Initial Position Paper Reflecting Cloud Service Provider and Cloud Adopter Requirements

D4.1 AND D5.1

Note, with the agreement of the project Officer, Contractual deliverables D4.1 and D5.1 have been merged to aid readability and value.

Dissemination level: Public

Work Package	*WP4 & WP5, Provider Track & Cloud Adopter Track*
Due Date:	*M4 (30/04/2015)*
Submission Date:	*01/05/2015*
Version:	*1.0*
Status	*Prefinal draft*
Author(s):	*Dave Bicket (CIF)* *Aimilia Bantouna (UPRC)* *Daniel Field (ATOS)* *Breda Beyer (CIF)* *Julia Wells (ATOS)* *Panagiotis Demestichas (UPRC)* *Teta Stamati (UPRC)* *Kostas Tsagkaris (UPRC)* *Panagiotis Vlacheas (UPRC)*

The SLALOM Project is co-funded by the European Commission through the H2020 Programme under Grant Agreement 644720

Contents

Figures

1 Executive Summary

Contractual issues in cloud computing have generated a significant amount of debate. Quantitative studies of cloud adoptions and its inhibitors consistently point to factors such as risk, security and data protection as the largest barriers to uptake. These are factors that should be managed by the contract between the parties.

The European Commission has promoted a raft of measures designed to combat these barriers [1]. This includes the establishment of several expert groups looking at, among other matters, cloud contracts [8] and SLAs [4]. Additionally a number of other bodies have established expert groups and guidelines to aid stakeholders establish, negotiate and interpret contracts and SLAs.

As SLALOM intends to establish the model clauses for cloud contracts and SLAs, it was necessary to review the available discussion and conclusions emerging from the available expert groups. However, very little of the available literature includes first hand feedback from stakeholders. In addition, a relatively recent development comes from the ISO SC38 group attempting to standardise cloud SLAs. A premise of SLALOM is to develop on top of existing standards, yet this ISO standard is under development and has not been validated outside of the working group. SLALOM produced and circulated a questionnaire that sought to identify issues with contracts and MSAs and to evaluate the practicality and desirability of the emerging ISO standard.

This document is the combined result of the literature review and the questionnaire. Its core purpose is to provide a summary of the relevant issues from the perspective of the stakeholders, particularly those of the provider and adopter. This will guide the development of SLALOM's models.

Additionally, this document has value to a broader audience of professionals involved in designing, negotiating or interpreting cloud contracts and SLAs: Proceeding section by section through the contract and SLA, this document summarises and contrasts the expert opinion and guidance from multiple sources. It contrasts this with first hand data from the stakeholders, and maps this discussion to both the ISO [9] and C-SIG [19] standard Service Level Commitments and Objectives. To the author's knowledge it is the only such meta-analysis that has been published.

Conclusions are not repeated here. The report has been authored so that each chapter is as self-contained as possible,each section including its own conclusions. Hence readers seeking advice on a specific issue need only refer to that chapter. In some cases the material presented in a chapter is itself formed of the conclusions from more extensive examination conducted by the various expert groups. Conclusions relating to the SLALOM approach itself are included in chapter 7. Quantitative analysis of the SLO component ranking is found in section 5.

2 Introduction

This document responds to the contractual deliverables D4.1 and D5.1 of the SLALOM Support Action, an EC-funded project (grant 644720) with the mission to develop standard technical and legal models for cloud computing contracts and SLAs. With the approval of the Project Officer, the two contractual deliverables have been merged to avoid redundancy, as both deliverables follow the same pattern.

2.1 Purpose of this document

This document is intended to:

1. Provide the initial position papers 'identifying the key restraints, concerns, business objectives and opinions of the provider segment [deliverable D4.1] and of the adopters [deliverable 5.1] with respect to cloud contracts and SLAs'.
2. Use the above to provide a details of stakeholder requirements for the SLALOM reference models, with a focus on provider and adopter requirements.
3. Serve as a document for use in further engagement and consensus building with stakeholders and as an update to all who have provided input into the project, and those who may be interested in the future SLALOM developments.
4. Be a useful resource to expert groups, adopters and provides and other stakeholders assessing Cloud computing contracts and SLAs. Note customised versions of the material may be produced and circulated as part of the project's communication activities.

Note that the report has been authored so that each chapter of the MSA is as self-contained as possible. Readers seeking advice on a specific issue need only refer to that chapter.

2.2 Context

Cloud Computing reached the top of hype cycle several years ago and the market has seen a steady growth in the number and variety of offerings. Although cloud and other technologies have influenced recent legislation, there are no specific laws covering cloud computing, and as a result the sector is governed by applicable laws relating to e-commerce, data protection and contract law, among others.

Studies repeatedly show that legal issues are considered a barrier to uptake of cloud. The European Commission (ECP) has invested in this area. In 2012 the EC produced a cloud strategy [1], indicating three key areas to increase uptake by addressing legal and other issues: the establishment of the European Cloud Partnership, to cut through the 'jungle' of standards, and to develop 'safe and fair' terms for cloud. Activities have been undertaken to achieve these goals. The ECP [2]was established in 2012 with very senior executives from representative providers, adopters and member states forming a steering board. Under the umbrella of the ECP several working groups, or C-SIGs (Cloud Select Industry Groups) were formed, looking at Service Level Agreements [4], certification schemes [5] and Code of Conduct [6]. An expert group on research was established [8]. All of these activities were conducted by

the Directorate-General DG-Connect. Another wing of the Commission, DG Justice, established an expert group looking at Contractual issues [8].

In addition, a number of other groups have studied the areas of SLAs and Cloud computing contracts, including ISO [9], ETSI [3], the Cloud Standards Customer Council [10] and the Cloud Industry Forum [11], among others. However, barring an ENISA study **Error! Reference source not found.**, very little quantitative surveying of stakeholder needs has been conducted.

As SLALOM sets out to define model clauses for the Master Service Level Agreement, (or contract) for cloud computing, a precursor is to incorporate the observations and conclusions from the various expert groups. By the time the SLALOM project was initiated in January 2015, the ISO group had developed a family of draft standards for Service Level Agreements (ISO/IEC 19084-x). This is generally aligned with the recommendations made by the C-SIG on SLAs [19]. Naturally SLALOM seeks to base its work on existing standards, However there was little stakeholder confirmation about this emerging standard. SLALOM saw a need to both quantitatively assess the practicality of the proposed ISO standard and confirm the findings of the various expert panels. A questionnaire was distributed widely to stakeholders (policy makers, providers, adopters, researchers and the legal profession).

This document is the result of that labour. It seeks to summarise the available expert discussion on each section of the Master Service Agreement and to contrast this both with (a) the Service Level Commitments and Objectives proposed by ISO and the C-SIG, and (b) first-hand feedback from the stakeholders.

2.3 Document Structure

This document first presents general feedback and observations from the work and questionnaire, and then proceeds to summarise the discussion around each chapter of the MSA[1] in turn. Where specific ISO or C-SIG SLOs are available these are included at the end of each chapter. Where discussion revolves around a subject expressed in a specific SLO the discussion is placed after that SLO. Specific quantitative feedback on the ISO structure is provided in chapter **Error! Reference source not found.**. The document then presents feedback on five scenarios emerging from research that were presented in the SLALOM questionnaire, and provides further details on the approach, including the SLALOM handout and questionnaire.

2.4 SLALOM overview

SLALOM is an initiative aligned with the European Cloud Strategy. The first phase of the initiative is an 18-month, EC-funded project whose objective is to create a Service Level Agreement (SLA) reference model consisting of model contractual terms and model technical specifications. It seeks to provide clarity and reassurance to the market through establishing a baseline of fair and balanced provisions for

[1] Note there is no standard MSA structure available. This structure used was based on common industry practice.

cloud SLAs. These can be adopted by most cloud service providers and consumers without great expense yet providing a high level of trustworthiness. The benefits to industry include greater uptake of cloud computing by reducing the recognized barrier to adoption of lack of trust and consequent risk.

