SLA - Ready

Making Cloud SLAs readily usable in the EU private sector

www.sla-ready.eu


**Title**: Requirements emerging from a state-of-the-art analysis - Final Report

**Author(s)**: Ruben Trapero, Neeraj Suri, TUDA; Arthur van der Wees, Arthur

**Contributor(s)**: Jesus Luna, CSA; Silvana Muscella & Stephanie Parker, Trust-IT.

**Date**: 31 December, 2015

Revised version following Year 1 review. Re-submitted 29 April 2016

HORIZON 2020

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

## Executive Overview

Negotiating a Cloud Service Level Agreement (Cloud SLA) is usually the reserve of large organisations with considerable budgets. By contrast, most small firms are typically offered a standard agreement, which they either accept or decline.

SLA-Ready aims to change this state of play by providing a common understanding of Service Level Agreements (SLAs) for Cloud services with greater standardisation and transparency so small 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. terminology, SLA attributes, Service Level Objectives (SLO), guidelines, as well as best practices and relevant standards to fill identified gaps in the current SLA landscape.

SLA-Ready will develop the Common Reference Model systematically following a two-fold approach. Firstly, we have analysed the SLA landscape by collecting data and eliciting requirements (D2.1 - Requirements emerging from state-of-the-art analysis). Secondly, we have made a more detailed gap analysis to shape further the Common Reference Model (2.2. Requirements emerging from a state-of-the-art analysis - Final Report). This final report, presented here, focuses on the following:

- Requirements compiled from a state-of-the-art/practice analysis.
- Analysis on missing requirements.
- Final requirements of the Cloud Service Provider (CSP) SLA repository.

D2.2 is the final version updated over D2.1 that provide the refined version of the initial SLA state of the art/practice (SoA/SoP) reported in D2.1, in order to form the basis of composing the CRM. The progress with respect to D2.1 is:

- The elicitation of the requirements of the CRM has been reorganized according to the components specified by the ISO/IEC 19086 standard.

[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.

- A comprehensive analysis of the SLA Management SoA/SoP has been added.
- The components of SLA have been extracted from additional sources: EU projects, ISO/IEC 19086, C-SIG, legal and industry practices.
- Performance components have also been added to the model.
- A comprehensive analysis of the economic and sociological aspects of the Cloud Service provisioning has been done.
- The elicited requirements are aligned with the revised life cycle model.
- The description of the SLA Repository has been updated to the final version.

**Policy Context**

The terms used in the SLA-Ready analysis are consistent with the terms applied in Chapter 2 of the European Commission's Cloud SLA Standardisation Guidelines [2], published in June 2014 (hereafter 'EC Standardisation Guidelines'). The Guidelines are the first output of the Cloud - Select Industry Group (C-SIG) on SLAs, as part of the European Cloud Computing Strategy to increase adoption by businesses through all sectors of the economy by building confidence and trust in cloud computing through safe and fair contracts.

Standardising aspects of Cloud SLAs will improve clarity and increase understanding of the different offers in the market. Clarity of the different aspects covered is important to make SLAs more comparable and comprehensive while being neutral from a technology or business model.

For example, agreements that govern cloud services must account for regional, national and local laws, regulations and policies, including any that relate to a specific sector. However, everyone benefits from globally common concepts, terminology and globally accessible technology.

Well-defined and unambiguous service level objectives are important to ensure the effective standardisation of Cloud SLAs and to enable clear communication between cloud service providers and their prospective customers.

It is also important to keep definitions up to date and consistent with an evolving cloud service landscape. In late October 2015, the European Commission is setting up a new

[2] European Commission, Cloud Service Level Agreement Standardisation Guidelines (C-SIG SLA 2014). Brussels, 2014

phase for the Guidelines by re-convening the industry members of the C-SIG (Cloud – Select Industry Group).

## Table of Contents

## Table of Tables



## Table of Figures

## Document information

| Deliverable number | D2.2 |
|---|---|
| Deliverable title | Requirements emerging from the state-of-the-art analysis – Final Report |
| Deliverable Nature | Report |
| Deliverable dissemination level | Public |
| Contractual delivery | December 2015 |
| Actual delivery date | December 2015<br>Revised version following Year 1 review. Re-submitted 29 April 2016 |
| Author(s) | Ruben Trapero, Neeraj Suri (TUDA), Arthur van der Wees (Arthur) |
| Contributor(s) | Jesus Luna (CSA), Silvana Muscella, & Stephanie Parker (Trust-IT) |
| Reviewer(s) | 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 | 100 |

## Disclaimer

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

## List of Acronyms

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

## *Glossary*

| | |
|---|---|
| **Cloud Service Provider Data** | Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider. Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on |
| **Data controller** | The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data |
| **Data Integrity** | The property of protecting the accuracy and completeness of assets |
| **Data Intervenability** | The capability of a cloud service provider to support the cloud service customer in facilitating exercise of data subjects' rights. Note: Data subjects' rights include without limitation access, rectification, erasure of the data subjects' personal data. They also include the objection to processing of the personal data when it is not carried out in compliance with the applicable legal requirements |

| | |
|---|---|
| **Data processor** | A natural or legal person, public authority, agency or any other body which processes Personal data on behalf of the Data controller |
| **Data protection** | The employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework |
| **Data Subject** | An identified or identifiable natural person, being an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity |
| **Disaster recovery** | Ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption |
| **Failure notification policy** | Specifies the process by which cloud service customers can notify the cloud service provider that a service outage has been observed, the process by which the cloud service provider notifies cloud service customers that a service outage has occurred, the process for providing updates on service outages, who receives notifications and updates, the maximum time between the detection of a service outage and the issuance of a notice of service outage, the maximum time interval between service outage updates and how service outage updates are described |
| **Identity Assurance** | The ability of a relying party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's true, accurate and correct identity |
| **(Master) Cloud services agreement (MSA)** | A legal document is the overarching part relating to the cloud service, that describes the terms agreed between the provider and the customer under which the cloud service is made available and used. The MSA has a number of synonyms such as "Customer Agreement", "Terms of Service" or simply "Agreement". The MSA references a number of subsidiary parts, such as the Cloud SLA, Security and Privacy Policies, the Acceptable User Policy, the Business Continuity Policy and the Service Description. |
| **Metric** | A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement |
| **Personal Data** | Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity |

| | |
|---|---|
| **Personally identifiable information (PII)** | Documented agreement between the service provider and customer that identifies services and service level objectives |
| **Remedy** | Compensation available to the cloud service customer in the event the cloud service provider fails to meet a specified service level objective |
| **Resilience** | Ability of a cloud service to recover operational condition quickly after a fault occurs |
| **Service Level Agreement (SLA)** | Documented agreement between the service provider and customer that identifies services and service level objectives |
| **Service Level Objective (SLO)** | A specific, measurable characteristic of a cloud service for which the cloud service provider makes a commitment |
| **Vulnerability** | A weakness of an asset or group of assets, e.g. software or hardware related, that can be exploited by one or more threats |

## 1. Introduction

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) (D2.3 & 2.4).

The CRM includes an integrated set of SLA components (e.g., common terminology, Service Level Objectives, 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, in particular the ISO/IEC 19086 standard) 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 D2.2 spans the requirements analysis and compiles the results of Task 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 (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 design of the repository of SLAs, to become part of the 'social marketplace for Cloud SLA' built in WP4.

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

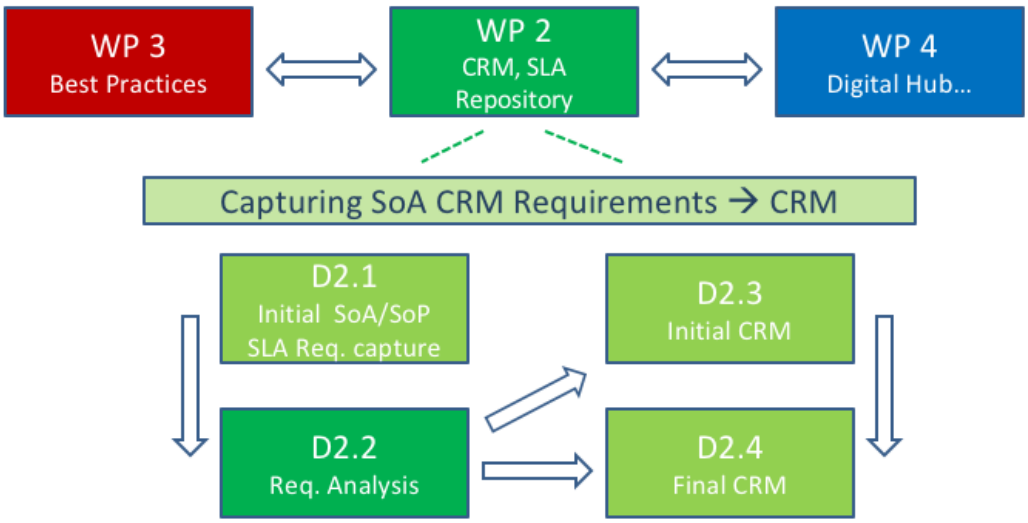
- Compiling a set of SLA-related information spanning the state-of-the-art/practice (SoA/SoP), to elicit the key SLA requirements: technical (performance, security and privacy), legal and socio-economic.
- Defining the foundations of the CRM based on the analysis of elicited requirements
- Initial design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

### 1.1. Positioning D2.2 within SLA-Ready

This deliverable (D2.2) is the second of two iterations of an analysis of requirements emerging from a state-of-the-art analysis of cloud SLAs. D2.2 is the final compilation of the State of the Art (SoA) of SLA attributes covering the areas of security, personal data protection, legal and economic aspects with a particular focus on metrics. The sociological analysis elicits requirements mainly from a cloud service customer, especially the levels understanding and acceptance of the Cloud SLA in the early stages of the SLA lifecycle. Eliciting requirements in these phases can help shed light on barriers to the adoption of cloud services and how we might overcome them. 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. Content from this deliverable will though also be used for awareness raising activities that are part of WP4 (Communications, impact and exploitation).

Figure 1 gives an overview of the role of D2.2 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/receiving feedback from relevant standardization efforts and initiatives, and aligning customer and provider requirements through interaction with the SLA-Ready Advisory Board (AB). Furthermore, WP2 also inputs relevant CRM information to WP3, such as the results of the gap analysis that will provide guidance to developing the best practices and influence relevant standardisation initiatives.

Figure 1. D2.2 within SLA-Ready




The SLA-Repository, a preliminary description is given 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, and more generally cloud services. Thus a core activity of WP4 is making the CRM more useful and practical. Moreover, WP4 will engage with key stakeholders, collecting and analysing feedback on specific information needs including from a socio-economic perspective.

### 1.2. Scope and Methodology

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

Firstly, there is a very wide variety of CSPs, business models and Cloud customers' needs. Hence, it is not feasible to develop a one-size-fits-all SLA CRM. SLA-Ready is driving 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 a "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 SMEs (as Cloud Service Customers, either current or prospective). It is important to note that CSPs and SMEs have very different degrees of technical awareness. The SME may or may not be fully technology savvy or may lack the expertise to interpret the fine nuances of terminology and concepts. Consequently, a "useful" CRM is designed to facilitate bridging this gap between the CSP and the customer. Hence this report documents the State of the Art/Practice aspects of SLAs, in order to develop a common reference model for Cloud SLAs.

### 1.3. Approach for the legal, economic and sociological aspects

Using real-world examples, the proposed approach/framework 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 analyse 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 analyse 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, the approach 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. The analytical framework for legal, economic and sociological aspects is therefore a combination of the following quantitative and qualitative analysis.

**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?

### 1.4. Structure of this report

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

- Section 2 outlines the SLA-Ready advocated use of the SLA lifecycle (aligned from the technical and legal perspectives) to capture the CRM Requirements. It also presents the state of the art on the topics related to the management of SLAs.
- Section 3 defines the template SLA-Ready proposes for capturing the CRM Requirements, in particular the associated SLOs and underlying metrics. This section also details the final set of CRM Requirements of security and privacy, legal and governance, and socio-economic aspects that will lead to a metrics-based analysis approach in subsequent deliverables.
- Section 4 summarizes the elicited set of CRM requirements

- Section 5 outlines the details of the repository of SLA, to become part of SLA-Ready's Social Marketplace.
- Section 6 concludes the report.

## 2. *The Cloud SLA management life cycle*

This section discusses an aligned vision of the technical and legal SLA lifecycles, along with their correspondence to the more general Cloud service lifecycle. Providing such alignment is an important goal of the present deliverable, and is meant to further substantiate the updated set of requirements presented in Section 0.

### 2.1. Aligning the Technical and Legal SLA Life cycles

As mentioned in the previous version of this report there are multiple ways to capture and analyse the requirements that will drive the development of the CRM. A SLA is neither just a single document nor a hard-coded document applicable between a CSP and a CSC. Rather, SLA arrangements evolve through a set of phases that consequently have to be managed in a dynamic manner. Furthermore, the SLA management process is inherently embedded into the Cloud service lifecycle.

