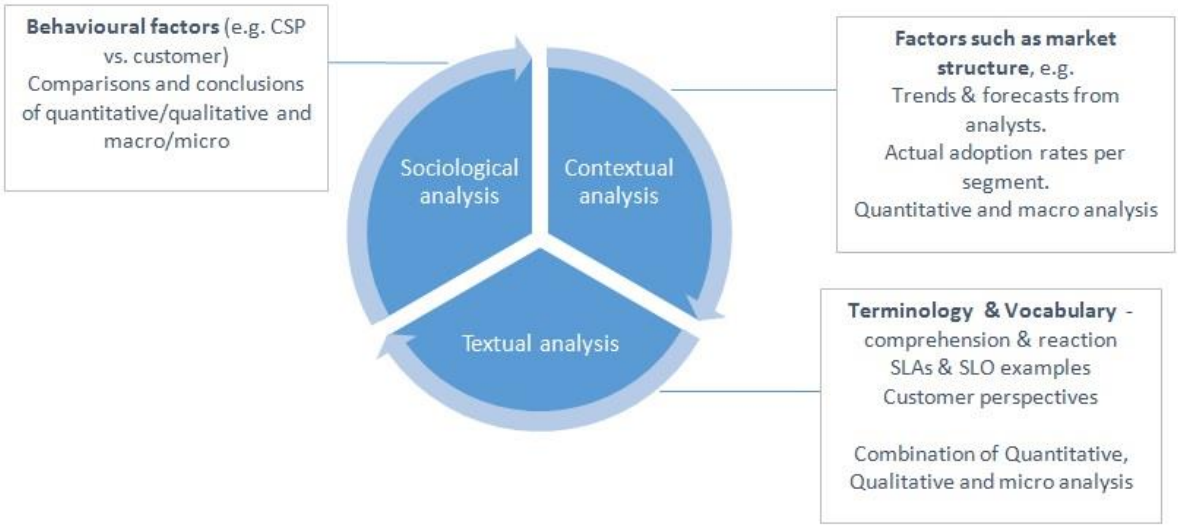
From an SME perspective, it analyses understanding and perceptions in relation to actual behaviour. It looks at actual terminology of the Cloud service contract, the SLA and SLO compared with the information required, adoption trends (current and forecast) and non-technical barriers to uptake. It compares requirements with those of other market segments, e.g. big corporations and public sector organisations.

2.2.2. Approach

Using real-world examples, it also asks how strategic planning is for the use of Cloud services and provides a comparison in relation to different requirements. It assesses how behavioural patterns by SMEs compare with those of other market segments, e.g. big corporations and public sector organisations. For example, we will analyze concerns around security, privacy and trust in order to understand whether they are real concerns or misconceptions due to a lack of expertise. We will also analyze examples of mismatches between corporate concerns and actual behaviour, e.g. Siemens adoption of Amazon Web Services despite months of negotiation with a European Cloud service provider.

From a CSP perspective, it assesses non-technical aspects of the service contract, SLA and SLO, with a focus on codes of conduct, standards and certification mechanisms, as well as openness, transparency and notice.

Figure 3 Analytical Framework



The analytical framework is therefore a combination of the following approaches:

Quantitative analysis: SMEs in numbers, including organizational structures. Current levels of adoption, adoption forecasts in per market segments.

Qualitative analysis: given that SMEs typically lack CIO/CTO/CISO leadership, security/legal expertise and financial resources, the analysis of qualitative data will consider sources that cover Cloud service adoption experiences, behavioural patterns, as well as behavioural choices such as interest in Cloud service usage prevented by customer concerns. Analysis of typical levels of expertise being as e.g. information security at C-level and overall awareness, also considering that SMEs do not typically have a CIO. Comparative aspects of less quantitative and qualitative SLOs - Perceptions versus real issues: shortcomings that is not totally technological but also due to human error or simply lack of clarity or understanding. How can we best assess inconsistency or lack of clarity about the type of security/privacy a customer wants and in relation to the lack of transparency about security/privacy Cloud service providers offer? What exactly is on offer? Where do I find this information? Is the SLO or SLA sufficient as a source of information? Should we expect them to solve a problem that is so complex and elusive?

3. Preliminary SLA Requirements

This section systematically captures the community best-practices of SLA requirements based on the template proposed by Section 2. The subsequent subsections individually detail the SLA requirements as follows. Section 3.1 addresses the technical dimensions of Security/Personal data protection and Performance. Section 3.2 addresses Data Protection and Legal considerations in SLA's. Section 3.3 highlights the economic aspects of SLA followed by Section 3.4 covering sociological dimensions. Naturally, the economic requirements are a horizontal attribute that covers all technical, personal data protection, legal and sociological elements of SLA's. We highlight two aspects that are helpful to parse the upcoming subsections 3.1 through 3.4.

Firstly, it is important to note that each SLA requirement entails a distinctive perspective. This is reality, and artificially trying to project identical considerations on them is not productive. However, SLA-READY has developed a template (cf., Section 2) that applies across the multiple SLA requirements using a common SLA life-cycle approach. While retaining the basic Life cycle of Section 2, each section is presented by highlighting its applicability from a lifecycle perspective. Specifically, the security, personal data protection and the legal SLA requirements will outline how the same base lifecycle gets detailed according to the needs of the chosen dimension.

Secondly, the template proposed by SLA-READY to capture the SLA requirements is a contribution that we believe is very helpful in systematically compiling and analysing SLA requirements, in particular from a metrics perspective. To put this template in context, we refer to some existing real-world SLA's below that highlight the predominantly textual and hard-to-understand (for the average user) legalese description of SLAs that SMEs typically have to understand before using them in any meaningful manner. Also, the associated SLA and SLOs can be significantly different depending on the use case of each SME (i.e. type and criticality of the application that will run in the Cloud). In this respect, some CSPs started offering SLAs that can be tuned or customized according to the use case/customer needs, for instance:

- **Customer Relationship Management' SLA (Salesforce)**: http://www.salesforce.com/company/legal/agreements.jsp.
- **Microsoft Dynamics**: https://port.crm.dynamics.com/portal/static/1033/sla.htm
- http://blogs.msdn.com/b/mvpawardprogram/archive/2015/01/19/insider-s-guide-to-managing-services-level-agreements-with-dynamics-crm-2015.aspx
- https://pinpoint.microsoft.com/en-eg/Applications/12884960727)
- **SLA for Mailing Systems (NIH)**: http://cit.nih.gov/NR/exeres/51E35023-3581-43CC-9F84-3D083652D3ED,frameless.htm

- **Amazon Web Services**: http://aws.amazon.com/agreement/
- **Gmail cover by the Google Apps SLA**: http://www.google.com/appsstatus#hl=en&v=status)

There are many hundreds of potential (and also use-case based) customizable SLO/attributes that can be defined in each SLA, which is naturally beyond the scope of any report. Hence, the intent in each subsection is to project the key requirements that are commonplace as state of the art/practice (SoA) based also on the feedback received from current standardization initiatives and recommendations (e.g., the "EC Standardisation Guidelines") through WP3.

These aspects form the basis of the SLA requirements capture in the following sections.