The first phase of SLALOM is divided into three sub-phases as shown in the figure below:

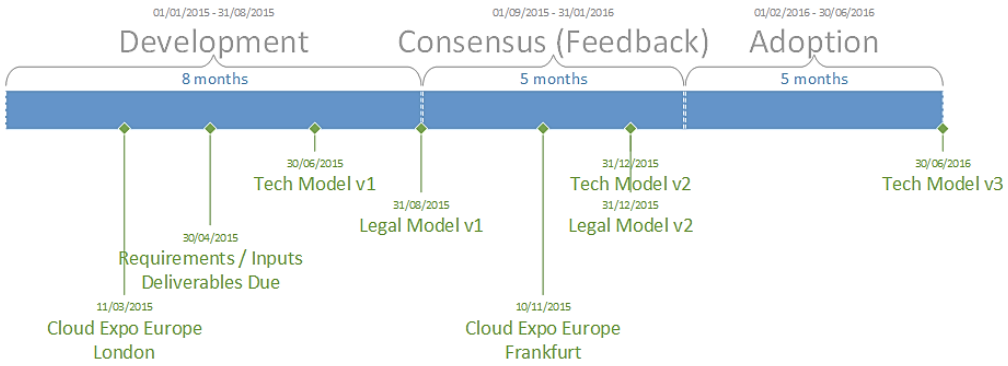


Figure 1: SLALOM Timeline

2.5 Glossary of Acronyms

Acronym	Definition
CSC	Cloud Service Customer = Adopter or End-User. (CSC is term used by ISO.)
CSP	Cloud Service Provider
SLA	Service level Agreement
SLO	Service level Objective
C-SIG	Cloud Select Industry Group
MSA	Master Service Agreement

In addition, the reader should note the following short hand:

All discussion of respondents and direct feedback from providers, adopters and 'other' should be assumed to refer to the SLALOM questionnaire and interviews unless otherwise specified.

Other in this context refers to respondents who are neither CSPs nor adopters: generally associations or researchers.

References to the DG Justice Expert group refer specifically to the Expert Group on Cloud Computing Contracts [8]. Although this is managed by the European Commission, The views expressed by its

experts and documents published do not represent the views of the European Commission as an institution.

3 General

3.1 Observations

In identifying and reviewing around 100 source documents on Cloud computing contracts and SLAs, several general observations can be made.

Firstly, there is a significant abundance of amateur or non-official advice, general thoughts and light recommendations on the matter. Most of this is not grounded in primary or secondary study nor is it the consensus of a panel of experts. Very little of it is formal work that has gone through a process of review, discussion and publication. Rather it is formed of blog posts, anecdotes and short news articles. There is a lack of detailed, comprehensive and validated material to guide CSPs and adopters. Of the 100 sources we identified, the majority were reiterating the conclusions of single sources already in the list, and so could be excluded. Ultimately, perhaps 25 key sources would constitute the category of original, detailed, comprehensive and validated documents. The very high proportion of 'click-bait' and page filling around this subject is likely to be a hindrance, giving the impression of increased complexity.

Almost all of the 25 sources finally examined in detail can be classed as advice from professional groups (including the ECP C-SIGs, the DG-Justice Group, the Law Society, the Cloud Standards Customer Council and ISO). Only one identified source included a quantitative survey of CSP and Adopter experiences with contracts and SLAs ([22]). Concrete examples of terms and disputes were also low. The documents produced by the DG-Justice expert group are an exception; here statements are frequently backed up by references to both actual contractual terms and examples of disputes. Nonetheless, and applicable to all the sources, the lack of quantitative data from practitioners poses a risk to the validity and applicability of the advice given. Whilst it is appreciated that court cases involving cloud contracts are low for a number of reasons, and industry practitioners are represented in these various expert groups there is a potential disconnect between what the market forces require and what the experts believe they require. Indeed the SLALOM questionnaire noted that respondents identifying themselves as adopters or CSPs tended to be more aligned in their responses that those who identified themselves as Associations or researchers. Furthermore, one SLALOM respondent recommended that we 'Speak to real cloud users and real cloud CSPs, rather than the old guard, and learn from them', implying an evident distrust or rejection of expert views.

3.2 Practicality and importance of the approach

3.2.1 The need for standardisation

Two questions were asked in the questionnaire to assess the importance of the work being done.

- "*What are your organization's key constraints for its increased provision/use of cloud computing?*" This was to determine the context within which this work is being done, to indicate

the relative priority which CSPs and Adopters have for inhibiting factors to increased provision/use of cloud computing.

- "*To what extent do you consider contract and SLA-related issues as inhibiting your organization's increased provision/use of cloud computing?* " This was to ask the question explicitly about contract and SLA-related issues.

The feedback from these questions demonstrated that contractual and SLA-related issues are not seen as 'show-stoppers' by either CSPs or End-Users. However, they are seen as inhibitors to cost-effective uptake, in particular by SMEs (both CSP and Adopter) which do not have the legal staff or external legal support which larger organizations have. Significant value is seen in 'standardization', so long as it does not prove burdensome (i.e., 'keep it simple') and so long as it does not constitute a straightjacket (i.e. 'one size fits all' which does not).

From perspective of CSPs there were few comments about general contractual issues unrelated to SLAs, except as detailed below (e.g. data location). The overwhelming view is that SLAs do not inhibit cloud uptake (10 responses, 2 non-responses). A limited number (4) said they want standardization, but do not say if they inhibit cloud uptake (3 SMEs, 1 just above: 250 – 999 employees). One stated that SLAs are important, but did not indicate if they inhibit cloud uptake.

Standardisation was seen as most important for the Enterprise sector; Public sector; Local government and Charities. One provider expressed the view that SLAs are not important for run-rate (= standardized, high-volume, low cost) services. Another added that there are no meaningful SLAs by public cloud providers.

Other issues mentioned were:

- Data location
- Availability (difficulty of achieving high levels)
- 'Off-shore or third party administrative roles in service assurance' [apparently = issue of subcontracting]
- Customer confusion

From the perspective of Adopters few considered this important. (4 ignored the question, 1 said it was not an inhibitor (if properly written); 1 said low; 1 said medium to low). Several commented directly or indirectly about desirability of standardizing and in particular managing variances of the same terms between vendors.

Only two strong comments were received: "Very significant. Too much time reviewing contracts for potential privacy liability risk assessment with no ability to negotiate limitation clauses' and "Lack of control about personally identifiable information outside of our doors"

From perspective of Others, 2 limited responses were received from the 5 ("basically" and “Significant"). One extensive comment read: " .. should be structured by strong, standard, simple and agile SLAs and contracts…"

3.2.2 Overall factors inhibiting cloud uptake

Additionally Respondents were asked to list Overall factors inhibiting cloud uptake. From the perspective of CSPs one mention was relevant to SLALOM’s scope: 'legal issues'. There was minimal mention of 'traditional' cloud issues: Data location; Security; Resilience; Robustness; and Availability. Instead most wee marketing and education related. Some relate to fast-changing technology and the ability to keep up whilst others reflected financial and management concerns of potential customers: Capex vs opex; Need to utilize existing infrastructure investment; and Reluctance of IT management to lose control. Some reflect particular concerns of small SMEs: Funding; and One cited exposure to government policy changes (for CSP serving government). Finally some reflect supply chain issues (Licensing).

From the perspective of Adopters there were limited mentions relevant to SLALOM scope: 'difficulty of comparing CSPs'; and Availability (2 mentions). The main concern is regulatory compliance: Personal data protection; and Data location. Security was the second-highest concern. There were a variety of other single mentions: Vendor lock-in; Feasibility; Performance; Storage; Redundancy; Threat deterrents; Accessibility; and Direct audit possibility.

From perspective of Others there were only 2 mentions: Cost; and Need for technical cloud brokerage platforms/portals.

3.2.3 The practicality of model terms and specifications

There is considerable overlap in the proposed ISO SLA standard ISO/IEC 19084-1 between measurable metrics and overall contractual content (or 'service commitments'), and SLALOM should give consideration to what it lists as needing to be covered. See the supporting analysis below, plus Section 5 (Component and Metric Prioritisation).

There are some strongly expressed views for and against having model terms and specifications. Views of principle include the following:

- **Pro**: they save time and resources, and provide better assurance of SLA appropriateness and adequacy, by providing a trusted verifiable starting point for providers and business users to negotiate. They are particularly helpful for SMEs who do not have the legal support to navigate and negotiate complex and varied contractual provisions from different potential vendors.
- **Con**: they create a 'one-size-fits-all' straightjacket which simply does not work.

There is also the issue of whether realistically they will be taken up by industry. There is a fairly poor track record of model terms being developed and adopted successfully. This issue is recognized, and

must be dealt with if SLALOM is to be as successful as intended. See 3.8**Error! Reference source not found.** below.

3.2.4 Guidance on contract standardisation

The EC-endorsed C-SIG guidelines to SLA standardisation, published in June 2014 [19], provide certain recommendations. These are: Technology-neutral, business model neutral, world-wide applicability, unambiguous definitions, comparable SLOs, conformance through disclosure, the ability to span customer types, cloud-specific, business and technical proof points, informative rather than descriptive, and finally, written by lawyers.