While there is not a standard definition for the latter, SLA Ready has for instance studied and evaluated the (A) final ETSI Cloud Standards Coordination report, and (B) the candidate ISO/IEC DIS 19086-1 draft[4]:

A. The final ETSI Cloud Standards Coordination report describes three (3) main phases, namely (i) acquisition, (ii) operation, and (iii) termination. It is worth to highlighting the conspicuous lack of some other main phases, such as for instance the pre-contractual phases of the Cloud SLA life cycle, as well as any Cloud SLA going-concern considerations such as amendment/change orders These missing stages are covered by the legal Cloud SLA lifecycle as described below.
B. From a technical perspective and based on the candidate ISO/IEC DIS 19086-1 draft the Cloud SLA management lifecycle covers the stages of design, evaluation, negotiation and acceptance, implementation and execution and changes. During the design stage, the CSP (sometimes along with the CSC) defines the Cloud services to be covered along with the respective SLO/SQO commitments. Once designed, the CSC proceeds to assess whether the offered Cloud SLA effectively fulfils its

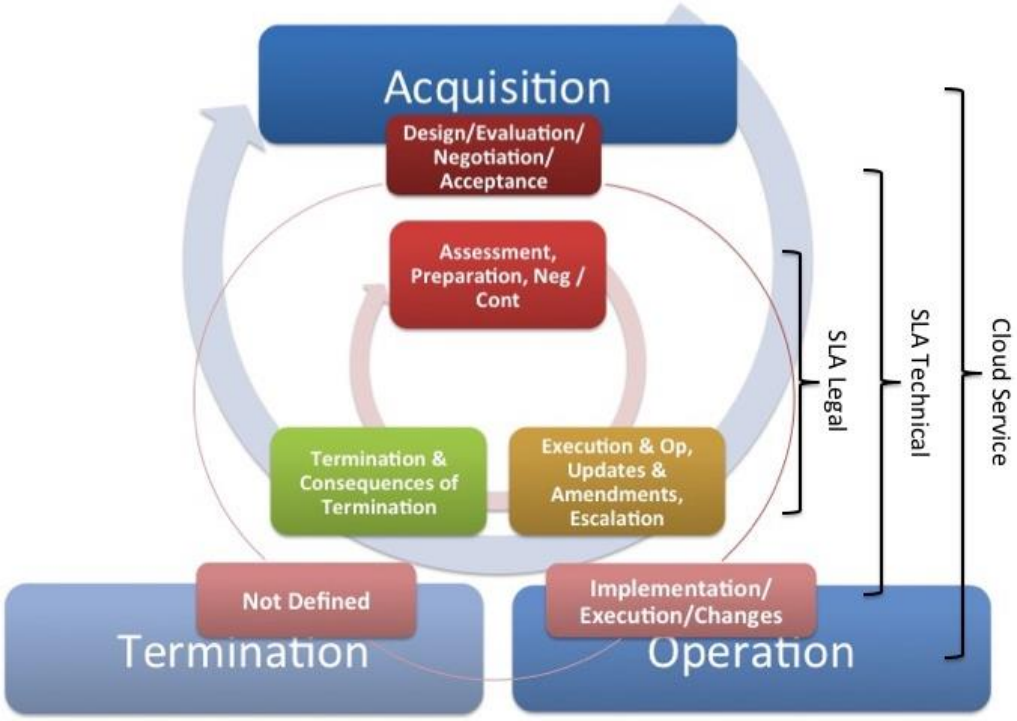
[4] Latest version available at the time of writing this Deliverable.

requirements (evaluation stage) and if supported will engage on a negotiation with the CSP before accepting the SLA. After the Cloud SLA has been accepted/agreed by the CSC it will be implemented (i.e., setting up processes for monitoring and managing the Cloud service, reporting any failures to meet SLOs and SQOs, and claiming any remedies), and executed by the CSP in order to start the provision of the service. From an ISO/IEC 19086-1 perspective, the Cloud SLA lifecycle finalizes with the consideration of a stage devoted to propose changes to the SLA (possibly due to modifications of the underlying ICT system, or evolving CSC requirements). It is worth highlighting the conspicuous lack of any Cloud SLA termination-related consideration in the ISO/IEC 19086-1 lifecycle. This missing stage is covered by the legal Cloud SLA lifecycle as described below.

The relationship perspective, and therefore legal relationship perspective, plays an important role in the study of the Cloud SLA lifecycle. As identified in the previous version of this deliverable (D2.1), the Cloud SLA lifecycle is only part of the total ecosystem that establishes all the various legal (pre-contractual, contractual as well as non-contractual) relationships between a CSP and a CSC. This covers the full process right from the very first contact of these parties, through to assessing, discussing, negotiating out, documenting and executing and nurturing the various relationships (which will in all events entail various legal relationships). This ecosystem can be described as the legal lifecycle.

The Cloud SLA lifecycle (cf., Figure 2) is an important part thereof, zooming in on the SLA related elements of the relationship. As an example, another part of the (legal) relationship between CSP and CSC is the Data Lifecycle which is mentioned in this document as well.

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




When zooming in on a Cloud SLA only from a legal, negotiation, contract management and exit scenario perspectives, the lifecycle of a SLA can be identified as following seven (7) headline Cloud SLA lifecycle phases:

1. **Assessment:** Any relationship starts with pre-assessing what one would like, why, when and with whom (for instance one or more CSPs), so the first Cloud SLA lifecycle phase, Assessment. This includes for instance doing market intelligence, checking specific needs, offerings, CSPs, performance of CSPs and setting up a business case.
2. **Preparation:** This second Cloud SLA lifecycle phase, includes for instance, the first contact and conversation with possible CSPs, further assessment, pre-evaluation and fine-tuning goals and assumptions.
3. **Negotiation & Contracting:** This can include preparing for negotiation and the actual negotiation and deal making with one or more CSPs, including sharing concerns, discuss in-scope and out-of-scope (cloud) services, debating about trade-offs and finding common grounds, reaching agreement, double-checking needs, goals and assumptions, and of course documenting the contractual arrangements, and signing thereof.
4. **Execution & Operation:** includes the actual start of setting up the cloud services, populating the respective cloud service with relevant data, on boarding and

training users, setting up communication channels and further operational activities while using the respective cloud services.

5. **Updates & Amendments:** includes updated or otherwise amended needs, goals and assumptions by the CSC during the term of the ongoing cloud services arrangements, as well as improved or added cloud services by the CSP there under. It also includes optimisation of the respective cloud services by CSP as per (contractual or other) non-compliance, breaches and other incidents during that term.
6. **Escalation:** deals with such (contractual or other) non-compliance, breaches and other incidents during the term of the ongoing cloud services arrangements that have resulted in a dispute that needs escalation, (perhaps even litigation as a last resort), negotiation and resolution, either by parties themselves or by arbitration, court or otherwise.
7. **Termination & Consequences of Termination:** deals with the end of the relationship between CSP and CSC, including the end of the legal relationship even though the latter will generally continue for several years after any termination as per mandatory laws and legislation. This last phase for instance includes the assessment of alternatives, settlement and termination arrangements, cloud services transition projects and services, data export, customer and (end)use care and diligence, and adequate data deletion.

In order to elicit the CRM requirements (cf., Section 3), SLA-Ready advocates the stages associated to the technical and legal Cloud SLA management life cycle by aligning them to the Cloud service management life cycle as follows.

**Table 1. Alignment of technical and legal Cloud SLA lifecycles with the Cloud service lifecycle**

| Cloud service lifecycle (ETSI CSC) | Cloud SLA technical lifecycle (ISO/IEC 19086-1) | Cloud SLA legal lifecycle | Comment |
|---|---|---|---|
| **Acquisition** | Design, Evaluation, Negotiation, Acceptance | Assessment, Preparation, Negotiation & Contracting | 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 is crucial for establishing a SLA between the Cloud Customer and the CSP. If allowed by the CSP, the negotiation of SLA conditions will occur on this stage. |

| Cloud service lifecycle (ETSI CSC) | Cloud SLA technical lifecycle (ISO/IEC 19086-1) | Cloud SLA legal lifecycle | Comment |
|---|---|---|---|
| | | | |
| **Operation** | Implementation, Execution, Changes | Execution & Operation, Updates & Amendments, Escalation | This operational stage 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 (or applying the agreed remedies). 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. Remedies can include changes to the SLA. |
| **Termination** | Not defined | Termination & Consequences of Termination | SLA termination (and its consequences), 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). |

As previously highlighted in this section, it is important to note in Table 1 that the current ISO/IEC 19086 Part 1 draft does not consider the notion of SLA termination. However, this prospective standard discusses a "Termination Policy" as part of a more general "Cloud Service Agreement" just like in the case of the SLA. In this context, the Termination Policy usually deals with the issues that arise when a Cloud customer terminates their use of one or more cloud services. The termination policy might include SQOs for areas such as notifications, data reversibility and data deletion. The ISO/IEC 19086 Part 1 draft also proposes a "Termination of Service" component which deals with the exit process, where the use of a Cloud service agreement is terminated and there is an orderly process by which the Cloud customer stops using the Cloud service.

Relevant SLA components/SLOs related to the lifecycle presented in this section can be found in Section 3.

## 2.2. State of the art

The following section provides a summary of the state of the art about aspects related to the management of SLAs. We have included here the current status of the approaches to define agreements, with special attention to security, and its evolution from policies to SLAs and machine readable specifications. The state of the art also includes a status of monitoring, providers' assessment, and negotiation of SLAs. It is worth highlighting that primarily EC projects are leading these efforts. However, it is worth noting that most EC projects have a significant industry/SME representation for these projects to reflect comprehensive academic and practitioner viewpoints

**Policies and SLAs**

The usage of policies to manage the increasing complexity on the management of networks and systems comes from several decades ago [1]. Even the definition of languages to structure the information included in policies has also been widely studied from a very early stage [3]. More recently, due to the popularity of internet services and the increasing users' concern on security and privacy issues (leveraged by the success of electronic commerce and payments, and social networks) security and privacy policies has also centre the attention of the research and industrial community.

There exist different definitions of security policies. NIST defines a security policy [4] as an "Aggregate of directives, regulations, rules, and practices that prescribes how an organisation manages, protects, and distributes information", and according to (Diver, 2007) the purpose of security policy is to protect people and information, set rules for expected behaviour by users, define and authorise the consequences of violation, minimise risks and help to track compliances with current regulations. Høstland et al. [5] and Kadam [6] focus on the definition and creation of templates for security policies. Depending on their application level, different security policies exist (such as Kannammal et al. [7], and Bronk [8] focussing on the network level). Depending on their purpose, the security policies can be specified at different level of abstraction e.g., at high level of abstraction - through modal logic formulas or a process algebra based language (Benjamin et al. [9]), or an automata based language (Aktug et al [10]). Such policies can be refined through adequate functions [11], in order to preserve security policy through all the degree of abstraction of the system (and language). Karadsheh [12] gives a detailed view of different types of security policies: depending on whether an enterprise information security policy (EISP) for organisational levels is considered, as defined by Whitman et al. [13], or an Issue-specific security policy (ISSP) for corporative services or system specific policies (SysSp) as in [14] by Swanson et al., etc.

Recent efforts have been devoted for including security policies in Service Level Agreements (security SLA or SecSLA). SLAs were typically considered in SoA architectures, such as WSLA [15] and WS-Agreement [16], as well as in cloud computing and grid computing such as by Henning [17]. In SPECS [18], security SLA is taken into account for the negotiation of security levels. Also Luna et al. [19] uses SecSLA as a basis to quantify security in cloud environments. SecSLA are also considered by the industry (Mohahan et al. [20] and Undheim et al. [21] and are adopted in the Web Service domain (Frankova et al. [22]). A set of good practices on modelling SLAs is provided by Feglar in [23].

SLAs provide a convenient way to handle the contents of security policies represented as security provisions (parameters). ENISA's survey [24] shows that currently many customers are unaware of the security aspects contracted with the provider and related to their services and do not control or monitor them. Often the SLAs consider only QoS (Quality of Service) related aspects and security aspects are less covered in spite of the existence of some approaches such as Bernsmed et al. [25]. The specification of security parameters in a security policy forces a provider to explicitly address security that can help cope with this problem.

Another challenge is that security policies or SLAs are often represented in natural language (non-machine readable) which impedes their management by the provider. Furthermore, the format varies from one provider to other. To this end, organisations such as the CSA are trying to provide a common format for the security provisions to be included in security policies and Sec SLA, such as the STAR repository [26]. This issue is also addressed in the researching academia by Zhengwei et al. [27] and Schilling [28].

Bernsmed [25] considers that SLAs can be modelled by a provider at the service level, normally based on either a set of expert-driven security requirements (e.g., for compliance reasons), or some kind of preliminary threat analysis. A machine-friendly approach that expresses the security provisions in the form {security attribute, value} (e.g., {Backup Frequency, Daily} is considered by industrial and academic works such as the ones described by Casola et al. [29], Luna et al. [30] and Taha et al. [31]. Krautsevich [32] also proposed adding security metrics to the agreement and provided a way to reason how well the service satisfies the security needs of the customer. Savola [33] and the CSA with the Cloud Control Matrix [34] goes one step beyond by organising these security provisions into "categories" derived from a taxonomy. This set of security provisions – now organised into taxonomic categories – are easier to be automatically processed, combined in security SLA and managed by users and providers.

More recent research (Luna et al. [35]) improves these models by also including dependencies between provisions that may also affect the subsequent reasoning. Other

activities such as the SLA@SOI project [36] has created a language independent SLA language to add QoS guarantee and party obligations. The SLA@SOI model was adopted by Contrail [37] by extending it to use a standard OVF descriptor to specify IaaS resources. In OPTIMIS [38] the activities were focused on the management of SLAs between infrastructure and service providers. To this end OPTIMIS created a machine readable language based on WS-Agreement and WS-Agreement Negotiation. Finally, 4CaaSt [39] created a description language to capture service dependencies across cloud layers.

**SLA assessment techniques**

Security metrics' importance for the decision making in ICT systems with respect to security has been recognised by organizations such as ENISA [40], CIS [40] and NIST [42]. Security metrics have been applied for quantifying the security of network systems though several attack graph-based security metrics (e.g., Idika et al. [43], Lippman et al. [44], Ortalo et al. [45], Pamula et al [46]), or to measure the degree of trustworthiness of software-intensive systems (e.g., Manadhata et al. [47], Savola [33], Wang et al. [48]). Multiple approaches are emerging to assess the functionality and security of CSPs. Li [49] presents a framework to compare Cloud providers according to performance indicators. Garg et al [50] use the Analytic Hierarchy Process (AHP) to rank providers based also on performance data to measure various Quality of Service (QoS) attributes. A framework of critical characteristics and measures that enable comparison of Cloud services is also presented in [51] by Siegel at al. With respect to security assessment presented by Almorsy et al. [52], the authors propose the notion of evaluating Cloud secSLAs, by introducing a metric to benchmark the security of a CSP based on categories. However, the resulting security categorization is purely qualitative. In Casola et al ([29]) a methodology for evaluating and comparing security SLAs expressed through the use of standard policy languages is presented. Luna [30] uses a similar approach to quantify the security of a Public Key Infrastructure, based on its Certificate Policy. In [53] Ghani et al. present a metric-based approach for assessing the security level of Critical Infrastructures. Security metrics are also used for the definition of SLAs. In [19], Luna et al. point to the need of developing a security metrics framework for the Cloud. Other security-metrics based approach propose mechanisms to describe and quantify security are given in [54] by Breier et al.

Few works focus on security metrics aggregation in order to enable the quantification of the security level in the end-to-end of all collaborators of the supply chain. Unfortunately, metrics aggregation mostly remains a research challenge as acknowledged by NIST [42] and ENISA [55]. Very few frameworks have been proposed to aggregate security metrics. Among them are the works done by Massacci et al. [56], Frankova et al. [22], Seamons et al. [57] and Smith et al. [58]. Predictive approaches for anticipating how security metrics

will develop have been also studied and applied (e.g., Trust Economics system modelling paradigm [59], [60] and the ADVISE modelling approach of [61].

**Negotiation of SLAs**

SLA negotiation is an important mechanism to guarantee the cloud service performance and enhance the trust between cloud service customers and cloud service providers. It has already attracted a lot of attention from academic communities that have proposed several important works.