3.1. SLA requirements Security/Personal Data Protection/Performance

The SLA requirements from the security, personal data protection and performance point of view covers the technical elements of SLA's typically encountered by SME's at state of the art reports and contracts. It is worth mentioning that there is a considerable paucity of structure and formality for either CSP or customer level SLAs. At this stage, the material presented below structures SLA elements (in particular measurable SLO/attributes) using a SLA-READY proposed template (cf., Section 2) that is amenable to projecting these key elements and also for the subsequent gap analysis.

This section reports a set of security and personal data protection-related elements found both at the Cloud SLA's state of art/practice (SoA). The main focus of the presented elements is showing an initial set of SLO/Attributes based on the following community advocated definitions as taken from the NIST RATAX[4] report:

- **Measurement**: Set of operations having the object of determining a Measurement Result.
- **Measurement Result**: Value(s) that expresses a qualitative or quantitative assessment of a property of an entity.
- **Metric**: A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement.

[4] http://www.nist.gov/itl/cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf

- **Service Level**: A measurement result for specific attributes of the Cloud service. Based on a CSA proposed to redefine the term SLO from ISO/IEC 19086 Part 1[5]
- **Service Level Objective (SLO)**[6]: The contractual target for a service level that the Cloud Service Provider agrees to meet. This is based on a CSA proposal to redefine the term SLO from ISO/IEC 19086 Part 1.

As described in our strategy document (D3.1, Engagement plan for standardisation and international cooperation), where available the reported SLO/Attributes have been derived from the latest version of the draft standard ISO/IEC 19086 Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 1: Overview and concepts". The associated metrics were extracted from an analysis to the relevant SoA including EU projects (FP7 and H2020) and international initiatives (e.g., industrial working groups). However, it is important to highlight that this report does not attempt to fully document the reported metrics (in accordance to ISO/IEC 19086 Par 2), rather to describe them from the SLA-Ready's perspective through the template introduced in Section 2.

The following tables report SoA Cloud SLA security and personal data protection metrics, most of which were contributed by existing and/or ongoing EU research initiatives[7] (FP7 and H2020), and other state of the art reports from NIST and the Consensus Information Security metrics organization. There are two ways to classify the SLA requirements either by the functionality of the SLO/Attribute or by the lifecycle phase. As advocated in Section 2, the latter represents the logical progression of developing a SLA and thus our choice. It is worth pointing out that many SLO/Attributes are valid over more than one phase of the SLA lifecycle and this is clearly indicated in the template.

5 At the time of writing D2.1, ISO/IEC 19086 Part 1 was still under discussion by the work group (SC38).

6 The community now uses the term "attributes" instead of 'SLO's. However, as we used the term SLO in the proposal and as "attribute" is not yet formally approved in the standards community, the document currently mentions these term interchangeably.

7 While multiple projects address SLAs, FP7 CUMULUS, SPECS and A4Cloud projects were targeted as (a) they explicitly investigate the usage of SLAs for Cloud security/privacy, and (b) are at a stage of maturity where their public results/deliverables have undergone some degree of review by the community.

3.1.1. Cumulus – Certification Infrastructure for Multi-layered Cloud Services[8]

Name:	Percentage of uptime
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	The percentage of time the resource was considered available, in comparison with the total elapsed time.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting HA: High Availability

Name:	Percentage of processed requests
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	The percentage of successful resource requests processed by the provider over the total number of submitted requests.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely provisioning requests
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	Measures the provider's ability to respond to provisioning requests for a resource within a maximum predefined delay.

[8] Please refer to http://www.cumulus-project.eu/

State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting HA: High Availability

Name:	Service provider data access level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the confidentiality level of the resource with respect to the personnel operating the CSP.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Percentage of systems with time synchronization
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the percentage of distinct clock sources in the resource that are synchronized with a reference point (usually through NTP). This is useful for reliable audit trails.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Maximum measured time difference
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the maximum absolute difference between distinct clock sources in the resource (independently of any reference time source such as NTP).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud

	CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Number of (successful) audits performed
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the number of independent reviews and assessments performed during a predefined period of time (for example, annually).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Tenant isolation level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the level of isolation provided to a resource owned by a tenant with respect to other competing tenants.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity

Name:	Data portability
Type:	Academic
Cloud service life-cycle phase:	Procurement, Operation and Termination
Source:	EU FP7 Cumulus
Description:	Data contained in the resource and belonging to the customer can be exported in predictable time, in a documented, open format.

State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Mean time between incidents
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute represents the average time elapsed between the recordings of two consecutive incidents applicable to the resource
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely incident reports
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute represents the percentage of incidents that are reported to the customer within a predefined time limit after their discovery, over the total number of incidents recorded.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely incident responses
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute represents the percentage of incidents that are

	assessed and acknowledged by the provider within a predefined time limit after their discovery, over the total number of incidents recorded.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely incident resolutions
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute represents the percentage of incidents that are resolved within a predefined time limit after discovery, over the total number of incidents recorded
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	User authentication and identity assurance level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute measures the strength of the mechanism used to authenticate a user accessing a resource.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Mean time required to revoke a user
Type:	Academic
Cloud service life-cycle phase:	Procurement, Operation and Termination

Source:	EU FP7 Cumulus
Description:	This attribute describes quantitatively how fast an organization revokes users' access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer)
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Password storage protection level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes how passwords are protected in the resource
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data DI: Data Integrity

Name:	Cryptographic brute force resistance
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute expresses the strength of a cryptographic protection applied to a resource based on its key length, using the ECRYPT 8 level. Instead of using key lengths alone, which are not always directly comparable from one algorithm to another, this normalizing scale allows comparison of the strengths of different types of cryptographic algorithms
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data DI: Data Integrity

Name:	Key access control level
Type:	Academic

Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	The attribute describes how strongly a cryptographic key is protected from access, when it is used to provide security to the resource (or assets within the resource).
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data DI: Data Integrity

Name:	Cryptographic module protection level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the level of protection that is afforded to cryptographic operations in the resource through the use of cryptographic hardware modules.
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data DI: Data Integrity

Name:	Country level anchoring
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute indicates that all processing operations applicable to the resource only take place within a set of predefined countries.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Data deletion quality level
Type:	Academic
Cloud service	Procurement, Operation and Termination

life-cycle phase:	
Source:	EU FP7 Cumulus
Description:	This attribute measures the quality of data deletion, ranging from 'weak' deletion where only the reference to the data is removed, to 'strong' deletion where data is overwritten / destroyed.
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data

Name:	Percentage of timely effective deletions
Type:	Academic
Cloud service life-cycle phase:	Procurement, Operation and Termination
Source:	EU FP7 Cumulus
Description:	This attribute describes how many deletion requests made by the customer and applicable to the resource are effectively completed within a predefined time limit
State of practice:	No
Recommended best-practice:	No
Use case:	SD: Processing Sensitive Data