Although other sources have followed their own guidance on how to standardize SLAs and contracts, (for example the ISO working practices) these sources don not offer explicit guidance for standardizing cloud contracts and SLAs to other standardization efforts.

SLALOM will follow these guidelines, with the exception of *'informative rather than descriptive'.* This document details the descriptive advice available where identified. It is the premise of SLALOM that there is significant value to be gained from providing a model baseline set of clauses. Additionally whilst the legal clauses in SLALOM will be produced by lawyers, we identify the need also for technical specifications, written by technical experts. ISO is also taking this approach (see 3.4.3).

3.3 Structure and order of the MSA and SLA

The literature review identified at least two expert groups, namely the ECP C-SIG on SLAs and ISO, who have identified a common, proposed standard structure for Cloud SLAs. No such standard proposal for a MSA exists, although there is common agreement on what it should contain, with slight variation on nomenclature and fine-grained division of topics.

A general observation can be made that sources representing the legal profession (e.g. the law society or the DG Justice group) or offering advice on what the contract should cover tend to follow a different structure to that posed by more technical writers, including the ISO and C-SIG groups. This is due to an inexact matching between the business risk being managed, the standard legal method to manage that risk and the implementation of the service that covers that risk. This was picked up upon by a respondent to the SLALOM questionnaire who listed 'Mapping user needs and SLA' as the biggest pain point for SLAs. A clear example emerges from data management. Here several issues emerge: confidentiality of the adopters IPR (confidentiality); safeguarding that IPR from third parties (security); compliance with data protection legislation (privacy, compliance); data portability (relating to contract termination); access by law enforcement agencies (privacy, compliance, confidentiality); and back up management (business continuity). Depending on the outlook of the author, different sources break this down in different fashions. For example, as part of the data management topic, ISO considers data confidentiality, data deletion, data portability, data access by law enforcement and data location as one section, mixing the issues of confidentiality, contract termination, and potentially jurisdiction. Data back-up is treated as a separate section under business continuity. The C-SIG considers a number of issues

such as user authentication and management as part of its security component, although these clearly have an impact on confidentiality.

3.3.1 Quantitative Assessment of MSA Approach

SLALOM validated the approach of having the MSA as an umbrella document including specific documents including the Acceptable Use Policy and the SLA.

Org Type	No of Responses (Full Questionnaire Only)	Average Rating
CSP	5	4 – Good
Adopter	4	4.25 – Good
Other	3	3.33 - Poor

Given the lack of a clear standard across the sources, the good reception of the MSA approach and the arbitrary separation of connected issues, SLALOM will be based on the emerging ISO standard (concretely the ISO/IEC 19086 family of standards)**.**

SLALOM questionnaire respondents were asked to provide a qualitative assessment of the MSA approach. There was some concern/disagreement about specific terms proposed which is incorporated in this document. Overall assessments of the MSA approach were given ranging from good to poor:

- Good: 'excellent'; 'very useful examples'
- Negative: 'I believe SLALOM is not addressing the problem from the correct perspective. Some cloud providers pitch service directly to consumers, and terms will need to be different from terms meant for enterprise, where there will tend to be greater scope for negotiation. In either case, SLALOM should be looking at the really key issues - controller, processor relationships, writing terms that serve the many available consumption models, DP compliance, etc. - what is proposed is too simplistic, and assumes all CSPs are like Facebook!'

From perspective of Adopters the overall assessment was “good”: 'useful'; 'I will use them today'. There was a suggestion for improvement: 'Maybe broader examples, organized for each kind of sector/industry'.

From perspective of Others overall assessments given ranged from good to very poor

- Negative: ' The "Model Terms" are either dictatorial (lengthy pages of terms and conditions that the Customer is required to accept to enable swiftly the cloud based services OR they are open to debate, with lengthy negotiations which reach agreements that are still highly in favour of the provider.

There was a suggestion for improvement: ' The comparisons of good and bad terms are informative, but we also need a straight-forward list of recommended terms.' The reader should note that SLALOM intends to deliver the latter. The former discussion, summarized in this document, comes mainly from the questionnaire responses and third party material.

Despite following a standard structure, it must be acknowledged that there is no such thing as definitive set of components that are required to regulate the agreement between CSP and adopter. Indeed one SLALOM respondent (an Adopter) stated that their biggest pain point in MSAs was: '*The lack of a standard framework, in order to give a reply to the question: "How can I be sure that all the parts of a CCC [Cloud Computing Contract] are covered?*'. The solution is more complex than providing an exhaustive list as the applicable laws also regulate the contract, and these may vary by jurisdiction, as may the court's interpretation of them. SLALOM's response to this need is to base its terms on existing best practice, complemented by additional terms identified through the literature search and questionnaire.

Nonetheless, SLALOM must also balance this request for exhaustiveness with the (louder) requests for simplicity.

3.4 Alignment and improvement with respect to ISO

It has been a fundamental premise of SLALOM that we need to align with, and leverage from, the ISO SLA standards currently under development (ISO/IEC 19086 family of standards). This premise remains, but since these standards are under development, they are moving targets. Furthermore, there is considerable content in these standards which is concerned with non-measurable requirements. These non-measurable requirements (or 'service commitments') are effectively contractual provisions rather than measurable service levels. The current situation is that the draft ISO SLA standards effectively cover much of the same scope as SLALOM, namely the overall cloud contract (at the Master Service Agreement level), and then more detail at the Service Level Agreement level.

Other sources, particularly the C-SIG SLA working group are also attempting to align themselves with this emerging standard.

Based on the SLALOM questionnaire responses, the proposed approach of using the ISO structure is considered good overall, but with a number of comments and recommendations for improvement. N.b. even some of those commenting that it is 'good' consider that it is too detailed to be practical.

In the questionnaire, a number of detailed recommendations have been made for consideration for SLALOM's work, and potentially also by ISO.

- Regarding the structure, it is suggested that the data management component has too many sub-components.
- Regarding other additional components, the following are suggested
    - Warranty (compliance with law and agreement)
    - 'Payment section (payment terms, indexation, consequence of non-payment)'
    - 'Penalties'
    - 'Service cancellation rights for both parties'
    - 'Termination of service component: Deleting derived and customer data?'
    - 'Mediation and arbitration'

- Subcontracting'
- Agility to integrate a service (or to stop a service). Associated: portability and reversibility'
- Scalability (to ramp up or ramp down) of a service
- 'Generic definitions. Availability is used for example, but there are many different definitions of it. Specific formula should be included'
- 'Cost reporting ! daily, weekly, monthly, wtd, mtd, ytd, forecasting...etc...'

- There are many further detailed suggestions contained in the supporting analysis below.

3.4.1 Quantitative Assessment of ISO Structure and missing components

Org Type	No of Responses (Full Questionnaire Only)	Average Rating
CSP	5	4.16 – Good
Adopter	4	4.2 – Good
Other	3	4 - Good

3.4.2 Qualitative Assessment of ISO Structure

From perspective of CSPs the balance of views was considered positive. There were concerns regarding the complexity (despite rating the structure as 'Good', the respondent commented “[it] is probably excessively complex in operation. Few [SMEs] will pay the extra for the additional work and structures involved”. One respondent was particularly negative: after an assessment of 'Poor' they stated “Tries to shoe-horn the old world into the new”.

From perspective of Adopters the only comment was that the “process view should be included somehow?”.

From perspective of Others the balanced view was 'good', a qualifying comment from an Other echoed the CSP concern on complexity, despite an assessment of 'Good'. “It is too detailed in some points and probably overambitious, eg. in terms of MTTR (mean time to recovery), or all the information on data backup. Would probably make SLAs too complex for a user or provider to understand or upkeep”.

One negative comment from an 'Other' giving assessment of 'Poor' was 'The above SLA's should be industrialised, standardised and cloud service providers should be 'certified' to be capable (or not) to provide a high (or medium or low) level of traceability, visibility, monitoring reporting. An industry standard should emerge, like for any other industry...'

We note that this latter note is against the principle of SLALOM of providing a standard baseline focused on the definition, but allowing the CSPs to compete on the value, of SLOs. Other expert groups had a similar or more limited stance on defining what level *should* be offered.

3.4.3 Service levels vs. service agreement structural components

For the purposes of this document it is necessary to explain an issue being discussed in SC38 WG3 concerning the draft 19086 family of standards. This explanation is important because (a) it reflects the way the SLALOM project itself is structured, into separate tracks for legal agreement structural components and for the technical specifications; and (b) it is helpful in order to understand some of the questionnaire results, and how they are further interpreted in this document.