Web Service Agreement (WSLA [62]) is proposed in the form of the standard protocol and dedicated formatted language, which aims to facilitate service providers in generating a formal copy of web service agreements and achieve real time monitoring on its compliance. It can create a formal contract with corresponding obligations both for service customers and service providers during the entire life cycle as creation, termination and state monitoring are carried out by two main types of services as Agreement Service and Agreement Factory Service. The former service aims to access established agreement content, real-time monitoring on the life cycle management. The later service is for creating agreements for both parties and then instantiating relevant services with corresponding QoS. It is also the base of WS-Agreement negotiation specification that is equipped with enhanced capabilities such as the support of more than one round of negotiation processes, including a language and protocol to negotiate the agreement offer and counter offer.

NextGrid [63] offers a business-objectives oriented service layer agreement and a specific flexible negotiation approach. It supports creating SLA dynamically in order to meet the requirements both from service providers and customers after bilateral consent. Additionally, it also offers a uniform framework to operate and manage the quality of all running services. The mapping mechanism of the uniform framework supports translating business-level objects defined in SLA into resource management policies and translating technical-level monitoring details into business-level consequences for comparing the SLA compliance as well as sending feedback to customers.

HPC4U [64] developed a reliable and predictable SLA-aware Grid middleware to offer several attractive features to the end users. This includes guaranteeing the quality of a critical project independent from underlay IT infrastructure; supporting both commercial and open source software components; organizing components in various groups of modular, implementing features in a transparent manner, etc. The SLA-aware and Grid-enabled Resource Management System (RMS) of HPC4U supports SLA negotiation, multi-site SLA-awareness scheduling, security and interfaces for storage, check-pointing and

networking support. A cluster middleware system will be developed to negotiate service level agreement with customers and assure the run-time SLA compliance.

Finally, BREIN [ref] created a dynamic, intelligent and adaptable infrastructure to increase the level and dynamism of collaborations among companies. It can create SLAs for improving the discovery capabilities of services providers based on its own template of "Semantic Annotated Service Level Agreements" (SA-SLA). The annotation carries a reference to a concept in a semantic model (BREIN Business Ontology) that provides a high level description of a specific terminology which can be translated by the Negotiation Broker and the Contract Net Protocol. Meanwhile, BREIN also improves the dynamic negotiation capability on architectural level, which can apply different kinds of negotiation protocols ranging from discrete offer negotiation to multi-round/phase negotiation.

**Monitoring SLAs**

In IT the term monitoring is an overloaded one. Most of the monitoring techniques that already exist are focused on the monitoring of performance indicators, as shown by Keller et al. in [62], Grabner [66], Ganglia [67], and Nagios [68]. DeSVi [69], [70] include SLA-aware functionalities. Monitoring has also become relevant in the cloud context (for example, the Amazon's CloudWatch [71]. The mOSAIC project focuses on missing monitoring capabilities in this case for multi cloud environments [72]. If we focus on security monitoring, we can see that there is no consensus about what security monitoring should cover and for what. Approaches in the area of continuous monitoring for detection of intrusion and malicious attacks for Web Service Providers or Cloud environment are presented by Brower in [73], Lazarevic et al. [74] and Spanoudakis et al. [75]. SPECS [18] is trying to assess a monitoring infrastructure for security parameters included in a security SLA, thus detecting violations and promoting enforcement activities to improve security. Security monitoring can be deployed across all capabilities, and users, not only the providers that own that responsibility. This is case of federated clouds (Clayman et al. [77]) where the monitoring infrastructure developed adapts automatically to changes in the monitoring capabilities that are available in service based systems running on clouds, following dynamic SLA monitoring checks (Foster et al. [78], [79]). The Lattice monitoring system [80] provides also support for monitoring dynamically changing cloud federations. Finally, NIST's SCAP specifications [81] and Cloud Security Alliance's Cloud Trust Protocol [82] provide interfaces for extracting monitoring data from clouds. In the case of the CTP, the status is still under working group.

## 3. CRM Requirements

This section systematically captures the community best-practices of CRM Requirements. The subsequent subsections individually detail the CRM Requirements as follows. Section 3.1 proposes a template to capture CRM requirements. Based on that template Section 3.2 addresses the technical dimensions of Performance and Data Management components. Section 3.3 addresses Security and Privacy components. Legal and Governance requirements are considered in Section 3.4. Section 3.5 highlights the economic aspects of SLA followed by Section 3.6 covering sociological dimensions. Naturally, the economic requirements are a horizontal attribute that covers all technical, legal and sociological elements of SLA's. We highlight two aspects that are helpful to parse the upcoming subsections 3.2 through 3.6.

Firstly, it is important to note that each CRM 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 3.1) that applies across the multiple CRM 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 CRM 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 CRM Requirements is a contribution that we believe is very helpful in systematically compiling and analysing CRM Requirements, in particular from a metrics perspective. To put this template into 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 customised 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 hundreds of potential (and also use-case based) customizable SLOs 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. This is also based on the feedback received from current standardisation initiatives and recommendations (e.g., the "EC Standardisation Guidelines") through WP3 – International Cooperation, Consensus and Standardisation.

These aspects form the basis of the CRM Requirements capture in the following sections

## 3.1. Capturing the CRM requirements

In order to build the foreseen CRM, it is essential to capture the basic measurable SLOs 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 requirement (Type: Academic, Industry-use, Standards recommendation)
2. Summary description of key SLO /CRM 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: e.g. CSIG-WG, EC Cloud Study, Web pointers.
5. Description of the SLO's purpose and value advocacy in the SLA
6. Is this SLO actually used as a practice? For example, is this SLO used because one is required to use it or because it is a useful SLO?
7. Is this a recommended best-practice SLA?
8. Prominent use-case(s) that apply for this SLO.

Based on these eight elements the proposed elements are represented as in Table 2 to facilitate their gathering and usage in other WPs (in particular WP3 for standardization purposes).

Table 2. 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: | Acquisition, Operation, Termination |
| Source: | EU FP7/H2020, standardisation body, other. |
| Description: | Brief information related to the element (e.g., objective). |
| Use case: | Reference Use Cases as taken from the ETSI CSC report:<br>**AP**: App on a Cloud<br>**CB**: Cloud Bursting<br>**SD**: Processing Sensitive Data<br>**DI**: Data Integrity<br>**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., 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 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 analysing or composing the initial set of ETSI CSC-based use cases.

The information provided by the template will be further analysed in WP2 to develop the basis of the planned CRM. The following sections reports a set of SLAs found both at the Cloud SLA's state of art/practice.

As described in our strategy document (D3.1, Engagement plan for standardisation and international cooperation), where available, the reported SLOs are organized in "components" following the terminology on 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 SLOs 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 underlying SLO's metrics (in

accordance to ISO/IEC 19086 Part 2), rather to describe them from the SME perspective through the template introduced in Section 2.

### 3.2. Performance and Data Management Components

The following tables report SoA Cloud SLA performance and data management, metrics. There are two ways to classify the CRM Requirements either by the functionality of the SLO or by the lifecycle phase. As advocated in Section 3.1, the latter represents the logical progression of developing a SLA and thus our choice. It is worth pointing out that many SLO are valid over more than one phase of the SLA lifecycle and this is clearly indicated in the template.

| | |
|---|---|
| Name: | Response Time |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | The maximum time between a defined stimulus or input to the cloud service and a defined point in the response. |
| Use case: | CB: Cloud Bursting<br>HA: High Availability |

| | |
|---|---|
| Name: | Capacity |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | This clause explains service properties related to the capacity of the service that can be included in the cloud SLA. These properties related to capacity include not only the capacity of the cloud resources (such as storage space, processing power) but the capacity of the network used to access the resources. |
| Use case: | CB: Cloud Bursting<br>HA: High Availability |

| | |
|---|---|
| Name: | Elasticity |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | The elasticity component describes the ability of a cloud service to dynamically adjust the amount of resources that are allocated to an instance of the service. The adjustment is performed on the basis of the current workload of the cloud service instance, i.e., |

| | |
|---|---|
| | increased workload results in the allocation of more resources, while decreased workload is answered by the de-allocation of resources.<br>Elasticity is related to one or more resource types. For instance, a virtual machine combines the following resources: Number of processors of a given specification, size of memory, number of network interfaces, size of hard drive, etc. Resources for a Web-based application service can be the number of parallel user sessions, and/or the number of parallel transactions. |
| Use case: | CB: Cloud Bursting<br>HA: High Availability |

| | |
|---|---|
| Name: | Service Resilience |
| Type: | Standards |
| Cloud service life-cycle phase: | Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | The availability of a cloud service can be impacted by faults, or failure of hardware and software components that underlie the cloud service. Since cloud services are housed in data centres, potential faults can also occur on the facilities and infrastructure side. Fault tolerance can be defined as the service's ability to remain in operation in the event one or more components fail while resilience is the ability of a service to recover after a fault occurs. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Customer data backup/restore |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation, Termination |
| Source: | ISO/IEC 19086-1 |
| Description: | The CSC data backup and restore component includes SLOs and SQOs such as backup methods, backup retention periods and the number of backup generations. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Disaster recovery |

| | |
|---|---|
| Type: | Standards |
| Cloud service life-cycle phase: | Operation, Termination |
| Source: | ISO/IEC 19086-1 |
| Description: | Ability of the ICT elements of an organisation to support its critical business functions to an acceptable level within a predetermined period of time following a disaster. The Disaster Recovery Component covers SLOs and SQOs such as the CSP's disaster recovery plan, Recovery Time Objective and Recovery Point Objective. |
| Use case: | CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | IPR |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | "Ownership" of data is a complex combination of intellectual property rights and control, and separate agreement on each of those issues is key to a meaningful overall agreement. The law, regulation, and custom for Intellectual Property Rights for data vary with different locations and the assignment of rights is closely tied to the business arrangement between the CSC and CSP, requiring a clear and comprehensive agreement about IPR. |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Cloud Service Customer Data |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation, Termination |
| Source: | ISO/IEC 19086-1 |
| Description: | Rec. ITU-T Y.3500 \| ISO/IEC 17788 defines cloud service customer data as a class of data objects under the control of the CSC. For example, such objects can include files, BLOBs, tables, database entries, emails and other objects created using the cloud service or transferred to the CSP for temporary or long term processing or storage. Cloud service customer data includes data input into the cloud service by the CSC and the results of the CSC's use of the cloud service to process that data. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| | DI: Data Integrity |

| | |
|---|---|
| Name: | Cloud Service Provider Data |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation, Termination |
| Source: | ISO/IEC 19086-1 |
| Description: | Rec. ITU-T Y.3500 \| ISO/IEC 17788 defines CSP data as a class of data objects unique to the operation of the cloud service under control of CSP. Unless the CSC and CSP specifically agree to include other data objects or data classes, all data used only to provide the cloud service is CSP data. Access control lists that govern tenant access to resources are an example of CSP data. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Account Data |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation, Termination |
| Source: | ISO/IEC 19086-1 |
| Description: | Account data is class of data specific to each CSC that is required to sign up for, purchase or administer the cloud service. This data includes information such as names, addresses, payment information etc. Account data is generally under the control of the CSP although each CSC usually has the capability to enter, read and edit their own account data but not the records of other CSCs. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Derived Data |
| Type: | Standards |
| Cloud service life-cycle phase: | Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | Rec. ITU-T Y.3500 \| ISO/IEC 17788 defines derived data as a class of data objects under CSP control that are captured as a result of interaction with the cloud service by the CSC. For example, an analysis of CSC use of the system based on a log of attempted log-ins is derived data, as is the results of analysing a collection of speech utterances from users of a speech recognition system. |

| | |
|---|---|
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Data portability |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | Cloud data portability includes the movement of data between cloud services to support distributed processing or to enable movement of data to another cloud service. Data portability includes the portability of cloud service customer data and other data objects as agreed between the CSP and the CSC. Data portability may be offered at limited data fidelity for storage optimization or similar reasons. For example, if images stored on a cloud service are converted to a lower resolution and only that lower resolution image is then available to the cloud service customer. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Data deletion |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | Data deletion is the removal of access to cloud service customer data through the user and administrator capabilities of the cloud service. Cloud services routinely replicate data across multiple servers and locations to improve the security of the data in the event of a system failure and improve the availability and performance of the data in normal processing. As a result, deletion of all instances of the data may require specific procedures and take significant time. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Data location |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | Cloud service customer data may be subject to requirements for |

| | |
|---|---|
| | the physical location of the data or the movement of that data across geographic jurisdictions. These requirements are potentially in conflict with the operation of a cloud service that distributes data over multiple locations to support data protection, efficiency of processing and effective support and maintenance of the service. |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Data examination |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | CSPs may electronically examine incoming data or files before being passed to the cloud service to prevent materials prohibited by the terms of service from being processed or stored on their systems. For example, a cloud email service may scan incoming emails for malware, spam or pornographic images. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Law Enforcement Access |
| Type: | Standards |
| Cloud service life-cycle phase: | Acquisition, Operation |
| Source: | ISO/IEC 19086-1 |
| Description: | CSCs and CSPs are subject to requests from law enforcement and the courts for information in the cloud service. CSCs and CSPs may also be required to preserve data from deletion in anticipation of a request, either by an existing regulation or practice or a specific request to retain specific data. Different jurisdictions have varying requirements for data acquisition and retention. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Data Life Cycle Monitoring & Amendment |
| Type: | Industry |
| Cloud service life-cycle phase: | Acquisition |
| Source: | Legal practice |
| Description: | If the 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. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Data portability |
| Type: | Industry |
| Cloud service life-cycle phase: | 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 |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

## 3.3. Security and Privacy Components

The following tables report SoA Cloud SLA security and personal data protection metrics. The CRM Requirements from the security and personal data protection point of view covers the technical elements of SLAs typically encountered by SMEs in 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 3.1) that is amenable to projecting these key elements and also for the subsequent gap analysis.