Name:	Percentage of tested storage retrievability
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attributes describes the percentage of data stored in the resource that has been verified to be retrievable during the measurement period.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Durability
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This security attribute describes the durability for stored data:

	the average percentage of data in the resource that will not be lost over a certain period, due to software or hardware failures.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Vulnerability exposure level
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the vulnerability exposure level of the resource in terms of numbers of vulnerabilities found with regards to the number of vulnerabilities tested, and the number of vulnerabilities that are relevant to the platform/software of the resource and a reference vulnerability source.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely vulnerability corrections
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute refers to the provider's ability to respond to vulnerabilities applicable to the resource with corrective measures within a maximum predefined delay.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of timely vulnerability reports
Type:	Academic

Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute refers to the provider's ability to report vulnerabilities about the resource to customers within a maximum predefined delay.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Recovery point
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the recovery point objective (RPO) or recovery point actual (RPA) of the resource. The RPA represents the data freshness of a backup – i.e. the time elapsed since data was stored for the purpose of eventually restoring the system in a stable state, for example in a backup
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity

Name:	Recovery time
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the recovery time of the resource: this is the time that is needed after a failure to restore the system to a stable state.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity

Name:	Percentage of authorized personnel that received training on the Information System
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the percentage of authorized personnel that has received relevant training on the Information System in order to ensure that is capable of configuring, installing, and operating the information system, and an effective use of the system's security features.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Percentage of recovery success
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the percentage of successful backup restorations performed and verified to be correct (by a checksum, a format check, etc.).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity

Name:	Configuration change reporting capability
Type:	Academic
Cloud service life-cycle phase:	Design/Evaluation & Execution/Changes
Source:	EU FP7 Cumulus
Description:	This attribute describes the capability of the provider to report changes to the resource. The value of the attribute should be able to represent configuration change types in a standardized manner.
State of practice:	No
Recommended	No

best-practice:	
Use case:	AP: App on a Cloud CB: Cloud Bursting DI: Data Integrity HA: High Availability

Name:	Percentage of timely configuration change notifications
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute refers to the provider's ability to report resource configuration changes within a maximum predefined delay.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting DI: Data Integrity HA: High Availability

Name:	Percentage of compliant applications
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 Cumulus
Description:	This attribute describes the percentage of executable applications within the resource that have been explicitly approved for use. The monitoring of approved applications is performed by first detecting the available applications on the resource and cross checking them against a predefined list of applications or an approved baseline application set, using version control, pattern recognition and/or hashes.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

3.1.2. A4Cloud[9] – Cloud Accountability Project

Name:	Authorized collection of PII
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 A4Cloud
Description:	This metric describes the coverage of authorizations for collecting personally identifiable information (PII).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Privacy Program Budget
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 A4Cloud
Description:	This metric describes the percentage of the organization's IT budget that is allocated for establishing and maintaining a privacy program.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Privacy Program Updates
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 A4Cloud
Description:	This metric describes the frequency of updates to the privacy program, policies and procedures by a competent role (e.g. Data Protection Officer (DPO)).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

[9] Please refer to http://www.a4cloud.eu/

Name:	Periodicity of Privacy Impact Assessments for Information Systems
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 A4Cloud
Description:	This metric describes the periodicity of Privacy Impact Assessments for Information Systems.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Number of privacy audits received
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 A4Cloud
Description:	This metric describes the number of independent reviews and assessments performed to the privacy program, policies and procedures in place.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

3.1.3. SPECS – Secure Provisioning of Cloud Services based on SLA Management

Name:	Forward secrecy allowance
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Enables the use of forward secrecy (FS) on a cryptographic channel.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	HSTS (HTTP Strict Transport Security) support
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Usage of HSTS protocol.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity

Name:	HTTP to HTTPS redirects support
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Enables redirections from HTTP to HTTPS tunnels.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity

Name:	Mandatory use of secure cookies
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Forces usage of secure cookies.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Use of client certificates for authentication
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS

Description:	Enables the use of client certificates for SSL/TLS-based authentication.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data DI: Data Integrity

Name:	Enables OCSP stapling
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Enables the use of OCSP for requesting the status of a digital certificate.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	Certificate pinning support
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Enables the pinning for digital certificates.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	Support of Encryption (client-side) for browser connections
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Using browser extension prevents MITM attacks where a custom JavaScript payload could be delivered that could read any secret.
State of practice:	No
Recommended	No

best-practice:	
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	Support of convergent encryption (client-side)
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	For a selected file to be encrypted a hash is generated by a trusted third party and then used as a key for encryption
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	Support for cryptographic hardware integration.
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	CSPs/Cloud Partners might provide hardware support to key management and other cryptographic capabilities.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity

Name:	Connection rate limit to impede brute force attacks
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Rate limit (upper threshold) of allowed connections per minute to implemented security mechanisms. This (positive integer) rate limit can be used to detect a suspicious behavior. If the specified value is 0, no checks will be applied.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud

	SD: Processing Sensitive Data DI: Data Integrity

Name:	Usage of validation tokens to detect anomalous user behaviour
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Enabling the validation of tokens might help to detect anomalous user behaviours. This implies different levels of detection requiring users tracking, hashes of tokens, or sourcing IP addresses which can also result on privacy vulnerabilities.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

Name:	Support for e2e encryption
Type:	Academic
Cloud service life-cycle phase:	Procurement, Operation and Termination
Source:	EU FP7 SPECS
Description:	End to end encryption can be supported, where keys are managed by the CSP.
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud CB: Cloud Bursting SD: Processing Sensitive Data

Name:	Level of redundancy
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	The replication level of the component being measured (typically applied to storage).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data DI: Data Integrity HA: High Availability

Name:	Provider's multi-tenancy support
Type:	Academic
Cloud service life-cycle phase:	Procurement and Operation
Source:	EU FP7 SPECS
Description:	Shows if multi-tenancy is supported on the provider's side (typically applies to VMs on IaaS).
State of practice:	No
Recommended best-practice:	No
Use case:	AP: App on a Cloud SD: Processing Sensitive Data

3.2. SLA Requirements: Legal, Personal Data Protection and Governance

There is no generic format, structure, obligation or best practice to document SLOs/Attributes related arrangements by Cloud service providers or by the relevant contractual parties, and per region, market, industry and kind of service, application and subject matter. These arrangements are sometimes presented in one combined and complex document, or split up in several documents where the context gets lost. However, it is commonly understood that these SLA aspects need to be documented in some way and that such arrangements have important and notable legal and related impact, consequences, implications and other effects, both by law and by contract.

As a brief and preliminary introduction to Chapter D2.2, this Paragraph describes several main SLA related challenges and requirements in the Cloud landscape. The basis for this is the current EC Cloud Service Level Agreement Standardisation Guidelines[10] ('EC Standardisation Guidelines').

3.2.1. SLA Architecture

The Cloud SLA describes and sets SLOs/Attributes for the Cloud service. A Cloud SLA generally is part of an overall (master) Cloud services agreement (MSA). It can also be spread in several parts thereof, as described below. For the avoidance of doubt, each and every part is collectively referred to as SLA or Cloud SLA, even though there may be more documents involved. The full structure thereof can be defined as the SLA architecture.