3.4.3.1 Service levels

The main issue concerns what is a 'service level'. CD1 of ISO/IEC 19086-1 (Service level agreement framework – overview and concepts) does not give a definition for 'service level'. However, a definition can be derived from one which is given for 'service level objective'. This is:

> Service level: 'a specific measurable characteristic of a cloud service'. 'Measurable' is a key element of this definition. If it is not measurable, it is not a service level. Notes which perhaps could be added are that (1) service levels are expressed using metrics, and that (2) they are expected to be subject to change during service delivery, and need to be measurable during service delivery. They are not intended for use in a binary sense (yes/no) for general contractual compliance.

'Service level objective' is defined, both in the formal definitions, and also in comments submitted on the first draft. The formal definition is 'a specific, measurable characteristic of a cloud service for which the cloud service provider makes a commitment'. A simpler definition, stated in terms of the above definition for 'service level', is given in one of the comments submitted, namely

> Service level objective: the target for a service level

The definition given for metric is as follows:

> Metric: a standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement.
>
> NOTE 1 - A metric implements a particular abstract metric concept.
>
> NOTE 2 - A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific objective.

Note that there are definitions and comments in the published ISO/IEC 17788:2014 (cloud computing – overview and vocabulary) for service level agreements, but these do not conflict with the comments above.

See Section **Error! Reference source not found.** for a more detailed discussion of what specific service levels and associated metrics should be considered priorities for SLALOM based on the work done.

3.4.3.2 Cloud service agreement structural components

The term 'component' is used extensively in the CD1 draft of ISO/IEC 19086-1. It does not have a formal definition, but the text states that 'The cloud SLA components clauses define the concepts commonly used in cloud SLAs.' It is the view of this document, based on the usage of the term in the draft, based on national body comments on the draft, and based on our own analysis, that this should be more fully described as a ***cloud service agreement structural component***. This does not mean that it is required, or that when used it must be in a particular form, but merely that for the purposes of structuring the content of the proposed standard it is a potential element in a cloud service agreement or related contractual documentation. ('Element' is an alternative word suggested in place of 'component'.)

Furthermore, it has been frequently commented upon that many of the components in the CD1 draft of ISO/IEC 19086-1 are not measurable in the sense of service levels. Examples include the statement of covered services; the definition of terms section; and provisions for security, personal data protection ('PII'), backups, disaster recovery, and audits. It has been suggested that some of these types of components should be called 'service commitments'. It has also been noted that that many components may typically be found in contractual documentation other than in the 'service level agreement' itself.

It is the conclusion of this document that the scope of CD1 of ISO/IEC 19086-1 significantly exceeds the requirements of dealing with 'service levels', but rather extends to dealing with the overall structural components of cloud service agreements in general. This broader scope largely agrees with SLALOM's scope.

3.4.4 Missing components identified in the questionnaire

From the perspective of CSPs several additional major components were proposed:

- Warranty (compliance with law and agreement)
- 'Payment section (payment terms, indexation, consequence of non-payment)', 'Process of payment'
- 'Penalties', ‘commercial incentive of penalty for lack of service’, 'There should be a commercial liquidated damage calculation for loss of service e.g. that leads to a credit note rather than a termination of the agreement’.
- 'Service cancellation rights for both parties'
- 'Termination of service component: Deleting derived and customer data?'
- 'Mediation and arbitration'

From the perspective of Adopters:

- Managing subcontracting and ensuring standardisation of obligation in this context. Please see Cloud Security Alliance Control Matrix that addresses this topic.

From the perspective of Others:

- 'Agility to integrate a service (or to stop a service). Associated: portability and reversibility'
- Scalability (to ramp up or ramp down) of a service
- 'Penalties'
- 'Cost reporting! daily, weekly, monthly, wtd, mtd, ytd, forecasting...etc...'
- 'Generic definitions. Availability is used for example, but there are many different definitions of it. Specific formula should be included'
- Costs monitoring/reporting
- Cloud based orchestration Tools, services, monitoring, reporting... (Cloud Management Portal services).

Among the literature source, the CSCC practical guide to cloud computing contracts [20] stated that, service deployment terms should be included in a CSA, covering the deployment model (Private, Community, Public or Hybrid cloud) and the deployment technologies adopted. This source was the only identified source to address contractual differences between these models.

3.4.5 Improvements to identified components

CSPs responding to the questionnaire noted the following:

- 'Have a quantifiable level of security'
- 'Security controls for cloud providers needs to be called out (denial of service protection - both volumetric and application layer).'
- 'DOS attack defence planning'
- 'Intrusion detection'
    - 'Clarify exactly what type of access cloud provider has to customer data (e.g. purely for customer support, or also product management to improve product). Some cloud providers gather detailed metrics, even if in aggregate, that customers often are not aware of. I don't think it's a bad thing to collect this data, but customer should be informed.'
    - 'Service desk response time, Change management response time (where applicable)'
    - 'Network availability, latency'
    - 'Governance component: Audit results?'
    - 'How to measure availability of service as a whole'
- Main negative comment: 'A specific element on security standards, other than that there is far too much, and would push up the cost of cloud computing in Europe if CSPs were forced to build monitoring tools to cover the entirety. The components also fail to recognise that many elements would be service options driven by customer choice - e.g frequency/method of back-up, asynchronous replication across data centres for DR, etc'

Missing security details were also noted by adopters: ‘a set of standard "minimum" security controls’.

The C-SIG on SLA's has proposed fourteen SLOs relating to the security component, including the management of security incidents.

3.5 Suggestions for improvement

Beyond the above comments relating to the alignment and improvement to ISO, the following recommendations were made.

From perspective of CSPs a clear desire was for a simple SLA. The CSP's felt that enterprise customers do not have the resources to be overly concerned with the fine detail. Given the lack of negotiating power, they have to accept the offered SLA, and could "resent paying for a service in order to have an SLA they won't understand, and won't care about". One CSP respondent also commented on the importance of common language and expectation setting between provider, reseller and end user.

3.6 Different types of cloud

In the SLALOM questionnaire, one Adopter flagged "Private cloud versus public cloud" as their biggest pain point in cloud SLAs. Similarly, one CSP highlighted this as their biggest MSA pain point: '*Many customers don't understand major areas of security vulnerabilities in SaaS applications - mostly in management consoles, by Customer Support, Product Management, etc. Since in many companies, SaaS have lots of access to customer data that the customer may not realize. Yet, the customer contracts try to require very specific security requirements that are archaic (e.g., intrusion prevention devices, instead of newer web application firewalls or privileged account management)'.* In the literature review very little instructive content was to be found on this issue, and indeed the differences between IaaS, PaaS, SaaS and other cloud models. Certainly differences in context were noted when discussing contracts and SLAs. However conclusions were not drawn. The same is perhaps more true of the content we discarded for the literature review. The click-bait and news articles often centred on the different types of cloud as their theme, but again without any considered or formal recommendation in terms of contractual content.

The major exception is the CSCC practical guide to cloud computing [20], from which the following table is taken:

IaaS	The main issues concern the mapping of high level application requirements to infrastructure services levels • *Compute metrics: availability, outage length, server reboot time* • *Network metrics: availability, packet loss, bandwidth, latency, mean/max jitter* • *Storage metrics: availability, input/output per second, max restore time, processing time, latency with internal compute resource* Production environments should have more stringent service level objectives than development environments.

	Network metrics in a cloud SLA generally cover the cloud provider's data center connectivity to the Internet as a whole, not to any specific provider or customer. End-toend network service levels may require a combination of separate agreements between the provider, the carrier, and the customer. *Cloud providers to commit to supporting open standard interfaces, formats and protocols to increase interoperability and portability*
PaaS	*At a minimum, PaaS SLAs should inherit IaaS SLAs for the the underlying infrastructure* distinguish between PaaS development environments and PaaS production environments *includes support for such open standards, as they become available, to reduce vendor lock-in.*
SaaS	Given the wide variation of services provided at the SaaS level, it is difficult to provide a comprehensive and representative list of SaaS service level objectives for customers to require in their CSAs. These objectives will be largely application-specific. *general SaaS service level objectives like monthly cumulative application downtime, application response time, persistence of customer information, and automatic scalability to be included in their CSA* *data maintained on the provider's cloud resources is stored using standard formats to ensure data portability in the event that a move to a different provider is required.*
Private (On-site)	similar to those of a traditional enterprise data center SLA
Private (Outsourced)	*security techniques for protecting the customer's perimeter and the communications link with the provider.*
Public	*must include stronger requirements than the Private (Outsourced) model since the provider's IT resources are now shared across multiple customers. Specifically, the provider must address the added security, availability, reliability and performance risks introduced by multi-tenancy.* The ability to measure and track specific service level objectives becomes more important in the Public deployment model.
Hybrid	increased likelihood of unique service and data integration requirements between cloud and enterprise services (e.g., so that external cloud can be used seamlessly to handle an overflow of demand beyond the capacity of the internal cloud) *A specific document should describe the private/public interface, along with quality metrics, performance characteristics and security requirements associated with the interface.*

Finally several sources, including [16] and several SLALOM questionnaire respondents (adopters) indicated the desirability of end-to-end measurements in terms of user experience. The type of cloud will have a bearing here. For more discussion of this see section 4.2.