### 3.3.1. Organisation of Information Security

| | |
|---|---|
| Name | Privacy Program Updates |
| Type: | Research |
| Cloud service life- | Acquisition and Operation |

| | |
|---|---|
| cycle phase: | |
| 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)). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Support |
| Type: | Recommendation |
| Cloud service life-cycle phase: | Operation |
| Source: | C-SIG |
| Description: | Support is an interface made available by the cloud service provider to handle issues and queries raised by the cloud service customer. |
| Use case: | DI: Data Integrity<br>SD: Processing Sensitive Data |

### 3.3.2. Human Resources Security

| | |
|---|---|
| Name: | Percentage of authorized personnel that received training on the Information System |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Configuration change reporting capability |
| Type: | Research |
| Cloud service | Acquisition and Operation |

| | |
|---|---|
| life-cycle phase: | |
| 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>DI: Data Integrity<br>HA: High Availability |

### 3.3.3. Access Control

| | |
|---|---|
| Name: | Service provider data access level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | This attribute describes the confidentiality level of the resource with respect to the personnel operating the CSP. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| | User authentication and identity assurance level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | This attribute measures the strength of the mechanism used to authenticate a user accessing a resource. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Mean time required to revoke a user |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and 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) |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Password storage protection level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | This attribute describes how passwords are protected in the resource |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name | HSTS (HTTP Strict Transport Security) support |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Usage of HSTS protocol. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Use of client certificates for authentication |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Enables the use of client certificates for SSL/TLS-based authentication. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Enables OCSP stapling |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Enables the use of OCSP for requesting the status of a digital certificate. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Certificate pinning support |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Enables the pinning for digital certificates. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

### 3.3.4. Cryptography

| | |
|---|---|
| Name | Cryptographic brute force resistance |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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 |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Key access control level |
| Type: | Research |
| Cloud service | Acquisition and Operation |

| | |
|---|---|
| life-cycle phase: | |
| 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). |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Cryptographic module protection level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Forward secrecy allowance |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Enables the use of forward secrecy (FS) on a cryptographic channel. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | HTTP to HTTPS redirects support |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Enables redirections from HTTP to HTTPS tunnels. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

| | |
|---|---|
| | DI: Data Integrity |

| | |
|---|---|
| Name: | Mandatory use of secure cookies |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Forces usage of secure cookies. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Support of Encryption (client-side) for browser connections |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Support of convergent encryption (client-side) |
| Type: | Research |
| 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 |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Support for cryptographic hardware integration. |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | CSPs/Cloud Partners might provide hardware support to key |

| | |
|---|---|
| | management and other cryptographic capabilities. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Support for e2e encryption |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation and Termination |
| Source: | EU FP7 SPECS |
| Description: | End to end encryption can be supported, where keys are managed by the CSP. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data |

### 3.3.5. Physical and Environmental Security

| | |
|---|---|
| Name: | Percentage of timely effective deletions |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and 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 |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Percentage of compliant applications |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud |

| | |
|---|---|
| | CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Usage of validation tokens to detect anomalous user behaviour |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

### 3.3.6. Operations Security

| | |
|---|---|
| Name: | Percentage of uptime |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | The percentage of time the resource was considered available, in comparison with the total elapsed time. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of processed requests |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | The percentage of successful resource requests processed by the provider over the total number of submitted requests. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| | HA: High Availability |

| | |
|---|---|
| Name: | Percentage of timely provisioning requests |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of systems with time synchronization |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 Cumulus |
| Description: | This attribute describes the percentage of distinct clock sources in the resource that are synchronised with a reference point (usually through NTP). This is useful for reliable audit trails. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Maximum measured time difference |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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). |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Number of (successful) audits performed |
| Type: | Research |

| | |
|---|---|
| Cloud service life-cycle phase: | Acquisition 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). |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Vulnerability exposure level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of timely vulnerability corrections |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Percentage of timely vulnerability reports |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Configuration change reporting capability |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Percentage of timely configuration change notifications |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>DI: Data Integrity<br>HA: High Availability |

### 3.3.7. Communications Security

| | |
|---|---|
| Name: | Tenant isolation level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

### 3.3.8. Systems Acquisition, Development and Maintenance

| | |
|---|---|
| Name: | Data deletion quality level |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation and Termination |
| 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. |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Connection rate limit to impede brute force attacks |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| Name: | Level of redundancy |
| Type: | Research |

| | |
|---|---|
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | The replication level of the component being measured (typically applied to storage). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Provider's multi-tenancy support |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 SPECS |
| Description: | Shows if multi-tenancy is supported on the provider's side (typically applies to VMs on IaaS). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

### 3.3.9. Information Security Incident Management

| | |
|---|---|
| Name: | Percentage of timely incident reports |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of timely incident responses |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of timely incident resolutions |
| Type: | Research |
| 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 |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Data portability |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Vulnerability Management |
| Type: | Recommendation |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | C-SIG |
| Description: | A vulnerability is a weakness in an information system, system |

| | |
|---|---|
| | security procedures, internal controls, or implementation that could be exploited or triggered by a threat.<br>Management of vulnerabilities means that information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

### 3.3.10. Business Continuity Management

| | |
|---|---|
| Name: | Country level anchoring |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Percentage of tested storage retrievability |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Recovery point |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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 |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| Name: | Recovery time |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

| Name: | Percentage of recovery success |
|---|---|
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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.). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity |

### 3.3.11. Compliance

| | |
|---|---|
| Name: | Number of privacy audits received |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

### 3.3.12. Openness, transparency and notice

| | |
|---|---|
| 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. |
| Use case: | SD: Processing Sensitive Data<br>DI: Data Integrity |

| | |
|---|---|
| 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Authorised collection of PII |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 A4Cloud |
| Description: | This metric describes the coverage of authorizations for collecting personally identifiable information (PII). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

### 3.3.13. Individual participation and Access

| | |
|---|---|
| Name: | Mean time between incidents |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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 |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

### 3.3.14. Accountability

| | |
|---|---|
| Name: | Privacy Program Budget |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Privacy Program Updates |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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)). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Periodicity of Privacy Impact Assessments for Information Systems |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition and Operation |
| Source: | EU FP7 A4Cloud |
| Description: | This metric describes the periodicity of Privacy Impact Assessments for Information Systems. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Number of privacy audits received |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

### 3.3.15. Privacy compliance

| | |
|---|---|
| Name: | Privacy Program Budget |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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. |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Privacy Program Updates |
| Type: | Research |
| Cloud service life-cycle phase: | Acquisition 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)). |
| Use case: | AP: App on a Cloud<br>SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Purpose Specification |
| Type: | Recommendation |
| Cloud service life-cycle phase: | Acquisition |
| Source: | C-SIG |
| Description: | In general, the cloud service provider may not process personal data, pursuant to the service agreement with its customer, for its own purposes, without the express permission of the customer. Otherwise, a cloud service provider that process the customers' personal data for its own purposes outside of an |

| | |
|---|---|
| | explicit mandate from its customers (e.g. in order to do market analysis or scientific analysis, to profile data subjects, or to improve direct marketing, all for its own account), will qualify as a data controller in its own right and must fulfil all the relevant obligations.<br>This component defines the list of processing purposes (if any), which are beyond those requested by the customer. |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Data minimization |
| Type: | Recommendation |
| Cloud service life-cycle phase: | Acquisition |
| Source: | C-SIG |
| Description: | The cloud service customer is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes. Furthermore, temporary data can be created during the operation of the cloud service, and may not be immediately deleted once they become unused for technical reasons. Periodic checks should ensure that such temporary data is effectively deleted after a predefined period. |
| Use case: | SD: Processing Sensitive Data |

| | |
|---|---|
| Name: | Intervenability |
| Type: | Recommendation |
| Cloud service life-cycle phase: | Acquisition |
| Source: | C-SIG |
| Description: | Directive 95/46/EC gives the data subject the rights of access, rectification, erasure, blocking and objection. Therefore, the cloud service customer must verify that the cloud service provider does not impose technical and organisational obstacles to these requirements, including in cases when data is further processed by subcontractors.<br>The contract between the cloud service customer and the cloud service provider should stipulate that the provider is obliged to support the customer in facilitating the exercise of data subject |

| | |
|---|---|
| | rights in a timely and efficient manner |
| Use case: | SD: Processing Sensitive Data |

## 3.4. Legal, and Governance requirements

From a CSC perspective, legal, sociological and economic analysis of the situation today also 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 described in Section 1.3, the analysis will cover supply side behaviour (CSPs), demand side behaviour (CSCs) and varying levels of comprehension across both (e.g. consistency of terminology, comprehension of terminology and vocabulary). Legal, sociological and economic analysis will use data from CSPs, the CSC community, including the respective value chains of CSPs and CSCs.

### 3.4.1. SLA Architecture

The Cloud SLA describes and sets SLOs/Attributes for the Cloud service, and defines for instance what services, support, assumptions, performance levels, incident management, remedies and other arrangements is in-scope and out-of-scope.

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.

The organisation 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 or Subscription Agreement
- Master Service Agreement or Master Subscription 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 CSC to understand the complete set of documents that govern the Cloud service and to identify SLOs/Attributes wherever they occur.

#### 3.4.2. Requirements

For obvious reasons, there is no generic format, structure, obligation or best practice to document SLOs/Attributes and related arrangements between CSPs and CSCs. A one-size-fits-all SLA, format, structure, obligation or best practice is also not be feasible or useful. This is because there is an overwhelmingly large variety and choice of service models, deployment models, data, application and users, as well as the choice and variety of market, segment, industry, multi-stakeholder use and involvement, and the value chain both in the chains before the CSP providing cloud services and chains after the CSC procures cloud services. The SLA related arrangements are sometimes presented in one combined set of documents, or split up in several documents and hyperlinks with which the context is difficult to comprehend. 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, operational 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 important SLA related challenges and requirements in the Cloud landscape. The basis for this is the current EC Cloud Service Level Agreement Standardisation Guidelines [1].

### 3.5. 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 CSC. All CRM 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, mainly selling 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 CSPs, 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. It is worth noticing that most of the terms found in this economic analysis are related to the concept of credit management, defined as the mechanism by which amounts are deducted from the amounts to be paid under the contract to the supplier if actual supplier performance fails to meet the performance standards set in the service levels. The use case can evolve around and result in different appreciation of SLA issues such as those in Table 3:

Table 3. 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 such a claim and the timeframe within which it needs to be made. |

While the SLAs can differ, including the criticality of a given SLO, depending on the use case, common grounds may still be found when analysing the economic requirements.

The following tables show components 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: | Termination |
| Source: | Market and customer feedback |
| Description: | Before using a new Cloud service the customer has an accurate estimation of the costs involved.<br>When using the service the customer understands the cost of the services consumed. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Billing periodicity |
|---|---|
| Type: | Industry |
| Cloud service life-cycle phase: | Operation |
| Source: | Market and customer feedback |
| Description: | A customer can anticipate payment for the consumed services. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| Name: | Pertinence of the SLA |
|---|---|
| Type: | Industry |
| Cloud service life-cycle phase: | Acquisition & Operation |
| Source: | Market and customer feedback |
| Description: | To be pertinent, the SLA accurately describes the services provided. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting |

| | |
|---|---|
| | SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Impartiality of the SLA Measurement process: |
| Type: | Industry |
| Cloud service life-cycle phase: | Acquisition & Operation |
| Source: | Market and customer feedback |
| Description: | The SLA should have a specific process for users to measure and measure it. |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

| | |
|---|---|
| Name: | Penalties |
| Type: | Industry |
| Cloud service life-cycle phase: | Operation |
| Source: | Market and customer feedback |
| Description: | Penalties are the counterpart of the SLA for service availability |
| Use case: | AP: App on a Cloud<br>CB: Cloud Bursting<br>SD: Processing Sensitive Data<br>DI: Data Integrity<br>HA: High Availability |

## 3.6. Sociological Aspects

In the context of SLA-Ready, **sociological** refers to human, non-technical aspects, such as:

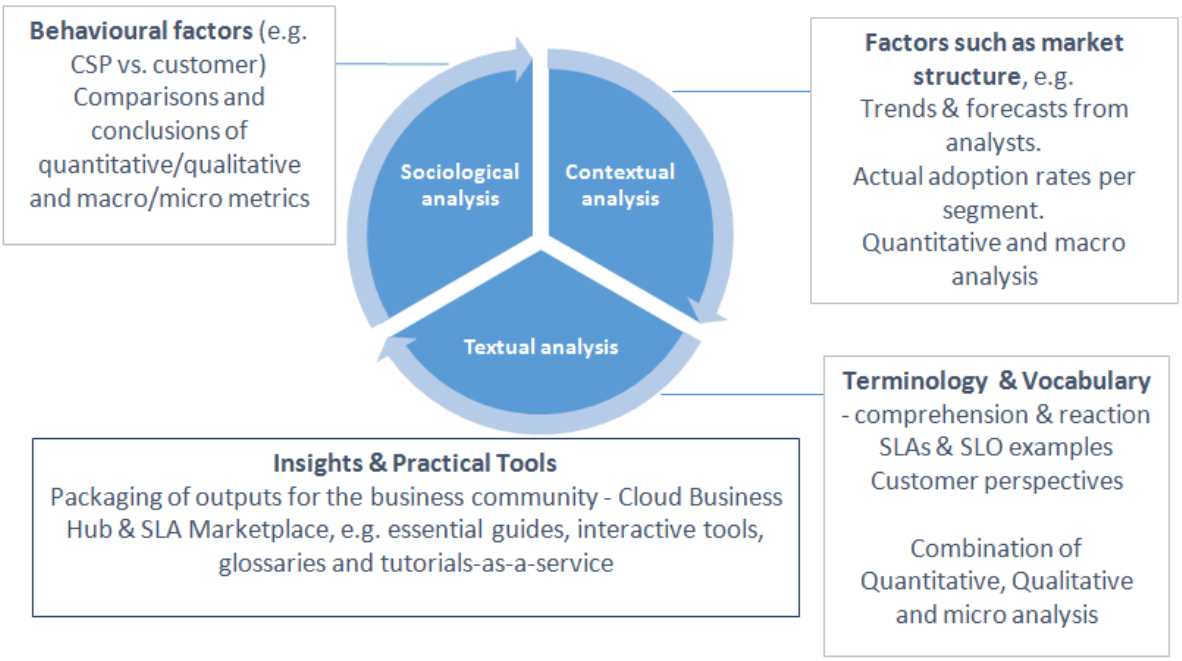
- Knowledge of the cloud and levels of related skill sets, from legal contracts to IT and security expertise.
- Understanding of the cloud service and familiarity with SLAs in general. In our experience only IT professionals have a proper understanding of SLAs.
- Expectations of the cloud service and CSP, as well as the ability to compare offers, just as easily as consumers can compare different products and services on the market.

The following subsections provide with a comprehensive analysis of these aspects that is used to elicit the requirements of the CRM.

### 3.6.1. Analytical Framework

As indicated in Section 1.3, our analysis is both quantitative and qualitative. Compared with the other aspects, it is less concerned with SLOs. The figure below captures the analytical framework we are using also for our socio-economic assessment in WP4.

Figure 3. Analytical Framework




In our sociological analysis, we have taken into account the views of IT analysts, business and IT media. Many of these views continue to highlight issues such as pricing, lack of clarity, transparency and risk-taking, as well as negative customer experiences, including

common mistakes CSCs make when not equipped with sufficient knowledge. We have specifically selected interlinked issues as part of our sociological analysis to help explain the lower than expected uptake of cloud services, and what information SLA-Ready needs to provide to SMEs as its main target group.