[10]https://ec.europa.eu/digital-agenda/en/news/Cloud-service-level-agreement-standardisation-guidelines

The organization and the names used for the MSA and its associated documents can vary considerably and the location of a particular SLO/Attribute within the document set can also vary. These documents may include, but are not limited to:

- Service Agreement
- Master Service Agreement (MSA)
- Service Level Agreement (SLA)
- Process Level Agreement
- Processor Agreement
- Privacy Level Agreement
- Acceptable Use Policy
- Privacy Policy
- Security Policy
- Business Continuity Policy including Disaster Recovery Plan
- Service Description

It is important for the Cloud service customer to understand the complete set of documents that govern the Cloud service and to identify SLOs/Attributes wherever they occur.

3.2.2. Legal Life Cycle & Cloud SLA Life Cycle

As identified earlier in Sections 1.2 and 2.1, the Cloud SLA Life Cycle is only part of the total ecosystem that establishes all the various legal (contractual and non-contractual) relationships between a CSP and a Cloud customer from the very first contact of these parties, through assessing, discussing, negotiating out, documenting and executing and nurturing the various legal relationships, which ecosystem can be described as the legal life cycle. The Cloud SLA Life Cycle is an important part thereof, zooming in on the SLA related elements of the relationship. As an example, another part of the legal life is the Data Life Cycle, mentioned in this document as well.

In Section 2.1, three main phases of the Cloud service life cycle are identified. When zooming in on one (1) SLA only from a legal, negotiation and contract management perspective, the life cycle of a SLA can be identified, being the following seven (7) headline Cloud SLA life cycle phases. There are further detailed based on the Cloud SLA life cycle mentioned in Section 2.1 as:

- Assessment
- Preparation
- Negotiation & Contracting
- Execution & Operation

- Updates & Amendments
- Escalation, and;
- Termination & Consequences of Termination

Examples

Name:	Document transparency
Type:	Industry
Cloud service life-cycle phase:	Assessment
Source:	Legal practice
Description:	It is not easy to find or otherwise obtain Cloud SLAs in general, and a comprehensive set of related documents in general that sets out the complete scope of Cloud service offerings and related legal rights and obligations. Cloud customers and its advisors such as Cloud architects and IT managers have difficulty to map these out so they can assess the offerings, including terms and conditions, let alone compare those with other offerings in order to make an informed decision on what to services to use, what to expect and what to trust. Even CSPs have difficulty in providing such comprehensive set, for several reasons, including the lack of transparency of Cloud service offerings and the unwillingness to make it possible for Cloud customers to compare its offerings with competitors and other peers.
State of practice:	Yes
Recommended best-practice:	No
Use case:	Access to, and usability of Cloud SLAs

Name:	Assumptions, carve-outs & exclusions
Type:	Industry
Cloud service life-cycle phase:	Preparation
Source:	Legal practice
Description:	If Cloud SLAs provided by Cloud customers describe certain SLOs/attributes, it is important that any and all assumptions, carve-outs and exclusions are correctly, clearly and accurately described ad detailed. This 'small-print' is quite important in order to properly assess the Cloud service, the offered levels thereof, and which SLOs/attributes that are important for the Cloud customer are missing and need to either be requested and negotiated out with such or another CSP, or be taken into account as a risk and allocated otherwise such as with an (additional) investment or insurance.

State of practice:	Yes
Recommended best-practice:	Yes
Use case:	Mapping and scoping carve-outs and other out-of-scope services

Name:	Knowledge & boldness (how) to negotiate
Type:	Industry
Cloud service life-cycle phase:	Negotiation & contracting
Source:	Legal practice
Description:	Cloud SLAs provided by Cloud customers are less fixed and non-negotiable as Cloud customer may think. For once as not only Cloud customers but also the CSPs are in this phase of this maturing Cloud services market searching for the proper offering and level of services and SLOs, and certain Cloud services and the deployment thereof as more legacy systems, software and services have as well need extra attention before it can be used by the Cloud customer and its end-users in the way contracted. As Cloud customers are obtaining more knowledge of what they and their end-users want and need, and obtain more insights in the Cloud services offerings of the prospective CSP as well as its competitors and peers, such Cloud customer has a better position to discuss, negotiate and contract out a Cloud SLA that is actually understandable, satisfactory, and workable for both the Cloud customer and the CSP.
State of practice:	No
Recommended best-practice:	Yes
Use case:	SLA Negotiation

Name:	Data Life Cycle Monitoring & Amendment
Type:	Industry
Cloud service life-cycle phase:	Updates & Amendments
Source:	Legal practice
Description:	If CSP and the Cloud customer have made clear arrangements on the classification and several types of data, the permitted use as well as the data life cycle thereof per classes, type and deployment, and the monitoring of those arrangements before parties execute the Cloud SLA, the execution and operation phase of the SLA life cycle is the phase to monitor, audit, update and where necessary amend those arrangements, not only to optimize the use of the Cloud services but also to aim to prevent the risk of breach of contractual or local legal requirements, and pro-actively mitigate incidents and related damages in case such breach occurs.

State of practice:	No
Recommended best-practice:	Yes
Use case:	Data Life Cycle Management

Name:	Data portability
Type:	Industry
Cloud service life-cycle phase:	Termination & Consequences of Termination
Source:	Legal practice
Description:	Cloud SLA rarely describes the data portability format, data portability interface or the data transfer date. One of the fundamental issues forgotten by both CSPs and Cloud customers is describing exactly what data is with scope of such portability arrangements, and what other data than customer data needs to be made available, accessible and transferable. This leads to discussions, vendor lock-in incidents and other escalations that are to be avoided.
State of practice:	No
Recommended best-practice:	Yes
Use case:	Transparent and unambiguous SLA language

3.3. SLA Requirements: Economic Aspects

As identified earlier in this document, the Cloud SLA Life Cycle is only one part of the overall process that establishes relationships between a CSP and a Cloud customer. All SLA requirements have an economic impact but there are differences between the supply and demand side priorities such as return on investment versus cost-driven market. This section looks at the supply-side perspective where return on investment can often be a priority for CSPs and SMEs alike, and costs are driving the market.

The go-to-market strategy of CSPs can also vary. For instance, smaller providers such as Numergy mainly sell through indirect channels via its partners. This means the SLAs and the associated contract signed with the final user/customer is drafted-by/signed with the partner (integrator, ISV, VAR, etc.). Other CSP, in particular larger organisations such as Amazon and Google, usually sell directly to customers online and provide “take it or leave it” SLAs online.

SLAs are key elements for any Cloud contract and from an economic perspective SLOs form the basis upon which providers can measure return on investment against penalties due to not meeting contractual obligations. State of the Art SLOs that ensure a balance

between customer and CSP economic priorities do not exist. We analyse here criteria that a SLA should fulfil in order to establish a trusted relationship.