3.7 Language issues

Both formal (questionnaire) and informal feedback from stakeholders identified the issue of language. Concretely a contract and technical specification need to be unambiguous in order to be valid, yet few stakeholders fully understand specific legal or technical intricacies. Moreover English is a lingua franca and many users of it are non-native speakers.

Pragmatically we need to accept and deal with several levels of documentation and specifications:

- Explanatory documentation can be in plain English, or as close to plain English as possible. But this type of language seldom works for contractual or technical specifications due to ambiguity.
- Legal terminology and wording is unavoidable for contracts and related documentation. However, to the extent that it is produced by SLALOM, it should be fair and balanced to all parties, which should allay some of the concerns especially for SMEs of dealing with such documentation.
- Technical specifications are intended to be precise and unambiguous, but they are often highly unintelligible to non-technical people. Consider, for example, specifications for XML. Few people can understand these. The technical specifications for metrics, such as are being worked on for the proposed ISO/IEC 19086-2, will almost certainly be similarly difficult for ordinary people to understand. Nonetheless, they are important to develop, because they facilitate comparability, and will also facilitate the automation of metric monitoring and management. To the extent that these are produced by SLALOM, it should provide reassurance that they do what they are intended to do.

3.8 Driving uptake

Conversations with stakeholders corroborate the project's opinion that uptake of SLALOM's results will be driven in three ways:

- Some large CSPs may be willing to implement many of SLALOM's model terms and specifications to demonstrate their intention of being highly transparent and balanced in their dealings with the cloud marketplace, and in particular with SMEs. This will probably be more likely the closer SLALOM's model terms and specifications align to the emerging ISO standards.
- Many small CSPs will likely implement many of SLALOM's model terms and specifications because they will be a differentiator against other CSPs, both large and small. Using SLALOM's model terms and specifications will also help control costs associated with developing and negotiating contracts.
- Ultimately uptake will probably be driven most by large Adopter organizations which mandate their use, including national and regional governments (such as the EC).

The observation has been made – including in questionnaire feedback - that large organizations, whether providers or consumers – have no need or incentive to adopt model terms and specifications, because they have the legal resources to deal with anything they encounter, and indeed they can generally insist on terms advantageous to themselves if they are larger than their counterparties.

SMEs are the ones who benefit most from model terms and specifications being adopted, yet they do not have the muscle to make it happen widely. Notably, the majority of CSPs providing input for SLALOM were SMEs.

Consequently one issue for SLALOM, and other standardisation groups to manage, is how to encourage large adopters to take the plunge, given this observed lack of incentive.

4 Master Service Agreement (MSA)

The following section discusses both the results of the literature survey and the questionnaire relevant to each section of the MSA. We start with an overall discussion on the MSA.

Overall, the proposed approach is considered good. Concerns primarily relate to the worries about a 'one-size-fits-all' approach. Assuming that sufficient flexibility can be built into the proposed model MSA terms and conditions, yet without throwing everything open to endless negotiation, it should help drive the speed of cloud contracting.

The questionnaire asked respondents to identify pain points in the current MSA practice. Many of the specific concerns will be dealt with later in this document. Here we list the general comments on the MSA.

From the perspective of CSPs:

- 'The length of time that potential customers take in looking at, and getting comfortable with, new areas of control within the contract - for example, controls on data access and location of data.'
- 'Cloud computing contracts are nothing different from managed services / outsourcing services contracts except that customers are very conscious about data privacy and data security related issues'
- Customer need for education / better understanding
    - 'Client ignorance in the technology and their own responsibilities in managing risk.'
    - 'Lack of understanding of Cloud and how to interpret the contract in relation to the provision which leads to big questions that are difficult to answer in layman's terms as things are so new. The What If scenarios which can get a bit unrealistic especially when people hear "gossip" on the news about the latest security breaches. People's lack of understanding.'
- Problems for customers in comparing different cloud service offerings
    - 'When prospects are comparing quotes it is very difficult to ensure they are comparing like for like. We find difficulty in helping the customer understand the differences between service offerings'
- Contracting and professional legal support
    - 'One of the benefits of cloud computing is to avoid contracts. Negotiated SLAs bring this back.'
    - 'Public sector type frameworks assist in definition and therefore avoid repeated queries and exceptions. Lack of legal support within SMB channel means that backing off provider terms to End user contracts is not always clear and the provider ends up supporting that process.'
    - 'They are usually almost worthless as caveats always dictate maximum forfeits based on actual user money spent.'
    - 'Reluctance to commit to a contract at all'
- Other
    - 'Complexity'

- 'What's a good standard'
- 'Customers like the flexibility to grow with cloud computing. There are still lessons to be learnt to ensure the company communicates well between technical/account management and financials. We are addressing this issue with the implementation of a centralised management solution which will improve this issue massively.'

From the perspective of Adopters:

- Security and personal data protection issues
  - 'It does not protect against unknown breaches or security incidents as long as the cloud provider is not legally subject to notify them.'
  - 'Completeness of SLA : how far to go, what is acceptable by the provider, take it or leave it approach if the provider has a dominant position on its market.'
  - 'Changing nature of contract provisions with no ability to foresee / negotiate privacy & data protection provisions.'
- Contracting and professional legal support
  - 'The lack of a standard framework, in order to give a reply to the question: "How can I be sure that all the parts of a CCC [Cloud Computing Contract] are covered?"'
- Other
  - 'Customer's rights'
  - 'Use of 3rd parties by main contractor who are they and where are they?'
  - 'Private cloud versus public cloud.'
  - 'making them simple for all parties to agree to and review as a partnership

From the perspective of Others:

- Contracting and professional legal support
  - 'It's the binary approach:
    - either you accept the terms and conditions AS IS and have quick access to the cloud services - or you do NOT accept the AS IS T's&C's, and not have access to the services Alternatively, you hope for a fair negotiation to protect the customers interests, as well as the cloud providers, and hope for the best...'
  - 'The lack of transparency on the cloud provider infrastructures and how the customers' data are managed on those infrastructures. And here again, a big binary jump forwards:
    - either you accept that your data are somewhere secure on the providers infrastructures, or....- you accept the higher price of "on premise" services, with a CAPEX model that creeps in with this "traditional model"'
  - 'Length and legal complexity of the contracts.'
  - 'Differences in definitions, obscure legal language, lack of auditing'
- Problems for customers in comparing different cloud service offerings
  - 'Difficulty of comparing different CSPs.'

4.1 PROVISION OF SERVICES

It is understood that this section deals with the description of the service, including common definitions.

From the literature and the questionnaire three issues were identified that should guide the descriptions of the service. These are: Common definitions; Clarity; and Completeness and relation to business requirements.

Both ISO and the C-SIG, among others, have created lists of definitions. SLALOM will use the ISO definitions as the baseline, complementing them with definitions from the C-SIG where absent in ISO. Several respondents to the SLALOM questionnaire identified problems with definitions, sometimes in service descriptions and other times with SLOs. Both CSPs and Adopters commented that comparing like for like was complex due to the lack of common definitions. Others complained that there was no standard to compare to. Across both the literature search and contact with stakeholders, the situation is summed up in the question "how are uptime and availability calculated?" Variants of this were met across the board, with the implication being that this goes for all metrics.

Other comments complained about the use of language (obscure legal or technical jargon) or an overuse of caveats. Some comments stated that having no standard definition to compare to was an issue.

Multiple respondents urged SLALOM to "make it simple" and that "clarity is key", at the cost of imperfection. There was a need to ensure consistency with other model documents to ensure consistency.

SLALOM will attempt to resolve these issues by promoting its (ISO-based) definitions as a European Standard, with a clear, unambiguous and balanced language.

There were also comments suggesting the need to align the definitions and service description with business needs: relevant for the users. It was also important to ensure that end users were fully aware of what control of what was and what was not being offered. As one Adopter put it, their biggest pain point was "The business area understanding we no longer have the same control that we once had when we provided the service internally."