### 3.6.2. The SME SLA Challenge: A sociological perspective

Most SMEs in Europe are micros (1-10 employees). Most new businesses, especially the growing number of new digital businesses, are one-man bands, which can gain real benefits from the life-giving properties of the cloud.

According to the EC's EuroStat, for the 80% of organisations not yet using cloud services, insufficient knowledge is the main blocking factor (42%). A survey by the UK Federation of Small Businesses (published January 2015) has found that the top reasons for not adopting cloud services are:

1. Clear terms and conditions.
2. Transparent pricing.
3. A balance between rights and responsibilities of users and providers.

Small firms typically lack the time, money and human resources to spend in investigating new technologies, as well as IT, security and legal expertise. They need a stepwise approach to cloud services, and all related aspects, especially for contracts and SLAs. For a clear path to the cloud, they need practical advice, and insightful but neutral pointers from professionals that can fill their knowledge gaps.

SLA-Ready aims to help prospective SME CSCs understand an SLA piece-by-piece and guide them through the different decisions that need taking along the seven phases described in detail previous sections. Complexities run all the way through these phases. However, the evidence we have collected to date shows that most small firms are not adopting the cloud at the expected rate. This is because they lack understanding as early as the pre-contractual phase, i.e., **assessment** and **preparation**. It is at this phase that the SME CSC has to also consider the overall SLA and implications of the service contract.

Our sociological analysis therefore pays particular attention to this phase. From a broader sociological perspective, we also analyse the issues that may represent barriers for an SME CSC based on our desk research.

The overriding goal is to understand what requirements might constitute a "good enough" SLA for a typical SME, and see how CSPs are responding to the needs of small firms, if at all[5].

### 3.6.3. CSC Questionnaire for Phase 1 of the Lifecycle

In analysing the assessment and preparation phase, we aim to identify potential issues a CSC may encounter in trying to make an informed decision about using a given cloud service. From a sociological perspective, this includes understanding of the CSC obligations and security risks and opportunities [84]. As a first step in identifying related requirements, we have devised a set of questions a typical small firm might pose in the first phase, indicated in the box below.

*How easily can I find the Cloud SLA?*

*Having found and read the contract, how does my first access to the Cloud SLA compare with my first access to the CSP marketing pages on the service? E.g. expectations of the using the services versus complexities in dealing with the SLA.*

*How easy is it for me to understand the terminology? What kind of knowledge or external expertise do I need to help me?*

*How easily can I understand the responsibilities I need to take on? How do the benefits compare with the risks and responsibilities? What about terminating the contract?*

*What support does the CSP offer? How helpful is it?*

*Can I easily compare the SLA and SLOs of different cloud service providers?*

*In deciding to use the cloud service, what key actions do I need to perform during operation?*

*How easy is to understand the termination of the contract, and the respective roles of the CSP and me as the CSC?*

### 3.6.4. Main findings in relation to the Requirements

[5] This analysis also forms part the activities performed by SLA-Ready under WP4 - Communications, Impact and Exploitation, sharing any findings relevant to defining the Common Reference Model.

This subsection highlights the sociological aspects that concerns the SLA management. These aspects are the basis for the elicitation of some of the requirements appearing in Section 4.

***Access to the SLA***

Not every CSP investigated has a publicly available SLA on the corporate website through a URL. In any case, it is hard for the CSC to locate the SLA.

There is no standardised way to access the SLA. Sometimes it appears under "Legal", sometimes under "Support". Sometimes, these sections appear at the very bottom of the website. Only in a few cases is the SLA in a primary position.

The table below provides examples of CSPs headquartered in the both Europe and the U.S.

**Table 4. SLA URL and Findable**

| CSP[6] | Cloud Service |
|---|---|
| Amazon Web Services – EC2 (Elastic Compute Cloud) http://aws.amazon.com/agreement/. US-headquartered | IaaS. Type: compute. Regions: Asia, Australia, Europe, South America, North America |
| CloudSigma Legal offices and jurisdiction in Switzerland. https://www.cloudsigma.com/legal-switzerland/ https://www.cloudsigma.com/legal-usa/ | IaaS. Type: compute. Regions: Europe, North America, South America. |
| Flexiant – Flexiscale, on demand pay as you go hosting solution UK-headquartered http://www.flexiscale.com/support/service-level-guarantee/ | IaaS. Type: compute. Service: servers. Regions: Europe |
| Memset Hosting http://www.memset.com/support/sla/ http://www.memset.com/about-us/service/ | Servers & IaaS. Regions: UK |
| Microsoft Azure (Virtual Machines) with | IaaS. Type: compute. Regions: Asia, Australia, |

[6] Since our first analysis (D2.1), two public cloud service providers have suspended their services: HP and greenQloud though both operate other cloud-related services. See HP http://www.infoworld.com/article/2996131/cloud-computing/facing-facts-hp-had-to-abandon-the-public-cloud.html and https://www.greenqloud.com/greenqlouds-public-cloud-services-close-but-our-qstack-future-is-bright/, now https://www.qstack.com.

| | |
|---|---|
| some comparisons of other services covered by an SLA (available as a word document with the "Terms of Service" governing 23 different cloud services). | Europe, South America, North America |
| OVH<br>France-headquartered<br>https://www.ovh.co.uk/dedicated-cloud/sla.xml | IaaS and web hosting. Regions: Europe, South America, North America, Africa |

Our analysis shows that the length of the SLA can be a double-edged sword. Clearly, the perception of SLAs change from CSC to CSC 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 the caveats with numbers that might have little meaning 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 format for the average CSC with an easy explanation of the issues, may not provide a clear definition for all terms discussed. An SLA should be a transparent document, easily understandable by the prospective CSC, especially small firms with few resources, and clearly covering all aspects of the Cloud service.

Other related issues that seem more important from an SME CSC perspective are:

- The different formats used to convey the SLA, ranging from plain web texts, web texts with expandable boxes, word documents, and PDFs. Where multiple documents or links are provided, it is hard to know which one(s) apply.
- While an SLA is a particle in the Cloud service level ecosystem, it is inseparable from the other contractual arrangements between the CSP and its CSC. It is therefore up to the CSC to ensure full understanding of the contractual arrangements and check for any changes therein, which are always made at the discretion of the CSP. Related-SLA terms are often scattered over multiple web pages/documents, which the SME CSC has to carefully consider. In cases where a dedicated section for SLA documents is not available on the CSP public website, prospective CSCs are referred sections dealing with legal and privacy terms of the service usage. Moreover, 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.

For example:

"*This Service Level Agreement forms part of your Agreement with* X CSP*, along with the Terms of Service and the Acceptable Use Policy, and is subject to all the terms and conditions stated in these documents".*

***SLA Support***

One of the biggest changes since our first sociological analysis (D2.1) is the increased attention CSPs are paying to customer support. The offer of 24/7 support is a differentiator used by leading CSPs with AWS leading the trend. CPSs like CloudSigma are also now offering a similar service. In most cases, the free trial is a core part of the marketing message.

It is however, important to note that this **support applies exclusively to the operational phase of the lifecycle**. The only support in the earlier phases is a free trial, at which point the CSP may have already "locked in" its CSC.

The table below compares different CSP customer support offers.

**Table 5. CSP Free Trials and Customer Support**

| Free trial and Customer Support |
|---|
| **AWS**: The AWS Free Tier is available for 12 months: http://aws.amazon.com/free/. 24/7 x 365 customer support based on a 4-tier approach (features, pricing, resources, intended use & restrictions): https://aws.amazon.com/premiumsupport/ |
| **CloudSigma**: Free 7-day trial. Free 24/7 support available through a live-chat on the website. |
| **Flexiant**: Free Trial. Support plans are based on different packages, conditions and costs, e.g. standard, premium, and premium plus, 24/7 x 365 UK-based support. No free trial. http://www.flexiscale.com/support/support-plans/ |
| **Microsoft Azure**: Free Trial, a 1 one-month trial for any new customer with €170-worth of credits: https://azure.microsoft.com/en-us/offers/ms-azr-0044p/ Options for technical and billing support: https://azure.microsoft.com/en-us/support/options/ |
| **OVH:** Support available Monday-Friday 9am-6pm (by phone). Web-based support: https://www.ovh.co.uk/community/ https://www.ovh.co.uk/support/ |

***SLA Negotiation***

While some organisations, such as large companies, governments and large public administrations have the bargaining power to negotiate a cloud contract, small organisations (e.g. micro firms, mid-sized firms and small public administrations) are typically offered "take-it-or-leave-it" contracts (sometimes also referred to as "out-of-the-box" or "cookie cutter version"). This seems to be one of the biggest barriers to cloud

service adoption, irrespective of any compelling marketing campaigns on the part of the CSC.

We have sourced the following examples from real CSPs related to these aspects.

> *"To the Service Offerings. We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings".*

Very few of the CSPs analysed give advanced warnings of changes to the Agreement. For example:

> *"We reserve the right and entitlement to alter the Agreement at any time. We will notify you in accordance with the Agreement at least thirty (30) days prior to any alterations becoming valid and binding."*

The need for companies to protect their business from potential legal disputes or liability for potential losses and damages makes the life of the CSC harder in clearly identifying and extracting the relevant elements of the Service Level Agreements, then comparing them across different offers.

One of the IaaS CSPs analysed makes an explicit reference to seeking legal advice. For example:

> *"If you do not accept any element of the Agreement you must not take up any of the Services offered by the Website. The Agreement imposes significant legal obligations on you and also places limits on your legal rights.* ***Please seek independent legal advice before entering into the Agreement****."*

The need for companies to protect their business from potential legal disputes or liability for potential losses and damages makes the life of the SME CSC harder in clearly identifying and extracting the relevant elements of the Service Level Agreements, then comparing them across different offers.

Another of the IaaS CSPs analysed makes an explicit reference to seeking legal advice. For example:

> *If you do not accept any element of the Agreement you must not take up any of the Services offered by the Website. The Agreement imposes significant legal obligations on you and also places limits on your legal rights.* ***Please seek independent legal advice before entering into the Agreement****.*

Termination is one of the lifecycle phases that should be clearly understood before entering into a contractual agreement. However, for an SME CSC, clauses dealing with termination are particularly complex, and, like many of the other components in the life-cycle, require the SME CSC to know where his/her rights and obligations lie.

One example of termination regards data deletion while implying vendor lock-in:

> *"We may terminate the Agreement without notice to you and without providing any refund against your Credit Balance if any of the following occurs: you do not use your account for a continuous period of three (3) months or more; your Credit Balance is zero (or negative) and you do not purchase any additional Credits within five (5) Working Days. In which case we shall additionally be entitled to immediately delete all data and information previously supplied as part of the Services and in relation to your account."*

Another example assumes the CSC is already familiar with CSP practices, such as data retrieval:

> *"We will provide you with the same post-termination data retrieval assistance that we generally make available to all customers."*

While yet another example indicates the obligations of the CSC with regard to back-up, including any related costs:

> *"You will not have access to your data stored on the Services during a suspension or following termination."*
>
> *"You have the option to create a snapshot or backup of your Cloud Servers or Databases, respectively, however, it is your responsibility to initiate the snapshot or backup and test your backup to determine the quality and success of your backups. You will be charged for your use of backup services as listed in your Order."*

### 3.6.1. Performance, Security and Personal Data Protection

The table below considers the most relevant SLOs from the C-SIG Guidelines from a sociological perspective, for the performance, security and personal data protection perspective alongside openness and transparency.

**Table 6. 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.<br><br>In terms of the sociological analysis, risks assumed by the Cloud customer (perceived or real) are a major aspect. Lack of understanding, expertise and skills can impede a proper risk assessment on the part of many SME CSCs. 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 CSC 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.<br><br>Relevant SLOs include applicable data protection codes of conduct, standards and certifications.<br><br>The sociological analysis looks at (i) understanding; (ii) acceptance and (iii) actions taken to ensure compliance on the part of the Cloud service customer.<br><br>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. |

***Performance metrics***

In the SLAs we analysed, the uptime or availability of the service is the only term present in all documents. Since our first sociological analysis, we have noted some changes to this, with CSPs increasing the levels of availability (from 99.95% to 99.99% and in one case 100%).

It is important to highlight that from a CSC perspective this guarantee should be analysed based on the type of service it applies, and most importantly to the type of business the service is essential. Otherwise it can be meaningless. Again, we are dealing with a lack of clarity for the SME CSC, but also for other types of organisations.

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.

As stated in [83] by Michael Allen (Solutions VP, Dynatrace): 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.

***Security and Privacy***

One thing that has not changed since our first analysis is the large gap for security and privacy terms in SLAs. Security is typically 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 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. Until the adoption of the European Data Protection regulation, the Acceptable User Policies continues to regulate all information the CSC gives the CSP, even for accessing services. The impact of the EU regulations remains to be seen. For now, the lack of flexibility and security features CSPs could guarantee is a barrier towards the trust on Cloud services.

According to the 451 Research take [83]: 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.

### 3.6.2. Service Credits

Most CSPs reserve the right to change prices at any time, and leave it up to the CSC to monitor any changes that may take place. For example:

> *"We reserve the right to change our prices at any time. Definitive pricing is available through the control panel at the time of purchase, and supersedes any information given here. Special offers may be subject to additional conditions. All prices are exclusive of VAT which will be added at the applicable rate. All services are offered subject to our terms and conditions."*

The typical financial compensation offered for not meeting SLAs is close to nothing. A credit service is the only way to make a claim and the terms and conditions are set by the CSP. There is no money credit and the CSC is tied to the CSP when obtaining compensation. For example:

> *"In order for* CSP X *to consider a Claim, Customer must submit the Claim to Customer Support within two months of the end of the billing month in which the Incident that is subject of the Claim occurs. Customer must provide to Customer Support all information necessary for* CSP X *to validate the Claim, including but not limited to detailed descriptions of the incident, the time and duration of the Incident, the affected resources or operations, and any attempts made by Customer to resolve the Incident."*
>
> *"We will be the sole arbiter regarding the award of credit and our decision will be final and binding."*

Gartner has also highlighted several issues related to monitoring costs and reduced benefits such as flexibility and cost savings. CSCs that are not be up-to-speed on how to monitor the cost of the cloud services risk incurring costs that had not anticipated. Gartner has reported on one CSC case where billing was unexpectedly high without the company concerned knowing if the bill was accurate or how the costs had been incurred [86]. The case shows that handing over IT operations to a third party presents difficulties in knowing how to use the new service and the need to manage costs properly.

Gartner sees is also as a symptom of the growing popularity of cloud services, but also points out a number of mistakes made by the CSC, such as not budgeting for several IT projects it had started; it did not shut down cloud instances that were not needed; and it did not adequately monitor the cloud services it was using. However, CSPs could also do

more to facilitate the CSC in understanding the bill, where every transaction or service (e.g. data transfers, storage, alerts) gets a line, by highlighting tools they offer, and by making sure the CSC has set up alerts if it overspends.