The following table outlines a number of issues that should be taken into consideration when assessing SLAs from an economic aspect. The use case can evolve around and result in different appreciation of SLA issues such as those in Table 2:

Table 2 Issues related to use case and SLA

Terms	SLA-Ready Definition
Predictable cost	Capability given to the customer to know the cost of consumed services. This is important for all Cloud customers purchasing services. Having a final cost is key to transparency
Billing periodicity	The availability of a payment schedule. This is important so customers know what to pay and when to pay it. This is particularly important for small firms budgeting on a short-term basis.
Pertinence of the SLA	Measure the adequacy between the provided services and the SLA. All customers need to clearly understand what is being offered and how in order to fully realise the benefits of Cloud computing.
Impartiality of the SLA Measurement process	The SLA measurement process should be impartial and transparent for customers to trust their provider. Standard measurements are needed for this.
Penalty	Financial compensation owed when the SLA is not respected by the CSP. Current practices typically push the penalty claims entirely onto the customer. Customers must be fully aware of this and know how to make a claim and when it needs to be made.

While the SLAs can differ, including the criticality of a given SLO, depending on the use case (as explained above in section 3 of this document), common grounds may still be found when analyzing the economic requirements.

The following tables show the state of practice at Numergy, with reference to the terms mentioned in the table above. They can be considered common requirements which are

an important step towards establishing a fair and balanced relationship between the CSP and SMEs:

Name:	Predictable cost
Type:	Industry
Cloud service life-cycle phase:	End of service
Source:	Market and customer feedback
Description:	Before using a new Cloud service the customer has an accurate estimation of the costs involved. When using the service the customer understands the cost of the services consumed.
State of practice:	The “pay as you go” Cloud service comes with a billing notification on a monthly basis. As a common business practice, the cost of Cloud services is often calculated after the consumption of the service using a measured indicator. E.g. the number of incoming data packet. Example SLA text: “You will be notified at least 30 days in advance of any changes to the Pay-As-You-Go rates. New services may be added periodically to the xxxxx platform. We will notify you in advance of these new services and any fees that might be charged for using them. However, you would only be charged if you elect to use the new services.”
Recommended best-practice:	All costs are predictable before consumption. The cost is supervised on the fly.
Use case:	All

Name:	Billing periodicity
Type:	Industry
Cloud service life-cycle phase:	Execution
Source:	Market and customer feedback
Description:	A customer can anticipate payment for the consumed services.
State of practice:	The “pay-as-you-go” Cloud service comes with a billing notification to the customer usually on a monthly basis. As a common business practice, the bill is established by the CSP using its own indicators as a measurement system to calculate cost (compute, storage, etc.). Billing and periodicity are the two ways in which the CSP or customer can manage or control the cash flow. Therefore, it is important to establish a balanced payment schedule that makes sense to both sides.
Recommended best-practice:	Bills should be issued on a maximum monthly basis. Shorter billing periods should apply to high volumes that come with a higher billing

	cost. The customer should be informed in advance of the frequency of the billing related to the service, ensuring that the billing schedule is known and accepted by the customer. The bill date shall be the date of meter reading. The bill shall clearly explain the consumed services for which a payment is claimed.
Use case:	All

Name:	Pertinence of the SLA
Type:	Industry
Cloud service life-cycle phase:	Design/Implementation & Execution
Source:	Market and customer feedback
Description:	To be pertinent, the SLA accurately describes the services provided.
State of practice:	SLAs are mostly defined from the point of view of the CSP. Depending on the specific service, SLAs typically cover diverse aspects and parameters ranging from the complexity and the cost effectiveness of implementing the measurement process and technical aspects.
Recommended best-practice:	The SLA clearly describes the service provided in a language that the customer can easily relate to. For example, the availability of the service does not equate to the availability of the platform. While CSPs link the SLA to the platform availability, customers are more concerned with the availability of the service. Measurements should be performed on core functionalities from a credible end-user scenario.
Use case:	All

Name:	Impartiality of the SLA Measurement process:
Type:	Industry
Cloud service life-cycle phase:	Design/Implementation & Execution
Source:	Market and customer feedback
Description:	The SLA should have a specific process for users to measure and measure it.
State of practice:	In most cases the SLA is measured by the CSP but the processes and tools used are not described and not modified.
Recommended best-practice:	It is recommended to use a trusted and impartial third party tool to measure the availability that uses different external and internal points. Active and passive technologies: Passive technologies are non-intrusive and use network statistics to rebuild the use of the service. Active technologies emulate end-user behaviour to check the

	availability of the service.
Use case:	All

Name:	Penalties
Type:	Industry
Cloud service life-cycle phase:	Execution
Source:	Market and customer feedback
Description:	Penalties are the counterpart of the SLA for service availability
State of practice:	The calculation of penalties uses complex formulas with a series of exemption clauses. The customer has to prove that the service has not fulfilled the SLA and make a claim for credits as the typical form of penalties.
Recommended best-practice:	The agreement is represented in a calculable way. Each SLA should be presented as a set of predicates. In order to monitor and process the SLAs and their parameters must be measurable, preferably in numbers, not descriptions. For numerical parameters, basic predicates based on simple algebraic relations can be defined such as following: p1. param < threshold p2. Threshold < param p3. value1 < param < value2 (conjunction of p1 and p2) and so forth. Three main modes can be implemented to manage the SLA contracts: • Real time" reporting with Alarm List, • On demand" reporting with Reporting Module, • Automatic, scheduled reporting with separate Reporting Module
Use case:	All

3.4. SLA Requirements: Sociological Aspects

The sociological analysis starts with an understanding of the difficulties a user has to face before contracting Cloud services in terms of SLA terminology that does not always capture the technological and legal aspects. As already discussed in Section 3.2, SLA terms are often scattered over multiple documents, addressing each of them separate aspects that the user should then carefully analyse and relate to each other. In some cases, a dedicated section for SLA documents is not available on the public website referring the user to the legal and privacy terms of the service usage. The definition of terms might be even given under different articles of the same document (see CloudSigma SLA policy terms, pg 48) or terms related to privacy & security are not always included under the available SLA terms. The need for companies to protect their business from potential legal disputes or liability for potential losses and damages makes the life of the user harder in

clearly identifying and extracting the relevant elements of the Service Level Agreements, then comparing the different offers. All these sociological factors can be detected via an analysis of the user behaviour in contracting Cloud services.

Other relevant sociological factors come from the user not being able to negotiate the terms of an SLA with a take-it-or-leave-it situation. This lowers user expectations in the potentials of Cloud services for their business or even losing interest in using public Cloud solutions.

Liability is another important aspect to consider. Public Cloud providers might not offer adequate compensations in case of damages, like data loss or unauthorized access due to security breaches. The lack of a specific indication of the security precautions the Cloud service provider uses or the possibility to negotiate them in the SLAs, under the Quality of Protection terms, might not assure the experienced users who would like to rely on Cloud for its business. In this situation the reputation of the brand of the Cloud provider plays an important role: the user, if not experienced, tends to trust large Cloud players more over small ones, since they might give the perception of a more reliable service or security measures even if the SLA terms are less detailed or do not include any compensation in case of faults. The recent incidents of security breaches[11] and large scale leakage of data have contributed to a socially driven change in the factors that influence customers entrusting data and raised concerns about Cloud provider's contractual obligations and fulfilment of SLAs. Indeed, SMEs are now starting to be concerned of the risks in sharing data and have less trust in organisations and service providers. More than 78% of users find it hard to trust how companies use their personal data[12], perceiving that too much information is held by organisations. The unclear SLA framework and the limited access to monitoring data to verify whether a Cloud provider has violated a contractual term, contribute to the mistrust in the contractual SLA guarantees.