4.1.1 Service level objectives and commitments

The following service level objectives and commitments have been identified in the literature. Where appropriate we add our findings from the questionnaire and literature search:

ISO 032 Covered services component [Overall]

ISO 033 SLA definitions component [Overall]

Multiple definitions exist (ISO, C-SIG, Gartner's report for the C-SIG, the Cloud Standards Customer Council, etc.) SLALOM will use these sources in this priority.

ISO 034 Service monitoring component [Overall]

ISO 035 Service monitoring component [/ Monitoring parameters]

ISO 036 Service monitoring component [/ Monitoring logs]

The CSCC [20] comments on the necessity of this component. They note that Log file entries are important to cloud service customers when analysing incidents such as security breaches and service failures as well as in monitoring the customer's day-to-day use of the service. They consider an associated SLO mandatory.

C-SIG Log access availability

C-SIG Logs retention period

Some important anecdotal evidence on this point is necessary. The expert groups in the literature study frequently take for granted that monitoring data is 1) needed by adopters and 2) should be provided to them. However one of the CSPs responding to the SLALOM questionnaire suggested that providing *'Admin and tools to monitor internally that we are meeting our SLAs*' was their biggest SLA pain point. It was qualified however with: '*In saying that, few people ask us to provide these measures.*'

This should be considered by SLALOM. An open issue for the project is to determine the extent to which adopters 1) actually want these and 2) how much they are prepared to pay for this. SLALOM should investigate the cost implications for CSPs in order to identify the most balanced way forward.

ISO 037 Roles and responsibilities component [Overall]

ISO 038 Roles and responsibilities component [/ Responsibility list]

ISO 039 Accessibility component [Overall]

GARTNER Automation and IT Operations Management:

- *(a service catalog describing add-on services*
- *self-service capabilities*
- *the support of VM templates for easy re-deployment.*
- *application life cycle management (ALM)*
- *metadata tagging*
- *a health dashboard for the service)*

GARTNER Degree of Customization (SaaS only)

(if a degree of customization of the software is possible, or if it is 'one size fits all'. This will depend if the software image is shared with other organisations or dedicated to a single organisation.)

GARTNER Isolation of instances on shared resources

(How full logical isolation is retained between independent application instances , which share physical computing resources (such as memory, CPU cores, threads, execution priorities, and database and network gateways))

GARTNER Portability (PaaS only)

(Portability of the PaaS environment to other PaaS providers and multiple infrastructures (hardware, OS and virtualization systems)

GARTNER Demand fluctuation

(The terms of service should specify how fluctuations in demand will be managed, including:

- *provisioning and de-provisioning mechanisms*
- *the limits to expanding capacity (e.g., quota-based approach)*
- *the speed at which new computing or storage capacity (within applicable defined limits) can be allocated*
- *cloud service customer should be able to set policies for allocation of their resources (e.g., prioritisation, preservation))*

4.2 SERVICE LEVELS

According to emerging ISO definitions, a service level is 'a specific measurable characteristic of a cloud service'. 'Measurable' is a key element of this definition. If it is not measurable, it is not a service level. In this section we take a slightly wider definition, considering both measurable levels and other commitments. Much of this content is expected to be placed in the SLA as an attachment to the MSA.

This section refers to the SLOs, metrics and KPIs that can (or even need to) be used for defining the provided level of a service and measuring its performance. The C-SIG on SLAs refers to them as [19] "capabilities" and can be essential to the use of the cloud service from the perspective of the cloud service customer. The need for the definition of standardized units of measurements for cloud services (with consensus from the involved stakeholders) and their consistent incorporation in the SLAs is also highlighted by NIST [25]. NIST reports that the Cloud Service Measurement Index Consortium (CSMIC) has designed a framework in order to help cloud adopters select among the different SLAs, that involving 7 categories of measurements, each containing at least 3 attributes. These can be seen in Table 1. Some of them are discussed in this section while others (e.g., Security) are explicitly discussed in the following sections.

Table 1. CSMIC measurement categories and attributes

Category	*Question*	*Attributes*
Accountability	Can we count on the provider organization?	Compliance, Ease of Doing Business, Provider Certifications, Provider contract/SLA verification
Agility	Can it be changed and how quickly can it be changed?	Elasticity, Portability (legal and technical), Scalability (up and down)

Assurance	How likely is it that the service will work as expected?	Availability, Reliability, Resilience/fault tolerance
Financial	How much is it?	Acquisition, on-going cost, transition costs
Performance	Does it do what we need?	Functionality, Interoperability, Service response time, Suitability
Security and Privacy	Is the service safe and privacy protected?	Access control and privilege management, Data integrity, Data privacy and data loss
Usability	Is it easy to learn and to use?	Accessibility and learnability

4.2.1 Existing SLOs and Metrics

The following service SLOs and metrics have been identified in the literature. Where appropriate we add our findings from the questionnaire and literature search as well:

4.2.1.1 Accessibility

ISO 040 Accessibility component [/ Accessibility standards]
ISO 041 Accessibility component [/ Accessibility policies]

The C-SIG on SLAs refers to this SLO using the term "**External connectivity**" and describes it as the SLO that "specifies capabilities of the cloud service to connect to systems and services which are external to the cloud service. The systems and services involved may be other cloud services or they may be outside cloud computing (e.g. in-house customer systems)."[19]. Moreover, according to the Gartner report [31], the accessibility SLO needs to describe accessibility technologies supported for the service (e.g. text-to-speech, text magnification, etc.) and could also include a) the possible limits to global, continuous and ubiquitous accessibility and b) the management rules that a network provider (potentially 3rd party) must follow for network availability.

Clearly there is a difference in terminology used with respect to accessibility, in one sense related to technologies that can access the service, and in another that the service is accessible to users with handicaps. SLALOM should follow the ISO definition.

Accessibility in terms of handicapped users may be applicable particularly for SaaS services. Whether this should be a standard consideration or an additional selling point is open to debate and also subject to wider guidelines and obligations covered by national legislation. Additionally the accessibility tools considered here may be part of software not provided by the CSP, such as browsers, and so compatibility with these rather than tool provision may be more appropriate.

4.2.1.2 Availability

ISO 042 Availability component [Overall]
ISO 043 Availability component [/ Total downtime]
ISO 044 Availability component [/ Availability]
ISO 045 Availability component [/ Availability percentage]

CSCC states that testing a CSA with respect to the level service availability must be possible [20] while the C-SIG on SLAs defines the availability as "*the property of being accessible and usable upon demand by an authorized entity"* [19], highlighting the complexity of the work "usable" with the example of a service being up and available, but performing so poorly that it is effectively unusable. The DG Justice expert group expands the term of service availability to everything related to the actual functioning of the cloud service, i.e., the continuity of the service (the time for which the service runs without interruption), the quality of the service (e.g. response time in case of interruption, incident managements) and its functionalities (e.g. amount of data that can be processed, number of users that can access)[15].

The DG Justice group considers the clear and comprehensive (to all stakeholders) description of availability and its level imperative so as to allow the monitoring of the contract being respected. However, they report that this is not always the case: A survey held in 2013 showed that issues related to availability (in particular security and reliability) rank amongst the top disincentives amongst (potential) cloud users [32]. Users are currently insufficiently aware[2] of what kind of availability is offered by the cloud service provider. Many cloud contracts do not contain comprehensive clauses on the availability of a cloud service at all. For instance, a cloud contract may not contain any clause regarding response time in case of incidents. Where such clauses do appear in the contract, they are often insufficiently clear or non-committal. Consumers and SME's are likely to be either insufficiently aware what they can expect of a cloud product or are unsatisfied with the level of performance provided. **The way the promised contractual performance is expressed (obligation of means vs. obligation of result) is an important aspect for both the clarity and the fairness of the contract.**

Finally, DG Justice also presents two models for balancing and ensuring the interests of both parties (cloud users and cloud adopters) within a contract:

> a) The first model would require that cloud contracts contain certain minimum and clear information on the main services' characteristics, which would in any case be needed to improve the awareness of users on the offered level of availability; and b) the second model would be to guarantee a minimum level of availability based on the legitimate expectations of the cloud adopters, which is akin to the rules of conformity of goods in some Member States. This model would be part of every contract, as a 'best practice'. Such an approach is currently envisaged by the United Kingdom in the draft Consumer Rights Bill, which, inter alia, requires digital content to match certain quality criteria. These include fitness for all the purposes for which digital content of that kind is usually supplied freedom from minor defects, safety and durability. In both cases, the following considerations apply: a) end-users/consumers and small firms may have different interests; b) 'free' services generate in general lower expectations as regards availability of the service than paid services; and c) the expectations on availability may depend on the type of cloud service (e.g. IaaS, PaaS, SaaS).