To overcome similar problems, Gartner advises CSCs to use the following strategy for managing and tracking the cost of cloud-based services. **Tagging resources** so CSCs can query or organise items using the tags as filters (most CSPs support tagging but tags are not set by default). **Creating a forecast** to help track the cost of the services (most CPSs have a cost calculator but this tool is only as accurate as the data the CSC provides and many CSCs may not know how many resources they will consume). **Optimising cloud use** by picking the right instance type and turn off instances not using and not returning value to the business.

While there are many tools on the market, not all of them work across different CPSs. Because we do not know what CSPs will use in the future, CSCs are advised to plan for solutions that help expand its cloud journey.

### 3.6.3. Market Forces and CSP Behaviour

Leading cloud providers are marketing powerhouses with clear and compelling marketing messages, and examples of users. They also offer free trials and 24/7 support. Users cited typically come from large organisations, both large companies and public administrations/authorities (usually presented with logos but also through a testimonial).

The biggest "shock" comes when prospective CSCs move to the second level – the SLA.

In this section, we analyse the overall behaviour of CSPs in the light of our updated analysis, with particular reference to CSP pricing practices and related sociological barriers. We also look at practices regarding the implementation of standards and certifications. Both aspects are insights that SLA-Ready can share with prospective CSCs.

**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? This an aspect on which SLA-Ready needs to provide guidance on.

**Market structure and Cloud pricing models**: The Cloud service market is currently price driven [87]. 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.

Work being done by the 451 Research through its Cloud Price Index (CPI) sheds key insights into the market forces behind the cloud pricing models. The CPI tracks the complex pricing models of both public and private clouds, analyses the total cost of ownership (TCO), and gives insights into the "golden ratios" that determine when private cloud and public cloud options become better options [88]. A 451 Report on the CPI published in July 2015 looks at where the real reductions are taking place and possible drivers behind them [85]. According to the report, cost reductions are taking place for compute, with a 4% price drop since October 2014. The author believes this is primarily a marketing ploy, with CSPs seeking headlines, publicity and market share in exchange for regular price cuts.

Little has changed in other cloud services, e.g., storage, managed services and support. In real terms, this means that margins are eroding on compute and the underlying cost base but CSPs still have a wide range of services on which they can derive new revenue and differentiate. CSCs can make greater savings by committing: best-case pricing has reduced 12% since last October. However, it is important that customers keep pace with the market price of the basics, and use them as a foundation to up-sell higher margin, value-added services. The overriding conclusion is that existing and prospective CSCs need neutral advice about cloud pricing.

**Standards and Certifications**

Trust in cloud computing and services is fundamental for increasing cloud adoption across the European Digital Single Market. The European Cloud Computing Strategy (2012), of which the C-SIG SLA work is part, aims to work towards a common understanding of best practices in Europe, for example, on security and data protection. A common understanding is needed to raise confidence and create trust for cloud adoption by

customers, businesses and public sector organisations, throughout all sectors of the economy.

Standards and security certification schemes play a key part in building trust, helping prospective customers to better compare cloud service offers also from a security point of view. The table below provides a sample of CSPs implementing standards and certifications identified during our second sociological analysis.

Trust is increasing in importance as more and more mission-critical workloads move to the cloud. It is vital that companies have confidence in the ability of their cloud service to support the needs of their business, while also providing value for money.

**Table 7. Standards and Certifications**

| CSP | Standard and/or Certification |
|---|---|
| Memset Hosting | ISO 27001:2013 Information Security Management System; ISO 14001:2004 Environmental Management System[7]. |
| Microsoft Azure (Virtual Machines) | ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, country-specific standards (e.g. Australia IRAP, UK G-Cloud and Singapore MTCS; ISO/IEC 27018[8]. |
| OVH | PCI DSS Certification, ISO/IEC 27001 certification SOC 1 Type II and SOC 2 Type II certifications, STAR self-assessment - Cloud Security Alliance[9] |
| Amazon | ISO 27018 [89]<br>Give credibility to service providers who want to protect their data by demonstrating that they follow internationally recognised guidelines.<br>27018 sets out what's meant by "personally identifiable information" (PII) and what should happen to it.<br>Under the terms of it, PII is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) might be directly or indirectly linked to a PII principal.<br>Nothing changes in terms of the CSC responsibilities. It is also important to note that ISO27018 is not a certifiable standards. No company can claim to be ISO27018 certifications and given the current approach used in ISO27001/2 there would be no way for a data controller (cloud customer) to verify whether e.g. Amazon (or any other provider) has really implemented the controls in 27018 and in which way those controls where implemented. This also applies to 27017.<br>Art29 WP has also highlighted this to the EC Privacy Code of Conduct. |

[7] See http://www.memset.com/about-us/iso-certificates/.

[8] See https://azure.microsoft.com/en-gb/support/trust-center/compliance/.

[9] PCI DSS Certification, ISO/IEC 27001 certification SOC 1 Type II and SOC 2 Type II certifications, STAR self-assessment - Cloud Security Alliance, OVH, https://www.ovh.co.uk/aboutus/certifications.xml.

| CSP | Standard and/or Certification |
|---|---|
| Memset Hosting | ISO 27001:2013 Information Security Management System; ISO 14001:2004 Environmental Management System[10]. |
| Microsoft Azure (Virtual Machines) | ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, country-specific standards (e.g. Australia IRAP, UK G-Cloud and Singapore MTCS; ISO/IEC 27018[11]. |
| OVH | PCI DSS Certification, ISO/IEC 27001 certification SOC 1 Type II and SOC 2 Type II certifications, STAR self-assessment - Cloud Security Alliance[12] |
| Amazon | ISO 27018 [89]<br>Give credibility to service providers who want to protect their data by demonstrating that they follow internationally recognised guidelines.<br>27018 sets out what's meant by "personally identifiable information" (PII) and what should happen to it.<br>Under the terms of it, PII is any information that (a) can be used to identify the PII principal to whom such information relates, or (b) might be directly or indirectly linked to a PII principal.<br>Nothing changes in terms of the CSC responsibilities. It is also important to note that ISO27018 is not a certifiable standards. No company can claim to be ISO27018 certifications and given the current approach used in ISO27001/2 there would be no way for a data controller (cloud customer) to verify whether e.g. Amazon (or any other provider) has really implemented the controls in 27018 and in which way those controls where implemented. This also applies to 27017.<br>Art29 WP has also highlighted this to the EC Privacy Code of Conduct. |

### 3.6.4. Overall Conclusions of the Sociological Analysis

Leading cloud providers have clear and compelling marketing messages, and examples of users. Free trials are used to lure CSCs, while 24/7 support is being used to differentiate. CSPs are paying greater attention to customer support, possibly due to negative press reports. Most of the CSPs cited here are updating their respective websites to highlight customer support. However, such changes relate to actual usage of a service by a CSC rather than assisting new CSCs.

It is also interesting to note that user testimonials typically come from large organisations, both large companies and public administrations/authorities (usually

10 See http://www.memset.com/about-us/iso-certificates/.

11 See https://azure.microsoft.com/en-gb/support/trust-center/compliance/.

12 PCI DSS Certification, ISO/IEC 27001 certification SOC 1 Type II and SOC 2 Type II certifications, STAR self-assessment - Cloud Security Alliance, OVH, https://www.ovh.co.uk/aboutus/certifications.xml.

presented with logos but also through a testimonial), rather than the small business community.

Our sociological analysis confirms yet again that the biggest "shock" comes when prospective CSCs move to the SLA as the crucial user/CSP interface. Currently, CSPs are doing very little to lower the entry barrier for prospective SME CSCs. Instead, they are by and large playing to market forces. The average CSP has a long way to go before its SLAs are aligned with the needs of customers.

A Cloud SLA comes with a host of potential problems, which some prospective SME CSCs may perceive as risks not worth taking. Because Cloud SLAs have not yet evolved into an industry standard, there are no standardised terms or conditions for any type of cloud service. It is hard to identify SLA best practices aligned with the European Guidelines, which is probably as low as 10%.

Clearly, different cloud services come with different types of risks and opportunities, as well as roles and responsibilities for the CSP and CSC. However, the complexity of the terminology makes it hard for the prospective CSC to clearly understand exactly what risks he/she is taking and what addition actions are required. As a result, it may be difficult to weigh the risks against the benefits, and move towards a situation of shared responsibility where the respective roles are clearly understood.

There is an urgent need for greater clarification of roles and responsibilities, rights and obligations, especially from an SME CSC perspective. Our analysis fits with the findings of the Cloud Computing Survey 2015 by the UK Federation of Small Businesses [90]. Most of the 1226 small firms surveyed (733 using a cloud service; 470 not using a cloud service; 23 "don’t know") recognise the value of the cloud for their business. The firm see the following three risks as being most important:

- Risk data might get lost/stolen/damaged: 61%.
- Not being able to access online services when needed: 55%.
- Not knowing who could access the data: 52%.

Public Cloud providers might not offer adequate compensations in case of damages, like data loss or unauthorised 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 [91] 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, as indicated by the Cloud Industry Forum's Cloud Computing Surveys 2014 and 2015.
- More than 78% of users find it hard to trust how companies use their personal data [92], 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.

In conclusion, improved SLA metrics should not be reserved to the largest customers, but need to become the order of the day for all users along with ways to ensure they are enforced.

## 4. Summary of Elicited Requirements

This section presents the summary of the CRM requirements based on the CRM Requirements landscape from Sections 2 and 3. The initial set of CRM requirements is not intended for completeness, but more to elucidate the (a) Cloud SLA lifecycle, (b) the commonly used SLA components and other elements observed over security, privacy, legal, sociological and economic aspects, and (c) the basic categorization of SLA elements to highlight concepts versus market reality.

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, availability, 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 harder to associate economic contracts around them, even though our research show qualitative measurements of these are becoming so objective that some can be measured on an (almost) quantitative measures level. Such as for instance the OECD Guidelines on measuring subjective well being demonstrate to a certain extent.

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

- The set of surveyed SLOs clearly shows the need for standardised definitions and also for industrial feedback to empirically validate them. Most of the underlying SLO metrics (and in consequence also the SLOs) found that the state of the art has 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 CloudTrust WG, and the corresponding ad-hoc group within ISO/IEC SC38.
- The initial 22 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) organisations, 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 over €5 billion contractual 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 8. 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 the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **2** | Findable | Can the SLA easily be found on the CSP's website? (Reference is made to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **3** | Contact details | Does the CSP have a support desk or other contact details to contact? (Reference is made to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **4** | Contact availability | What is the availability of the support desk of the CSP?(Reference is made to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **5** | Number of pages | How many pages does the SLA consist of? (Reference is made to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **6** | SLA language | Is the SLA offered in more than one language? (Reference is made to the legal analysis of Section 3.4) |
| **7** | Machine-readable format | Does the CSP also offer a machine-readable version of its SLA? (Reference is made to the legal analysis of Section 3.4) |
| **8** | Revision date | What is the date of the last revision? (Reference is made to the analysis of SLA components of Section 3.3) |

| | | |
|---|---|---|
| **9** | Update frequency | Is the SLA updated regularly? (Reference is made to the analysis of SLA components of Section 3.3 and to the legal analysis of Section 3.4) |
| **10** | Previous versions and revisions | Are the previous versions of the SLA available and is there transparency on revisions made? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **11** | SLA duration | What is the duration/term of the SLA? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **12** | Unilateral change | Can the CSP change the SLA unilaterally? (Reference is made to the analysis of SLA components of Section 3.3, to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **13** | SLA change notifications | Does the CSP provide SLA change notifications? (Reference is made to the analysis of SLA components of Section 3.3, to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **14** | SLA transparency | Does the SLA provide transparency on its components? (Reference is made to the legal analysis of Section 3.4 and to the sociological analysis of Section 3.6) |
| **15** | SLA reporting | Does the CSP provide reports about the SLA performance? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **16** | SLA continuous reporting | Are the CSP reports updated continuously? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **17** | Service credit | Does the CSP provide service credits? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3, to the legal analysis of Section 3.4, to the economic analysis of Section 3.5 and to the |

| | | |
|---|---|---|
| | | sociological analysis of Section 3.6) |
| **18** | How are service credits assigned | Who determines whether a service credit shall be provided? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3, to the legal analysis of Section 3.4, to the economic analysis of Section 3.5 and to the sociological analysis of Section 3.6) |
| **19** | Maximum service credits | How much does the CSP credit? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3,and to the economic analysis of Section 3.5) |
| **20** | General carve-outs | What are the assumptions, exclusions, scope of force majeure, and other carve outs to the Cloud services, SLOs and SLA? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **21** | Choice of law | Which choice of law is included in the SLA? (Reference is made to Sections (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **22** | Possibility of specials and other customisations | Are there "specials" and other customisations possible (as far as we know)? (Reference is made to the analysis of SLA components of Section 3.2 and 3.3 and to the legal analysis of Section 3.4) |
| **23** | Performance SLOs | These relate to the SLO aspects of, for example, availability and capacity. (Reference is made to the analysis of SLA components of Section 3.2, and to the sociological analysis of Section 3.6) |
| **24** | Security SLOs | This requirement comprehends SLOs related to cryptography, authentication and other aspects derived from relevant security control frameworks. (Reference is made to the analysis of SLA components of Section 3.3, and to the sociological analysis of Section 3.6) |

| | | |
|---|---|---|
| **25** | Data Management SLOs | These SLOs related to the measurable description of the CSP's data life-cycle's commitments. (Reference is made to the analysis of SLA components of Section 3.3, and to the sociological analysis of Section 3.6) |
| **26** | Personal Data Protection SLO | This SLO category includes those related to accountability and codes of conduct. (Reference is made to the analysis of SLA components of Section 3.3) |

The first 22 requirements in Table 4 are important to take into account and consideration, even though these for obvious reasons were 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 23 – 26 (cf. Table 4).

## 5. SLA Repository Requirements

This section provides an update on the Cloud SLA Repository's development, which will be one of the major outcomes from SLA-Ready targeting trust and transparency of Cloud SLAs. The SLA Repository is more than just a collection the Cloud SLAs, but it actually reports a comprehensive analysis of these based on an assessment criteria leveraging SLA-Ready's CRM. As presented later in this section, the proposed assessment criteria directly map to the requirements elicited in Section 4.