[11] Cloud Security Alliance. "Cloud Computing Vulnerability Incidents: A Statistical Overview". March 2013

[12] Orange. "The future of digital trust: A European study on the nature of consumer trust and personal data". February 2014. Available from: http://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf

3.4.1. Cloud Service model and SLAs: A customer perception of uptime

Cloud services can be offered under different models, among the most common IaaS, PaaS and SaaS. Customers expect a different type of service for each of the Cloud model they are interested to.

CSPs offering services of different Cloud models use a general SLA that is common to all of services with additional documents clarifying the characteristics, (for example, Amazon AWS Customer Agreement with the EC2 and S3 services and HP Cloud SLA) or publish most of the definitions applicable to multiple services in a single document (e.g., Microsoft Azure). In all cases, the only SLA term present in all documents is the uptime or availability of the service, which can be guaranteed up to 99.95% in some cases. This guarantee can be meaningless in most of the cases since it should be analysed based on the type of service it applies but most importantly to the type of business the service is essential. For instance, 99.95% monthly availability only permits about 21 minutes of downtime (and in most cases 99.9% with a 40 minutes period of downtime), that can correspond to large money loss for a company if it happens during the most critical period for the business. While these percentages can be very promising for most of the business using the Cloud, it might be critical for a business that needs reliability of the infrastructure of the Cloud services in general to function correctly. The compensation of the CSP in such cases is only in service credit percentage!

3.4.2. Security/Privacy contemplated in SLAs

There is still a large gap for security and privacy terms in SLAs. Security is contemplated in the SLA documents or agreements regulating the contract in a qualitative form, not expressing any clear information about the type of security measure, the maximum response time to incidents, or what is the impact of security breaches to services for customers? This lack of detail does not offer any valuable means for customers to judge how their applications and data are duly protected and what the risks of using Cloud services. The privacy regulation is still under discussion, but the new directive should oblige Cloud providers to share the liability for data breaches and violations of the law. Currently, only a few providers contemplate the terms of the new European directive on data privacy and privacy terms are not part of the SLA, as mainly discussed under the Acceptable User Policies which regulates all information the user gives the CSP, even for accessing services. This could be a large barrier for companies that need to analyse carefully the terms and have the opportunity to have them implemented in a SLA as they are liable with their corresponding customers if Cloud services are used for their business. An unclear framework and the lack of flexibility and security features CSPs could guarantee is a barrier towards the trust on Cloud services.

3.4.3. Simple vs. complex SLA terms

The perception of SLAs change from customer to customer based on the type of information they are looking for or the way it is presented, generating two extreme cases. On the one hand, there are lengthy documents explaining all caveats with numbers that might have little mining for the customers who might not have the means to monitor and verify their correctness, see the case of most of CSPs so far discussed. On the other hand, a simple web page with the main information presented in a more readable form for the average customer with an easy explanation of the issues, while not providing a clear definition for all terms discussed, see https://www.greenqloud.com/sla/. A SLA should be a transparent document, easily understandable by the prospective customers, especially small firms with few resources, and clearly covering all aspects of the Cloud service.

Table 3 Terms for the Sociological Analysis

Term	SLA-Ready Definition
Security, privacy and trust	Security SLOs can be either quantitative or qualitative. The C-SIG identifies eight categories for security. However, relevant SLOs may not exist for each of them. In the sociological context, the most relevant SLOs include service reliability security incident management and reporting, monitoring, auditing and security verification (e.g. certifications available), and service changes. In terms of the sociological analysis, risks assumed by the Cloud customer (perceived or real) are a major aspect. Lack understanding, expertise and skills can impede a proper risk assessment on the part of many SMEs. Ultimately, this is about lack of control with risks outweighing benefits. In this respect, it is useful to compare concerns and actual behaviour.
Codes of Conduct in relation to data controller compliance	As data controller, the Cloud customer must accept responsibility for abiding by the applicable data protection legislation. The customer has the obligation to assess the lawfulness of the processing of personal data and to select a CSP that facilitates compliance with the applicable legislation. Relevant SLOs include applicable data protection codes of conduct, standards and certifications. The sociological analysis looks at (i) understanding; (ii) acceptance and (iii) actions taken to ensure compliance on the part of the

	Cloud service customer. It also assesses the extent to which the CSP makes available all the necessary information, e.g. information enabling the assessment of the service, standards or certification schemes.
Openness, transparency and notice	The Cloud customer is capable of fulfilling its obligation as data controller only if the CSP informs the customer about all relevant issue. Relevant SLOs include list of tier 1 subcontractors, special categories of data (Transparency in the Cloud means that it is necessary for the Cloud service customer to be made aware of Cloud service providers' subcontractors contributing to the provision of the respective Cloud service), as well as accountability, e.g. personal data breach policy, documentation. The sociological analysis examines the extent to which transparency practices are effectively provided based on selected examples sourced by the project.

3.4.4. What do customers and analysts highlight?

The following views from an initial comparison of CSP SLAs, Cloud customers and analysts that highlight a number of interlinked requirements, especially from a sociological point of view, such as lack clarity, transparency and risk-taking from a customer point of view. They therefore also help explain the lower than expected uptake of Cloud services.

Access to the SLA: Cloud SLAs can be hard to find, if they are available at all. Different CSPs publish the SLA in different sections of the website. Sometimes the terms and conditions are in a different section of the website. Examples:

Memset: http://www.memset.com - SLA under top menu "Support" - www.memset.com/support/sla

CloudSigma: www.cloudsigma.com - SLA is under "Legal", right at the bottom of the homepage www.cloudsigma.com/legal-switzerland

Green Cloud: www.greencloud.com - under "Legal" at the bottom of the homepage but clearly labelled 'SLA' www.greencloud.com/sla

Market structure and Cloud pricing models: The Cloud service market is currently price driven[13]. CSPs have very different approaches to Cloud pricing models. Pricing cuts take place on a regular basis among the top CSPs (According to Business Insider, AWS has dropped prices 8% from October 2013 to December 2014, while both Google and Microsoft have cut prices 6% and 5%, respectively, in the same period, while other Cloud providers, such as Rackspace and AT&T, have lowered their prices even more).

Factoring in types of service, **network costs, and security**: The very different public Cloud pricing models make direct comparisons difficult with increased risks on the customer side. Some CSPs charge for network traffic; some do not. Some charge for replication services, and some provide it as a standard feature. Understanding the pricing models of each public Cloud contender will constitute most of the work when comparing prices, cost differences and which services are delivered.

The actual price of the service is only a single data point. The low price will lose its value if the service chosen does not meet expectations. The customer also risks paying more than necessary. Put simply, if the Cloud service does not fit the customer requirements, it is not right at any price.

In order to have a better idea of the final Cloud service price tag, prospective customers of a Cloud service need to factor in the type of service, network costs and security. What does the SLO tells us about the types of service, charges for network traffic, security and management? What are the sociological barriers to a clearer understanding or related to lack of resources?