[2] See the Report by Europe Economics 2011: Digital Content Services for Consumers: Assessment of Problems Experienced by Consumers 159, which in general mentions lack of information of the digital service as a problem

The SLALOM ethos is aligned with the suggested model (a), above. I.e that here should be standard clauses, with standard meanings present in every contract to facilitate comprehension, clarity and comparison, but does not in general agree with model (b), that specific values should be prescribed for any service level. SLALOM considers that market forces can and should, in general, dictate acceptable minimums.

Notwithstanding the above, SLALOM acknowledges the value of such legally stipulated minimums in other areas of commerce. SLALOM is not the competent entity to establish minimums in this case but should legal institutions do so, SLALOM would consider their future incorporation into SLALOM models.

Finally, for reference, Figure 2 presents how availability is currently defined in different SLAs according to an ENISA SLA survey report [22].

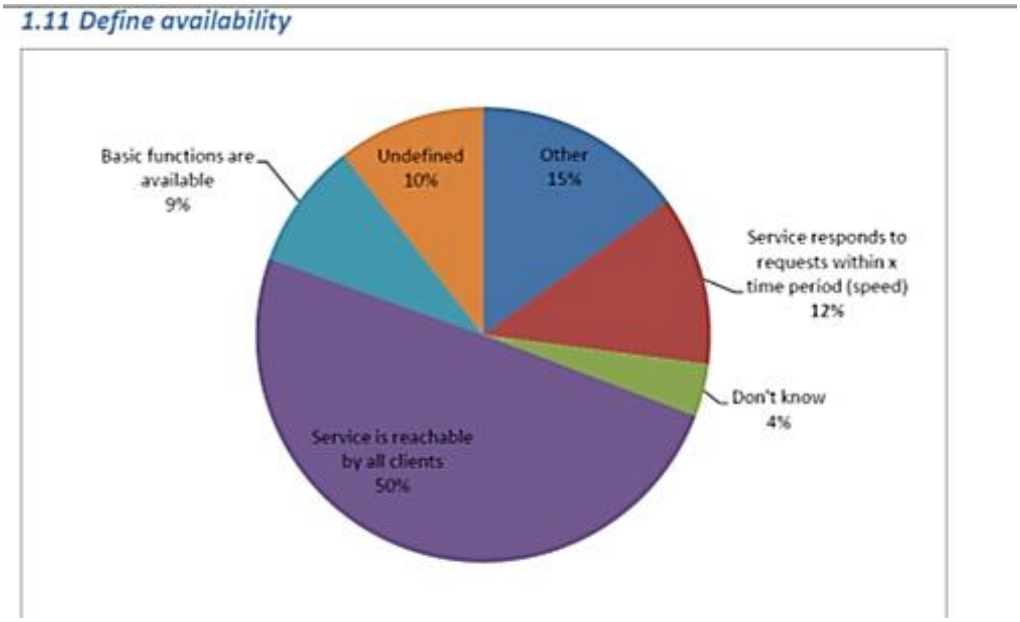


Figure 2. Availability definition is SLAs [22]

4.2.1.3 Uptime

ISO 046 Availability component [/ Uptime]
ISO 047 Availability component [/ Uptime percentage]

Uptime is one of the main aspects to availability and cloud adopters are recommended to pay attention specifically to the way it is calculated. According to best practices, SLAs are typically calculated monthly, and only consider the period during which the cloud adopter was a client of the cloud provider in the calculation of uptime versus downtime. However, there are also cloud providers that do not follow the approach of "best practice". On the contrary, they calculate the availability period starting 12 months prior to a client joining the service, with the assumption that the previous 12 months were delivered at

100% uptime (whether the cloud adopter was a client then or not) [24]. Therefore, the SLA should also describe the way that the uptime is calculated.

Another issue that needs to be dealt is the fact that it may be very difficult for an end-user/consumer or a small firm to demonstrate that a cloud provider has not worked with reasonable care and skill to achieve a certain level of availability, including in particular the amount of uptime a month [15]. The Ministry of Justice guidance on Cloud Computing and CJSM [29] points towards the same direction: i.e. the need for understanding how the percentage of availability is calculated. It additionally emphasises the importance of the definition of "up", e.g., a cloud system may be "up" according to an SLA if a number of features are unresponsive provided that core systems are available.

SLALOM clearly needs to consider the period of calculation, the definition of 'up', and how it is calculated, monitored and reported.

4.2.1.4 Downtime

ISO 048 Availability component [/ Allowable downtime]
ISO 049 Availability component [/ Downtime]

Whilst the literature source note the obvious necessity of maintenance on the systems, which might result in downtime, there is discussion of how it should be approached. The Cloud Standards Customer Council's practical guide suggests cloud adopter to ensure that there is a mechanism to inform them of changes and, if not, amend their contract to put the onus on the provider to provide reasonable advance notice of updates so that they are aware of the downtime of their service [20]. Again the **importance of defining the measurement window is raised.** Dimension data's white paper [24], apart from hard downtime, also poses questions related to the performance degradation. In particular the white paper states that under 'best practices' "*cloud SLAs should cover both unavailability (hard downtime), as well as performance degradation. Many providers offer clear SLA language explaining what happens if their infrastructure goes completely offline, but fail to mention whether performance degradation is also considered an SLA violation*." They suggest cloud adopters ensure that performance degradation and unavailability are both covered in the SLA. Moreover, it advises cloud adopters to be cautious with respect to the issues coming from the complexity of the cloud architectures: "*A simple server-only uptime SLA fails to address one of the most important components of cloud architecture, namely the network. Consider the implication to your business should network performance vary widely. Is this something you can easily architect around? You should have a clear understanding as to whether the provider guarantees network performance as well as uptime performance*." The same whitepaper points out that some cloud providers mandate that numerous 'availability zones' or 'regions' need to fail for them to consider the failure an SLA violation and propose cloud adopters to also ask for some SLA against failures of their cloud product in a single location as well.

Feedback from SLALOM respondents confirmed these problems. From the CSPs, one commented that '*We had to make the Availability SLAs a quarterly measurement instead of monthly.*'

'Customers don't often realize the difference in actual downtime. Performance SLAs are very difficult to meet due to many aspects of the network that are beyond the SaaS provider's control'.

Indeed the responsibility for aspects outside for their sphere of influence was repeatedly described by CSPs: *'The reliability of third party service - such as connectivity. … 'Managing client expectations. Many operate imperfect legacy systems and yet expect cloud technology and its purveyors, integrators and SaaS providers to provide 100% up time.' … 'You can be asked to put something under SLA that you would never be asked in traditional process - over-expectation'*.

One CSP saw the demand for end-to-end SLAs as detrimental overall – [the] '*Customer wants to measure end user experience, which is highly variable. So we have to set the bar low, yet only a small percentage of users really fall under this category of likely poor performance*'.

Downtime and Uptime are clearly related aspects. It appears fair to allow CSPs to define a certain level of downtime for planned maintenance and to exclude this from the uptime window. Effectively then uptime SLOs would be a commitment to avoid unplanned maintenance (outages and so on) whilst downtime SLOs would be a commitment to optimise and reduce planned maintenance. Conditions could be placed on the downtime component (such as advanced warning) that separates it from unplanned outages and maintenance. As for uptime, the period, calculation, definition, monitoring and reporting should all be considered.

4.2.1.5 Response time

ISO 050 Cloud service performance component - cloud service response time component [Overall]
ISO 051 Cloud service performance component [/ response time observation]
ISO 052 Cloud service performance component [/ response time mean]
ISO 053 Cloud service performance component [/ response time variance]
ISO 054 Cloud service performance component [/ Nth percentile of response time]
ISO 055 Cloud service performance component [/ Cloud service response time over threshold]
ISO 056 Cloud service performance component [/ Delay duration time]

C-SIG: Maximum response time,
C-SIG: Percentage of successful requests
C-SIG: Percentage of timely service provisioning requests
C-SIG: Level of redundancy
C-SIG: Service reliability

The C-SIG on SLA's guidelines [19] report on varying perspectives regarding the response time SLOs and the point at which the cloud adopter stimulus is measured: the measurement of the response time may start when the cloud adopter initiates the stimulus on their device, or it may start when the request from the cloud adopter arrives at the cloud service provider's endpoint – the difference being the network transit time, which may be outside the control of the cloud service provider. Similarly, the point at which the response is measured can vary. The fact that many cloud services support multiple different operations and that it is likely that the response time will differ for the different operations is

also highlighted within the same report and thus, it is suggested that response time SLOs need to clearly state which operation(s) are concerned.

SLALOM should consider this carefully. Whilst adopters demand end-to-end SLAs, and providing them would be a competitive advantage for CSPs, the CSPs are reasonably demanding to limit their own risk to factors under their control. The balance here requires further investigation.