During the duration of the project the SLA Repository will be made available through different channels and with different access restrictions, just as presented in the following timeline:

Table 9. SLA Repository – release timeline

| Planned release date | Deployment channel | Access Restrictions | Comments |
|---|---|---|---|
| **Q4/2015** | Live document – assessments by SLA-Ready consortium | Only to members of the consortium | Initial version featuring the list of CSPs to analyse and the assessment criteria. Only updated by consortium. |
| **Q2/2016** | Live document – CSP validation | Only to members of the consortium and assessed CSP | This version of the SLA Repository contains assessment data validated by the CSPs |
| **Q4/2016** | SLA-Ready Marketplace | Publicly available (read-only) | During this stage the SLA-Repository is made available through the project's Marketplace (please refer to Deliverable 4.2). |
| **Q4/2016** | CSA STAR Registry | Publicly available (read-only) | Summarized CSP SLA information of at least 20 providers is extracted from the SLA Repository, and made available through the CSA STAR Registry [26]. |

Figure 4 shows a high-level view of the process followed by SLA-Ready to gather (Step 1), assess (Step 2), validate (Step 3) and deploy (Step 4 and 5) the Cloud SLAs through the different channels referenced in Table 9.

The rest of 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, and the general requirements associated to its deployment in the channels presented in Table 9. The actual design of the SLA-Repository will be presented in Deliverable 2.3.

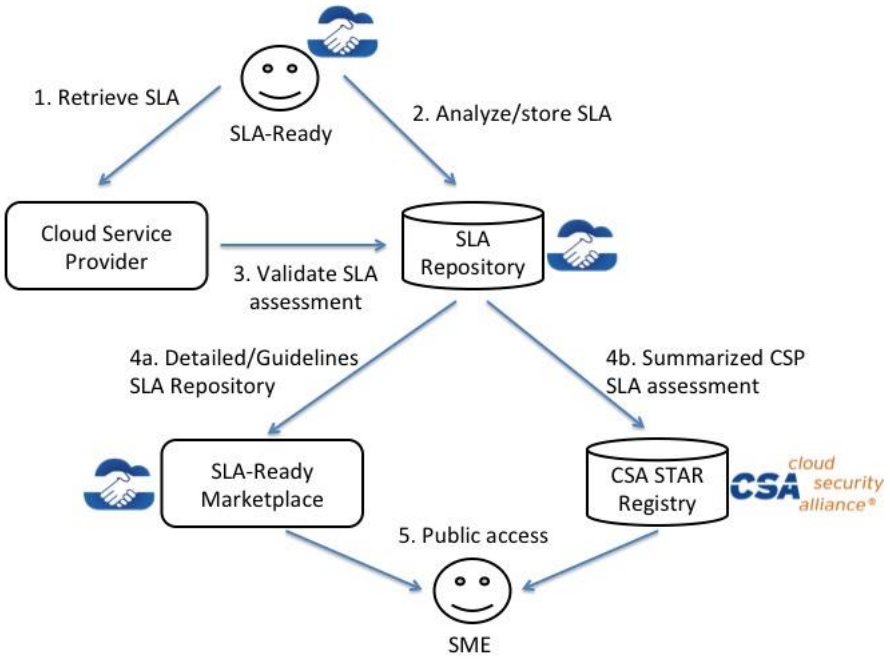



Figure 4. Deployment requirements for the SLA-Repository.

## 5.1. Cloud Service Providers to analyse

The initial version of SLA-Ready's SLA repository will gather and analyse the Cloud SLAs from the CSPs listed on the CSA STAR Registry (currently 139), which are shown in Annex 3. The rationale behind this decision is that fact that those CSPs are already engaged and committed to CSA's activities related to trust and transparency, in particular by having achieved CSA STAR Level 1 (self-assessment[26]). SLA-Ready (through WP4) has started to create synergies with those CSPs in order to facilitate the upcoming validation of the SLA assessments performed by the consortium.

## 5.2. Assessment and Validation Criteria

As mentioned early in this section, the SLA 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 can be used to create awareness in SMEs willing to exploit the full benefits of Cloud computing. For this reason, the compiled SLAs will be analysed based on an assessment criteria leveraging the CRM requirements elicited in Sections 3

and 4. In order to develop the referred repository of SLAs and related documentation, the varied CSP information needs to be structured according to the CRM. This includes the CSP general information, 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.

The assessment criteria will be structured as a set of questions resembling the CSA Common Assurance Questionnaire (CAIQ [94]), foundation of the STAR Registry. The goal of each question will be to guide assessors (either members of the consortium of participant CSPs), in providing concrete and neutral answers related to the SLA under analysis. The consortium acknowledges the fact that it is not possible to avoid some degree of subjectivity while analysing an SLA, however our expectation is to minimise it by providing a double evaluation (consortium assessment and CSP validation) of each analysed SLA. In cases where these double assessments show a high level of discrepancy between them, then SLA-Ready will engage on a dialog with the CSP in order to solve the potential issues that have appeared.

The answer to each assessment question will be mapped to concrete values (e.g., Yes/No, True/False, intervals, ratios, and so forth), in order to facilitate the extraction of information that allows performing operations like CSP comparisons. Some of these operations can be automatized in order to facilitate the integration with e.g., the CSA STAR Registry (cf., Deliverable 4.2).

### 5.3. Deployment Channels and Accessibility

The SLA Repository will be deployed in the three different channels mentioned in Table 9:

- Live document: SLA-Ready will start developing the SLA Repository based on a live document, shared only among members of the consortium, where raw data related to CSPs is compiled and analysed based on the criteria described in Section 5.2. As previously mentioned, this draft version of the repository aims to provide an initial assessment meant to be validated by the corresponding CSPs before its publication (Marketplace/CSA STAR).
- SLA-Ready Marketplace: SLA-Ready's Marketplace is the main entry point to the project's outcomes including CRM, best practices, tutorials, and SLA Repository. With respect to the latter, the Marketplace will provide detailed information related to its design and content along with SME-friendly guidelines to exploit the provided data (e.g., to compare CSPs side-by-side). The SLA data available on the Marketplace's version of the SLA Repository should have been previously

validated by the corresponding CSP. Deliverable 4.2 presents more details related to the design of the Marketplace.

- CSA STAR Registry: this is a public website where CSPs are invited to publish their answers to standardized set of security and privacy related questions (CAIQ). This provides Cloud customers with an overview of a CSP's security and privacy posture. This public repository contains data related to public CSPs worldwide. Available STAR information is presented according to self-assessment reports based on the security controls proposed by CSA Cloud Control Matrix [34] (CSA CCM) and third-party assessment summaries also based on the CSA CCM. Another reason why we are initially leveraging the CSA STAR Registry 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. In order to keep the user-friendliness associated to STAR it is not required to show all the detailed CSP SLA information/analysis, but only a comprehensive/easy-to-understand metric related to the SLA's degree of compliance with the CRM. Cloud customers willing to obtain detailed information related to any of the CSP SLAs included on CSA STAR will be referenced to the SLA-Ready Marketplace. Deliverable 4.2 will further detail the integration activities related to CSA STAR.

There is a potential legal barrier to publication of the SLA Repository. 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 is 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 presents the final requirements for the creation of the 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 review resulted on the elicitation of several requirements that will be used to guide the subsequent work in WP2, in particular the CRM design to take place in D2.3 and D2.4.

This deliverable also reported about the design and content (including a list of CSPs to consider -see Annex 3-) 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 analyse 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 and WP4 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 analyse the SLAs comprising the repository, in order to start the identification of gaps and best-practices.

The outcomes of this deliverable are the basis for the CRM created in D2.3 and D2.4.

## 7. References

[1] European Commission, *Cloud Service Level Agreement Standardisation Guidelines (C-SIG SLA 2014)*. Brussels, 2014.

[2] R. Wies, "Policy Definition and Classification: Aspects, Criteria and Examples," In Proceedings of the IFIP/IEEE International Workshop on Distributed Systems: Operation and Management, 1994, pp. 10-12.

[3] T. Koch, C. Krell, and B. Krämer, "Policy definition language for automated management of distributed systems," In Proceedings of Second IEEE International Workshop on Systems Management, 1996, pp. 55-64.

[4] National Institute of Standards and Technology, *Guide for developing security plans for federal information systems, vol. 800-18*. Gaithersburg, MD: US Dept. of Commerce, 2006.

[5] K. Høstland, P. A. Enstad, Ø. Eilertsen and, Gunnar Bøe. "Information Security Policy. Best Practice Document," UNINETT led working group on security (No UFS126). 2010.

[6] AW. Kadam, "Information security policy development and implementation," *Journal Information Systems Security*, vol. 16, no. 5, pp. 246-256, 2007.

[7] A. Kannammal and N.Ch.S.N. Iyengar, "A model for mobile agent security in e-business applications," *International Journal of Business and Information*, vol. 2, no. 2, pp. 185-198, 2007.

[8] C. Bronk, "Hacking the nation-state: security, information technology and policies of assurance," *Information Security Journal: A Global Perspective*, vol. 17, no. 3, pp. 132-142, 2008.

[9] A. Benjamin, et al., "Controlling usage in business process workflows through fine-grained security policies," *Springer Trust, Privacy and Security in Digital Business*, vol. 5185, pp. 100-117, 2008.

[10] I. Aktug and K. Naliuka, "ConSpec: A Formal Language for Policy Specification," In Run Time Enforcement for Mobile and Distributed Systems (REM'07), 2007.

[11] F. Martinelli and I. Matteucci, "Idea: Action Refinement for Security Properties Enforcement," In Proc. of Engineering Secure Software and Systems, (ESSoS), 2009, pp. 37-42.

[12] L. Karadsheh and S. Alhawari, "Applying security policies in small business utilising cloud computing technologies," *International Journal of Cloud Applications and Computing*, vol. 1, no 2, pp. 29-40, 2012.

[13] M. Whitman and H. Mattord, "*Principles of information security*," 3rd ed. Course Technology, Boston, 2009.

[14] National Institute of Standards and Technology, U.S. Department of Commerce, M. Swanson and B. Guttman, "Generally accepted principles and practices for securing information technology systems," 1996.

[15] H. Ludwig, A. Keller, A. Dan, R.P. King, and R. Franck, "Web Service Level Agreement (WSLA) Language Specification," Tech. Report wsla-2003/01/28, IBM, 2003.

[16] K. Andrieux, A. Czajkowski, K. Dan, H. Keahey, T. Ludwig, J. Nakata, J. Pruyne, S. Rofrano, M. Tuecke, and M. Xu, "Web Services Agreement Specification (WS-Agreement)," Open Grid Forum, 2007.

[17] R. Henning, "Security Service Level Agreement: Quantifiable Security for the Enterprise?," In Proc. of the New Security Paradigms Workshop (NSPW 1999), 1999.

[18] The SPECS Project. 2013 [Online] Available: http://www.specs-fp7.eu/ [Accessed: Sept. 15, 2015]

[19] J. Luna, R. Langenberg, N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," ACM Workshop on Cloud computing security workshop, pp. 103-112, 2012.

[20] B. Monahan and M. Yearworth, "Meaningful Security SLAs," Technical Report. HP Laboratories, 2008.

[21] A. Undheim, K. Bernsmed, and M.G. Jaatun, "Security in Service Level Agreements for Cloud Computing". 1st International Conference on Cloud Computing and Services Science, pp. 636-642, 2011.

[22] G. Frankova and A. Yautsiukhin, "Service and protection level agreements for business processes," In The 2nd European Young Researchers Workshop on Service Oriented Computing, 2007.

[23] T. Feglar, "ITIL Based Service Level Management if SLAs Cover Security," *Journal of Systemics, Cybernetics and Informatics*, vol. 3, no. 4, pp. 61-71, 2003.

[24] M. Dekker and G. Hogben. "Survey and analysis of security parameters in cloud SLAs across the European public sector". Tech. Report TR-2011-12-19, European Network and Information Security Agency, 2011.

[25] K. Bernsmed, M.G. Jaatun, P.H. Meland, A. Undheim, "Security SLAs for Federated Cloud Services," In Proc. of the 6th International Conference on Availability, Reliability, and Security (ARES 2011), 2011.

[26] Cloud Security Alliance. "The Security, Trust & Assurance Registry (STAR)," [Online] Available: https://cloudsecurityalliance.org/star/, 2011, [Accessed Sept. 15, 2015]

[27] J. Zhengwei et al. "A Meta-Synthesis Approach for Cloud Service Provider

Selection Based on SecSLA," Fifth International Conference on Computational and Information Sciences (ICCIS), 2013, pp. 1356 – 1360.

[28] A. Schilling, "A Quantitative Threat Modelling Approach to Maximize the Return on Security Investment in Cloud Computing," in Proceedings of the 1st International Conference on Cloud Security Management (ICCSM'13), 2013, pp. 68-78

[29] V. Casola, et.al. "A SLA evaluation methodology in Service Oriented Architectures,"*Quality of Protection of Springer Advances in Information Security*, vol. 23, pp. 119 – 130, 2006.

[30] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A security Metrics Framework for the Cloud," in Proc. of the 6th International Conference on Security and Cryptography (SECRYPT 2011), 2011, pp. 245-250.

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

[32] L. Krautsevich, F. Martinelli, and A. Yautsiukhin. "Formal analysis of security metrics and risk," in Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, pp. 304-319, 2011.

[33] R.M. Savola, "On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems," in *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 10, no. 1, pp. 230-239, 2010.

[34] Cloud Security Alliance. "The Consensus Assessments Initiative Questionnaire". [Online] Available: https://cloudsecurityalliance.org/research/cai/, 2011. [Accessed Sept. 15, 2015]

[35] J. Luna, et.al. "Quantitative Assessment of Cloud Security Level Agreements: A Case Study,". In Proc. of Security and Cryptography, pp. 64-73, 2012.

[36] FP7 SLO@SOI Project. [Online] Available: http://sla-at-soi.eu/, 2011 [Accessed Sept. 15, 2015]

[37] FP7 Contrail Project. [Online] Available: http://contrail-project.eu/, 2013 [Accessed Sept. 15, 2015]

[38] FP7 Optimis Project. [Online] Available: http://www.optimis-project.eu, 2014. [Accessed Sept. 15, 2015]

[39] FP7 4CaaSt project. [Online] Available: http://www.4caast.eu/, 2014. [Accessed Sept. 15, 2015]

[40] P. Trimintzios, "Measurement Frameworks and Metrics for Resilient Networks and Services," European Network and Information Security Agency (ENISA), Technical report, 2011.

[41] "The CIS security metrics V1.1.0.". Center for Internet Security (CIS), Technical Report, 2010.

[42] W. Jansen, "Directions in security metrics research." National Institute of Standards and Technology (NIST), DIANE Publishing, U.S. 2010.

[43] N. Idika and B. Bhargava, "Extending Attack Graph-Based Security Metrics and Aggregating Their Application," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 9, n. 1, pp. 75-85, 2012.