Performance metrics: Service providers should address these concerns by sharing performance metrics beyond basic availability and uptime with their customers. It's not enough to simply keep tabs on whether all the lights are on in the data centre; Cloud providers need to offer insight into IT performance from an outside-in perspective so that they can monitor how their Cloud infrastructure is impacting on their customers and report back to them transparently. (Ref: Michael Allen, Solutions VP, Dynatrace)[14].

[13] See, for example, http://fortune.com/2015/05/26/which-Cloud-company-is-next-to-go/ and https://www.sdxcentral.com/articles/news/ibm-goes-full-openstack-for-Cloud-services/2015/05/.

[14] http://www.techweekeurope.co.uk/cloud/cloud-management/cloud-provider-sla-2015-159831

Lack of customer guarantees: SLAs are just marketing tools: guarantees give consumers faith that the service provider can deliver, and service credits make them believe they can 'punish' the provider if the provider lets them down. But in reality, service providers structure their contracts so they have much to gain, and little to lose, if something goes wrong. Although SLAs may provide an indication of a service's performance, enterprises must remember that downtime, poor performance, security breaches and data losses are their risks to bear. End users must evaluate the risks, against the costs and the benefits, and plan accordingly. (Ref: The 451 Research Take)[15].

[15] http://www.techweekeurope.co.uk/cloud/cloud-management/cloud-provider-sla-2015-159831

4. Elicitation of Requirements

This section presents an initial compilation of the CRM requirements based on the SLA requirements landscape from Sections 2 and 3. The initial set of CRM requirements is not intended for completeness, but more to elucidate the (a) SLA lifecycle, (b) the commonly used SLA elements observed over security, privacy, legal, sociological and economic aspects, and (c) the basic categorization of SLA elements to highlight concepts versus market reality. The intent of this document is primarily to collect information and perform a preliminary analysis, while D2.2 (final version of D2.1) will systematically conduct the gap analysis on the SLA SoA based on the baseline criteria shown in this section.

We do highlight that the various requirements of SLA's (cf., Section 3) also display varied degrees of sophistication and real-world adoption. Given the classical performance basis in the development of SLA's, the economic factors dominate for classical technical metrics of performance, reliability, uptime, etc. as detailed in Section 3.4. As expected, the attributes in Security, Personal Data Protection and Legal aspects are primarily propositions as the economic criteria for these in SLA's are still mostly qualitative. The lack of quantitative measures supporting security, personal data protection and legal aspects also makes it hard to associate economic contracts around them.

The initial compilation of the SoA in SLA components led to a common set of certain needed elements for the SLA-Ready CRM as identified and addressed in Section 3. These elements are presented and structured in Table 4. The initial compilation of these requirements furthermore led to the following observations:

- The set of surveyed metrics clearly shows the need for standardized definitions and also for industrial feedback to empirically validate them. Most of the metrics (and in consequence also the SLOs) found at the state of the art have either been produced by the research community or by potential Cloud customers that are envisioning state of the art use of the potential of Cloud computing. This opens evident questions about their feasibility, economics and applicability in real-world Cloud services scenarios. SLA-Ready will partially contribute to the ongoing validation efforts in working groups like the recently created CSA Metrics WG, and the corresponding ad-hoc group within ISO/IEC SC38.
- Furthermore, while most of the metrics presented in Section 3 are applicable primarily to the first two stages of the SLA life cycle it is also clear the need to devote more efforts to elicit technical metrics that can be related to the SLA termination process. The next version of the present deliverable, i.e., D1.2, will further elaborate this particular issue.

- The initial 18 requirements set out below are the main and vital requirements derived and bundled from best practices from the business-to-business real-world market. These include both national, European and global (including SMEs) organsiations, including several hundred relevant professionals involved (such as procurement, sourcing, IT, business/sales, contract, legal, finance and compliance departments), in more than 5,000 business-to-business deals the past decade representing a revenue of €5 billion revenue. They have also recently been validated by several senior Cloud architects as being requirements that SMEs and other companies and organisations use to check, verify, compare and assess Cloud service offerings, including Cloud SLAs.

Table 4 Preliminary SLA-Ready's Common Reference Model requirements

Item	Name of SLA element	Description
1	SLA URL	If the SLA is publicly available, what is the website URL where it can be found? (Reference is made to Section 3.3)
2	Revision date	What is the date of the last revision? (Reference is made to Section 3.2)
3	Last update	Is the SLA updated regularly? (Reference is made to Sections 3.2 and 3.3)
4	Findable	Can the SLA easily be found on the CSP's website? (Reference is made to Section 3.3)
5	Nr. of pages	How many pages does the SLA consist of? (Reference is made to Section 3.3)
6	Contact details	Helpdesk number or other details to contact the CSP (Reference is made to Section 3.3)
7	Service Credit	Does the CSP provide service credits? (Reference is made to Sections 3.1, 3.2 and 3.3)
8	How are service credits assigned	Who determines whether a service credit shall be provided? (Reference is made to Sections 3.1, 3.2 & 3.3)
9	Maximum service	How much does the CSP credit? (Reference is made to

	credits	Sections 3.1 and 3.3)
10	SLA change notifications	Does the CSP provide SLA change notifications? (Reference is made to Sections 3.2 and 3.3)
11	Unilateral change	Can the CSP change the SLA unilaterally? (Reference is made to Sections 3.2 and 3.3)
12	SLA duration	What is the validity period of the SLA? (Reference is made to Sections 3.1, 3.2 and 3.3)
13	SLA reporting	Does the CSP provide reports about the SLA performance? (Reference is made to Sections 3.1, 3.2 and 3.3)
14	SLA continuous reporting	Are the CSP reports updated continuously? (Reference is made to Sections 3.1, 3.2 and 3.3)
15	SLA transparency	Does the SLA provide transparency on its attributes? (Reference is made to Section 3.3)
16	Data & (Personal) Data protection	Is there something mentioned about data and (personal) data protection? (Reference is made to Sections 3.2 and 3.3)
17	Feasibility of specials & customisations	Are there “specials” and other customisations possible (as far as we know)? (Reference is made to Sections 3.1, 3.2 and 3.3)
18	General Carveouts	What are the assumptions, exclusions, scope of force majeure, and other carve outs to the Cloud services, SLOs and SLA? (Reference is made to Sections 3.1, 3.2 and 3.3)
19	Performance SLOs	These relate to the SLO aspects of, for example, availability and capacity.
20	Security SLOs	This requirement comprehends SLOs related to cryptography, authentication and other aspects derived from relevant security control frameworks.
21	Data Management SLOs	These SLOs related to the measurable description of the CSP’s data life-cycle’s commitments.

22	Personal Data Protection	This SLO category includes those related to accountability and codes of conduct.

The first 18 requirements in Table 4 are important to take into account and consideration, even though these for obvious reasons where not incorporated in the EC Standardisation Guidelines.

The EC Standardisation Guidelines are an excellent platform to build a comparison sheet in order for potential Cloud customers to assess whether, based on their SLAs, Cloud services are interesting to procure and use, and to compare several, possibly relevant CSPs. Therefore, the initial set of SLA-Ready CRM requirements considers in particular the same SLO categorization from this report, as seen on items 19 – 22 (cf. Table 4). We acknowledge the fact that some specific SLOs/Attributes in the Guidelines will likely never be found in a SLA, but in general most are present. The analysis in D2.2 will provide a comprehensive mapping between the metrics presented in Section 3 and the SLO categories from Table 4.

The requirements presented in Table 4 will be used as a baseline for analyzing an initial set of collected Cloud SLAs (i.e., the SLA Repository discussed in Section 5). The results will be presented in D2.2 as a gap analysis, and applied by WP3 to start eliciting the corresponding best practices.

5. The SLA Repository

This section reports the current development of SLA-Ready's Cloud SLA repository. The planned repository will be publicly accessible by the end of the project, providing customers with a searchable catalogue of different CSP SLA. These will be analyzed with respect to the final SLA-Ready CRM requirements. The repository (along with the analyzed information) will also be integrated into the final version of SLA-Ready's social marketplace (cf. WP4).

This section discusses the limitations (e.g., legal and technical) related to the deployment of the repository, along with the information sources to be used for gathering SLA information, the initial layout of the repository, and the first version of the criteria to be adopted by SLA-Ready to analyze the compiled SLAs. The information extracted and analyzed from the repository will be another foundation of WP2's CRM for Cloud SLAs.

5.1. Catalogue of CSPs

The initial version of SLA-Ready's SLA repository will be based on a list of CSPs comprising those listed on the CSA's STAR Repository[16]

The reason why we are initially leveraging the CSA STAR Repository is because it provides the only listing of CSPs where Cloud customers can get an impartial view and understanding of which security and privacy requirements are satisfied by which CSPs.

The CSA STAR is a public website where CSPs are invited to publish their answers to standardized set of security and privacy related questions (CAIQ[17]). This provides customers with an overview of a CSP's security and privacy posture. This public repository contains data related to more than 130 public CSPs worldwide. Available information is presented according to CSA Open Certification Framework (CSA OCF, namely:

- Self-assessment reports based on the security controls proposed by CSA Cloud Control Matrix[18] (CSA CCM).
- Third-party assessment summaries also based on the CSA CCM.

Providers on the CSA STAR have a strong commitment with both security assurance and transparency. Through WP4, SLA-Ready partners will contact the CSPs listed in the CSA-STAR requesting that their analyzed SLAs are made publicly available in the SLA-Ready repository.

5.2. Preliminary design of the repository's structure

The SLA-Ready repository will go beyond gathering a set of Cloud SLAs. The consortium recognizes the need to develop useful information based on the gathered SLA data, which may be used to create awareness in SMEs willing to exploit the full benefits of Cloud computing. For this reason, the compiled SLAs will be analyzed based on the initial requirements criteria described in Section 4. In this way, users of the repository will be able to compare side-by-side the different CSPs based on the baseline SLA-Ready's CRM requirements. As mentioned in Section 4, on one hand the foreseen analysis will result on the elicitation of gaps required to further develop the CRM (WP2), and on the other hand on the identification of "common denominators" across CSPs that will be part of the best practices (WP3).

[16] Please refer to https://cloudsecurityalliance.org/star/

[17] https://cloudsecurityalliance.org/research/cai/

[18] Please refer to https://cloudsecurityalliance.org/research/ccm/

5.3. Accessibility

In order to develop the referred repository of SLAs and related documentation, the varied CSP information needs to be structured. This includes the CSP general information, including name, URL, brief description of services, and information related to last update in repository, as well as applicable service model (any of IaaS, PaaS or SaaS), link to the latest webpage addressing CSP's SLA and the like.

However, there is a potential legal barrier to publication. For example, copyright and other intellectual property rights, and whether the presented version of a CSP's SLA is the most current version. Other issues may arise from opinions raised on the SLA, or other reputational and other damages.

Hence, for these and also as per strategic reasons (e.g., SLA-Ready should not be influenced by a CSP) the first version of the repository (to be reported in D2.2) will be accessible only for internal research use. It is our expectation that subsequent releases may become publicly accessible depending on the feedback received from the Advisory Board, and once all potential legal concerns have been addressed.

6. Conclusions

This report presented the first version of SLA-Ready's Common Reference Model based on a preliminary survey of the relevant landscape (state of art and state of practice). The consortium followed a multidisciplinary approach to gather and categorize relevant Cloud SLA information (e.g., including both technical and legal aspects), although common denominators like the lack of standard vocabularies and commonly used sets of metrics were evident from all perspectives. Our preliminary review resulted on the elicitation of several requirements that will be used to guide the subsequent work in WP2, including D2.2 and in particular the CRM design to take place in D2.3 and D2.4.

This deliverable also reported about the initial design and content (including an initial list of CSPs to consider) of the SLA Repository. On one hand, our initial analysis provided the consortium with further (legal and related) insights related to the feasibility of publicly releasing the first version of the repository. On the other hand, this task also proved useful to start designing the methodology and criteria to analyze the actual content of the SLAs in order to provide an added value to the SLA-Ready repository. The "SLA evaluation" criteria (mostly based on the requirements elicited in Section 4) will be further developed (and validated) by WP2 so it can become one of the framework's core elements. The set of elicited requirements shown in this report will be used by WP2 and WP4 to analyze the SLAs comprising the repository, in order to start the identification of gaps and best-practices.

7. Annex 1 References and Source Documents

Table 5 References and source documents

SDO	Ref #	Title/Topic	Relevance to SLA-Ready (preliminary analysis)
ISO/IEC SC27 WG1	27004	Information security management – Monitoring, measurement, analysis and evaluation	Discusses important aspects associated to the management of Cloud security SLAs.
ISO/IEC SC27 WG1	27007	Guidelines for information security management systems auditing	SLA-Ready might contribute with a discussion on the role of auditors and SLAs.
ISO/IEC SC27 WG3	19791	Information technology – Security techniques and Security assessment of operational systems	As above, SLA-Ready might contribute with a discussion on the role of security assessment and SLAs.
ISO/IEC SC27 WG3	Study Period	Continuous security monitoring of operational systems	Terms of reference in this study period may fit the SLA topic.
ISO/IEC SC27 WG4	27044	Guidelines for security information and event management (SIEM)	Research community has identified a strong link among SLA management and SIEM.
ISO/IEC SC27 WG4	19086-4	Cloud computing – Service Level Agreement (SLA) Framework – Part 4: Security and privacy	Highly relevant standard for SLA-Ready given its SLA focus.
ISO/IEC SC27 WG4	27036-4	Information security for supplier relationships – Part 4: Guidelines for security of Cloud service	Early draft with potential to integrate a discussion on the role of SLAs.

ISO/IEC SC38 WG3	19086-1	Cloud computing – Service Level Agreement (SLA) Framework – Part 1: Overview and concepts	Highly relevant standard for SLA-Ready given its SLA focus.
ISO/IEC SC38 WG3	19086-2	Cloud computing – Service Level Agreement (SLA) Framework – Part 2: Metrics	Highly relevant standard for SLA-Ready given its SLA focus.
ISO/IEC SC38 WG3	19086-3	Cloud computing – Service Level Agreement (SLA) Framework – Part 3: Core requirements	Highly relevant standard for SLA-Ready given its SLA focus.