[44] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz and R. Cunningham, "Validating and Restoring Defense in Depth Using Attack Graph," in Proc. of Military Communications Conference (MILCOMM 2006), 2006, pp. 1-10.

[45] R. Ortalo, Y. Deswarte and M. Kaâniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security," *IEEE Transactions on Software Engineering (TSE)*, vol. 25, n.5, pp. 633-650, 1999

[46] J. Pamula, S. Jajodia, P. Ammann and V. Swarup, "A weakest-adversary security metric for network configuration," in Proc. of the 2nd ACM Workshop on Quality of Protection (QOP 2006), 2006, pp. 31-38.

[47] P.K. Manadhata and J.M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering (TSE)*, vol. 37, no. 3, pp. 371-386, 2011

[48] J.A. Wang, H. Wang, M. Guo and M. Xia, "Security Metrics for Software Systems," in Proc. of the 47th ACM Southeast Conference (ACMSE 2009), 2009.

[49] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: Comparing public cloud providers," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2010, pp. 1–14.

[50] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for comparing and ranking cloud services," J. Future Generation Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[51] J. Siegel and J. Perdue, "Cloud services measures for global use: The service measurement index," in Proc. Annu. SRII Global. Conf., 2012, pp. 411–415.

[52] M. Almorsy, J. Grundy, and A. Ibrahim, "Collaboration-based cloud computing security management framework," in Proc. IEEE Int. Conf. Cloud Comput., 2011, pp. 364–371.

[53] H. Ghani, A. Khelil, N. Suri, G. Csertan, L. Gonczy, G. Urbanics, and J. Clarke, "Assessing the Security of Internet Connected Critical Infrastructures (The CoMiFin Project Approach)," in Proc. of the 1st Workshop on the Security of the Internet of Things (SecIoT 2010), 2010.

[54] J. Breier and L. Hudec, "Risk Analysis Supported by Information Security Metrics,". In Proc. of the 12th International Conference on Computer Systems and

Technologies (CompSysTech 2011), 2011, pp. 393-398.

[55] P. Trimintzios, "Measurement Frameworks and Metrics for Resilient Networks and Services," European Network and Information Security Agency (ENISA), Technical report, 2011.

[56] F. Massacci and A. Yautsiukhin, "An algorithm for the appraisal of assurance indicators for complex business processes," in Proceedings of the 2007 ACM workshop on Quality of protection, 2007, pp. 22-27.

[57] K.E. Seamons, T. Chan, E. Child, M. Halcrow, A. Hess, J. Holt, J. Jacobson, R. Jarvis, A. Patty, B. Smith, T. Sundelin, and L. Yu, "TrustBuilder: negotiating trust in dynamic coalitions," in Proceedings DARPA Information Survivability Conference and Exposition, 2003, pp. 49–51.

[58] B. Smith, K.E. Seamons, and M.D. Jones, "Responding to policies at runtime in TrustBuilder," in IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04), 2004, pp. 149–158.

[59] A. Beautement, R. Coles, J. Griffin, B. Monahan, D. Pym, M.A. Sasse and M. Wonham, "Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security," Workshop on Economics in Information Security. 2008, pp. 141-163.

[60] R. Coles, J. Griffin, H. Johnson, B. Monahan, S. Parkin, D. Pym, A. Sasse, and A. van Moorsel, "Trust Economics Feasibility Study," in Workshop on Resilience Assessment and Dependability Benchmarking, IEEE Computer Press, 2008.

[61] E. LeMay, M.D. Ford, K. Keefe, W.H. Sanders and C. Muehrcke, "Model-based Security Metrics using ADversary VIew Security Evaluation (ADVISE)," in Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems (QEST 2011), 2011, pp. 191-200.

[62] A. Keller and H. Ludwig. "The WSLA framework: Specifying and monitoring service level agreements for web services," *Journal of Network and Systems Management*, vol. 11, no. 1 pp. 57-81, 2003.

[63] D. Snelling, A. Ali, F. Wray, A. Basermann, M. Fisher, M. Surridge, and P. Wieder, "NextGRID Architectural Concepts," In Towards Next Generation Grids, pp. 3-13, Springer US, 2007.

[64] F. Heine, M. Hovestadt, and O. Kao, "HPC4U: Providing highly predictable and SLA-aware clusters for the next generation grid," In 4th Cracow Grid Workshop, Cracow, Poland. 2004.

[65] E. Novikoff, "The role of remote monitoring in Cloud Computing", [Online], Available: http://enki.co/blog/the-role-of-remote-monitoring-in-cloud-computing.html. [Accessed Sept. 15, 2015]

[66] A. Grabner, "Proof of Concept: dynaTrace provides Cloud Service Monitoring and Root Cause Analysis for GigaSpaces", May 06, 2009, SYS-CON Media, Inc. [Online], Available: http://apmblog.dynatrace.com/2009/05/07/proof-of-concept-dynatrace-provides-cloud-service-monitoring-and-root-cause-analysis-for-gigaspaces/. [Accessed Sept. 15, 2015].

[67] Ganglia home page. [Online] Available: http://ganglia.sourceforge.net/. [Accessed Sept. 15, 2015].

[68] Nagios home page. [Online] Available http://www.nagios.org/. [Accessed Sept. 15, 2015].

[69] V. C. Emeakaroha, R. N. Calheiros, M. A. S. Netto, I. Brandic, and C. A. F. De Rose, "DeSVi: An Architecture for Detecting SLA Violations in Cloud Computing Infrastructures" 2nd Intl ICST Conference on Cloud Computing (CloudComp 2010), 2010.

[70] V. C. Emeakaroha, M. A. S. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. F. De Rose, "Towards autonomic detection of SLA violations in Cloud infrastructures," *Future Generation Comp. Syst*, vol. 28, no. 7, pp. 1017-1029, 2012.

[71] Amazon CloudWatch, [Online] Available: http://aws.amazon.com/cloudwatch/. [Accessed Jul. 15, 2015].

[72] mOSAIC, [Online] Available: http://www.mosaic-cloud.eu/. [Accessed Jul. 15, 2015].

[73] J. Brower, "The security Onion Cloud Client - Network Security Monitoring for the Cloud," The SANS Institute, Tech. Report, 2013.

[74] A. Lazarevic, V. Kumar, J. Srivastava. "Intrusion detection: a survey," *Managing cyber-threats: issues approaches & challenges*, Springer, pp. 19-78, 2005.

[75] G. Spanoudakis, K. Mahbub, "Non intrusive monitoring of service based systems," *Int. Journal of Cooperative Inform. Systems*, vol. 15, no. 3, pp. 325-358, 2006.

[76] A. Valdes and K. Skinner Adaptive, "Model-based Monitoring for Cyber Attack Detection," *Recent Advances in Intrusion Detection*, pp. 80-92, 2000.

[77] S. Clayman et al., "Monitoring Service Clouds in the Future Internet," *In Towards the Future Internet - Emerging Trends from European Research,* G. Tselentis et al. IOS Press: Amsterdam, The Netherlands, 2010. pp. 115 – 126.

[78] H. Foster, G. Spanoudakis, "SMaRT: A Workbench for Reporting the Monitorability of Services from SLAs,", 3rd International Workshop on Principles of Engineering of Service-Oriented Systems, 2011, pp. 36-42.

[79] H. Foster, G. Spanoudakis, "Advanced Service Monitoring Configurations with SLA Decomposition and Selection," 26th ACM Symposium Applied Computing – Track on Service Oriented Architecture and Programming, 2011, pp. 1582-1589.

[80] W. Gilani et al., "SLA-aware Service Management, " Deliverable DA3.a, M38, FP7 SLA@SOI Project, 2011.

[81] N. Kroes, "Cyber Security – A shared responsibility," Information Security Forum Conference, Chicago. 2004. [Online] Available: https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility [Accessed Jul. 15, 2015].

[82] CSA Cloud Trust Protocol. [Online] Available: https://cloudsecurityalliance.org/research/ctp/, 2011. [Accessed Jul. 25, 2015]

[83] B. Sullivan. "Why Your Cloud SLA Could Be the Most Important Contract You Ever Sign," Tech Week Europe Newsletter. 2015. [Online] Available: http://www.techweekeurope.co.uk/cloud/cloud-management/cloud-provider-sla-2015-159831, [Accessed Jul. 15, 2015].

[84] M. Dekker and D. Livery "Cloud Security Guide for SMEs". European Network and Information Security Agency, Tech. Report, 2015.

[85] O. Rogers, 451 Research Analyst, "Does a cloud price war risk providers' profits?," 451 Research Analyst. [Online] Available. https://451research.com/report-short?entityId=85987, 2015.

[86] J. Sparapani, "Track the cost of cloud-based services with better financial management". TechTarget. SearchCIO. [Online] Available: http://searchcio.techtarget.com/tip/Track-the-cost-of-cloud-based-services-and-dont-fear-your-next-bill, [Accessed Jul. 15, 2015].

[87] B. Darrow, "Which cloud company is next on the auction block?,". Fortune. 2015. [Online] Available: http://fortune.com/2015/05/26/which-cloud-company-is-next-to-go/, [Accessed Jul. 15, 2015].

[88] Cloud Price Index, 451 Research, 2015, [Online] Available: https://451research.com/images/Marketing/productsheets/451_Research_CPI_US_PUB_11_15_2015.pdf, [Accessed Jul. 15, 2015].

[89] M. Cooter, "Why the cloud provider community needs to get on board with ISO 27018," ComputerWeelkly, 2015, [Online] Available: http://www.computerweekly.com/feature/Why-the-cloud-provider-community-needs-to-get-on-board-with-ISO-27018?utm_medium=EM&asrc=EM_MDN_49646770&utm_campaign=20151109_AWS%20to%20open%20UK%20datacentre%20in%20late%202016_&utm_source=MDN [Accessed Jul. 15, 2015].

[90] Cloud computing survey, Federation of Small Business, 2014, [Online] Available: http://www.fsb.org.uk/LegacySitePath/policy/assets/fsb%20cloud%20computing%20servey%20-%20february%202015.pdf. [Accessed Jul. 15, 2015].

[91] Cloud Security Alliance: Cloud Vulnerabilities Working Group, "Cloud Computing Vulnerability Incidents: A Statistical Overview," 2013, [Online] Available: https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/. [Accessed Jul. 15, 2015].

[92] Orange, "The future of digital trust: A European study on the nature of consumer trust and personal data," 2014. [Online] Available: http://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf. [Accessed Jul. 15, 2015].

[93] OECD Guidelines on Measuring Subjective Well-being, OECD Publishing, 2013, [Online] Available: http://www.oecd.org/statistics/Guidelines%20on%20Measuring%20Subjective%20Well-being.pdf, [Accessed Jul. 15, 2015].

[94] Cloud Security Alliance: Consensus Assessments Working Group, 2013, [Online] https://cloudsecurityalliance.org/group/consensus-assessments/, [Accessed Jul. 15, 2015].

## *Annex 1 References and Source Documents*

Table 10. 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. |

## *Annex 3 List of CSPs for the SLA Repository*

This annex presents the list of CSPs comprising the CSA STAR registry, which will be analysed in the context of the planned SLA Repository.

| | | | |
|---|---|---|---|
| Acer CyberCenter Services Inc. | Digital Sense Hosting | Netskope | SpringCM |
| Achievers Corporation | Dropbox, Inc. | New Century Inforcomm Tech Co., Ltd. | StarRez |
| Acquia | Dyn | New Relic | Symantec.cloud |
| Adallom | eagle.io | New World Telecommunications Limited | Tableau Software |
| Alibaba Cloud Computing Ltd. | EDC Corporation - AIMS Parking | NewBase Computer Services Pty Ltd | TechonoArt Corp. |
| Amazon AWS | Eduserv | Nucleus | Telecom Italia S.p.a. Hosting Evoluto |
| Aria Systems | Egnyte | O4IT | Telvent Global Services, S.A.U. |
| Aryaka | eHosting Datafort | Okta Inc. | Terremark |
| Blackthorn Technologies | Esri ArcGIS Online | OneLogin, Inc. | Think On Inc. |
| Bluedon Information Security Technology | Everbridge | OneNet | TokenEx |
| Box.com | Evolve IP | Onspring Technologies | TokenEx, LLC |
| Brainloop | Exostar LLC | OVH | Towngas Telecommunications Co. Ltd. |
| Brivo Systems, LLC | Exponential-e Ltd. | Peer 1 Hosting | Trackyou Ltd |
| BroadBand Tower, Inc. | Eyefreight BV | Perfecto Mobile | TripleCheck Consulting Inc |
| CapLinked | Falk-Enrich GmbH License12 | Perspectium Corp | Varolii Corporation |
| Capriza | FASTWEB | Ping Identity | Verizon Digital Media Services |
| Carbon60 Networks | FireHost | PIPED BITS CO.,LTD. | Virtustream, Inc. |
| Caretower Ltd. | Hewlett-Packard | Platform9 Systems Inc. | VMware, Inc. |
| CARI.net | HighRadius | PODFather Ltd | Vocera Communications, Inc. |
| CenturyLink | HKT | Poste Italiane S.P.A. | Websense Inc. |
| China Enterprise ICT Solutions Limited | Hong Kong Cyberport Management Company Limited | Projectplace International | Wipro Technologies |

| | | | |
|---|---|---|---|
| christian.brown@centurylink.com | Hootsuite Media Inc. | Promapp Solutions | Wolters Kluwer ELM Solutions, Inc. |
| Chunghwa Telecom | HP Enterprise Cloud Services - Virtual Private Cloud (VPC) | PT Sigma Cipta Caraka | Zendesk |
| Chunghwa Telecom Co., Ltd. | HP Enterprise Cloud Services for Government (ECS-G) | Pulsant Limited | Zscaler |
| Cirrity LLC | Huawei Software Technologies | RapidCompute - Division of Cybernet | |
| CITEC | Hyland | Recall Corporation | |
| Citrix ShareFile | iland | Red Hat OpenShift | |
| Clari Inc. | Intracom Telecom | Ribose | |
| Close IT Support T/A Support on the Spot | IT-GRAD | ServiceNow | |
| Cloud Dynamics Inc. | Jive Software | SHI International, Corp. | |
| CloudAlly Ltd. | Krescendo | Shibumi | |
| CloudLock | Laconic Security | Siteimprove | |
| CloudSigma AG | MaaS360 by Fiberlink | Skyhigh Networks | |
| Code 42 Software, Inc. | Microsoft Dynamics CRM Online | Sliced Tech | |
| CSC | Microsoft Office 365 | Slovak Telekom | |
| Cvent, Inc. | Microsoft Windows Azure | Snipp | |
| Data Noah GmbH | MicroStrategy | SoftLayer | |
| Devellocus, LLC | Mimecast | Solutionary | |