ISO 057 Cloud service performance component - cloud service capacity component [Overall]
ISO 058 Cloud service performance component [/ Number of simultaneous cloud service connections]
ISO 059 Cloud service performance component [/ Limitation of available cloud service resources]
ISO 060 Cloud service performance component [/ Cloud service throughput]
ISO 061 Cloud service performance component [/ Cloud service bandwidth]

ISO 062 Cloud service performance component - elasticity component [Overall]
ISO 063 Cloud service performance component [/ Elasticity]
ISO 064 Cloud service performance component [/ Speed]
ISO 065 Cloud service performance component [/ Precision]

Finally the Gartner report [31] for the European Commission also refers to:

> *Network aspects* mentioning that a) network latency avoidance strategy for the cloud service need to be documented within the SaaS terms of service; b) SaaS terms of service should specify the throughput and latency between Internet point-of-presence for specified geographies and the cloud service; and c) SaaS terms of service should provide guidance on network requirements for the cloud service customer. The need for including network availability and latency aspects has also been highlighted from the CSP answers in the SLALOM questionnaire. Moreover, according to the feedback received through the SLALOM questionnaire, CSPs propose to expand performance not only by geographic location due to high variability (e.g., Russia & China may have 10x worse performance than users in USA) but also tie it with use experience.
>
> *Enterprise integration in the case of "hybrid IT" environments* for which the services description needs to include interoperability with legacy systems and should include a) secure extension of the user organization's WAN, b) features for data migration between the cloud service and other user environments and c) features for migrating workload features between the cloud service and other user environments
>
> *Scaling aspects* such as a) the possible scaling limitations (common), b) load balancing (optional), c) auto-scaling (optional), d) resizing of existing VMs (e.g., speed of resizing, limitations) (optional) and e) speed of provisioning additional VL's or storage units (optional). The need for including scaling aspects within the contract is also supported by the questionnaire feedback with respect to the missing measurement from the ISO work.

Feedback from the SLALOM questionnaire supports proceeding with the proposed metrics model approach. There are significant challenges because practical worked examples of ISO (or C-SIG) metrics are unavailable at present. ISO is still developing its proposals for how metrics should be specified, SLALOM proposes to follow. However, the goal of having something which can be automated is an important one.

Although there are potentially a large number of metrics which can be incorporated into SLAs;

- The number of measurable metrics (for use with service level objectives) is significantly less than the number of components which are identified in CD1 of the ISO SLA standard 19086-1. This issue refers to the distinction between SLOs and 'service commitments' (effectively contractual clauses with commitments which are not measurable in the sense of service levels, as generally used in this document). ISO (SC38 WG3) is working on this issue at present.
- There is a clear prioritization amongst CSPs and Adopters for specific metrics, or groups of metrics, as follows:
    - Availability (e.g. uptime and downtime, planned and unplanned) – consistently the highest priority metric
    - End-to-end responsiveness/throughput [particularly wanted by Adopters, but seen as difficult by CSPs because of third-party providers beyond effective control, with geography a significant factor]
    - Response time for one-off issues [e.g. time to provision; to respond/resolve to service interruptions or to support requests]
    - There is repeated emphasis on the need to keep things simple; and that too many metrics are unrealistic and impractical
- There is furthermore support for using a data exchange format (such as XML) for metric specifications

It is therefore proposed, for the purposes of SLALOM's final deliverables, that detailed specifications are developed for only a limited number of core metrics, principally in the three priority categories cited above. For further details of the metric prioritisation see section 5.

4.3 VARIATION OF THE SERVICES;

Both the ECP C-SIG group and the CSCC guide highlighted the need for service variations to be communicated to the adopter in a timely fashion, and suggested associated SLOs. Many current contracts state that the service description and levels can be modified, unilaterally and at any time by the provider. In the context of other service interruptions, discussion in the literature has covered the differences between free and paid services. This can be extrapolated to cover this point: that is what is a reasonable expectation from the adopter is dependent on the type of service they are using (and its impact on the adopter) and the cost they are paying for the service.

A specific remark on software versions was made by the DG Justice expert group in their paper Liability For Non-Performance Including Remedies [16]. Where software is provided by the CSP (including third

party software), the CSP may "push" updates. Although this is a different situation to changes in the service level (as in theory it is beneficial to all parties), the DG Justice group considered that "the [MSA] should require that the customer be given advance notice of the update. The customer should have the ability to opt out, or at least to defer the update. However, the supplier may be unwilling to continue to support older versions indefinitely, and there should be a legitimate exception for updates that correct serious security vulnerabilities".

The Ministry of Justice [29] guidance suggests that adopters be mindful of potential expansion plans. They suggest that professional CSPs should enquire about these, and that the two parties should be clear of any prices or policies relating to increasing or decreasing service requirements. However this is not formulated as a service level commitment and is likely to only apply to a subset of cases.

4.3.1 Service level objectives and commitments

C-SIG: Cloud service change reporting notifications
C-SIG: Percentage of timely cloud service change notifications

4.4 OBLIGATION OF THE USER

This chapter may also refer to an acceptable use policy as an attachment to the MSA.

Although many sources identify the Acceptable Use Policy as part of the contract or MSA, none of the studied literature documents raised any points of discussion on it.

The SLALOM questionnaire did identify that from the perspective of the CSP, adopter education was wanting, particularly around their responsibilities for managing risk. This observation does not necessitate any contractual changes – the contract should unambiguously declare the responsibilities of the CSP and other risks not shouldered by the CSP are naturally the responsibility of the adopter. However it is perhaps a suggestion for CSPs and industry forums and experts to offer clear guidance to potential adopters.

SLALOM therefore concludes that existing AUP clauses are not problematic to either party.

4.5 CONSIDERATION

Consideration refers to payments, pricing policy and so on.

Multiple SLALOM questionnaire respondents identified that the emerging ISO standard currently has no section on payments *'(payment terms, indexation, consequence of non-payment …)'.*

Both the Cloud Industry Forum's Code of Practice 0 and the Gartner study for the C-SIG [30] identified the need for these to be clear and ambiguous in a contract.

The above sources suggest that the following items be considered in a pricing component:

- Pricing policy (basis of charging with fully-declared costs)
- Payment terms
- An allocation based charging model (by user, transaction, GB, etc.)
- A defined price band list per consumption volumes (i.e., price associated to different volume levels)
- Full transparency on how pricing is calculated (which metrics/formulas are applied for calculation)
- Pricing according to SLA requirements

SLALOM should produce a payment module considering the above. As there is scant information available, SLALOM may wish to seek further advice from the stakeholders.

4.6 TERM AND TERMINATION; CONSEQUENCES OF TERMINATION AND EXPIRATION;

The discussion in this section is broadly drawn on references [18]**Error! Reference source not found.**[20][22][27][28].

The duration of the contract and the process for renewal and/or termination should be clearly set out in the SLA, as well as the causes that would lead to the premature termination of the same before the agreed on term. In short, an exit clause is required of all agreements, detailing obligations of each part upon termination of the contract.

From the literature it transpires that the conditions of termination are not always clear as regards the recovery of user data, the format of such data upon termination of the contract, and who bears the costs for transfer (either to the user or switching to another CSP), or the final deletion of the data. The cost may vary depending on the causes of termination and the conditions of the service provided (“free” / pay). Further, if the termination is caused by breach by either part, there are issues of penalties and indemnification.

CSPs should outline clearly if they guarantee portability or not, and under what (economic) conditions. It seems that contracts generally do not foresee the obligation for the cloud provider to cooperate with a new cloud provider in case of switching, although a recent French court case has applied ”good faith” to oblige a CSP to aid a user transfer data to another provider (Tribunal de Grande Instance de Nanterre, 30 Novembre 2012).

Switching may imply important costs linked to the transfer of the data, depending on the type of data involved (copy or full migration, etc.) and logically a CSP will want to pass on to the user such costs or some part of them. Here some of the sources considered that a distinction could be drawn taking into account the motives of the user for switching. If they are “independent of their sphere of influence” (e.g. the bankruptcy of the cloud provider, the modification of the contract by the provider), then the user should not bear the associated costs. If on the other hand, it is due to convenience (better service, price, etc.), then this would justify that the user bears the costs of porting data. Further, in the case of free services, the CSP should not bear costs related with return of data to the user.

As a matter of general practice, it seems that the costs for recovery of data are borne by the user, and the costs of deletion at the termination by the CSP.

There may be variation in national rules default conditions applying to termination of cloud computing contracts, also including typology of contracts (services, lease, etc.) but often there are not specific clauses on what has to be done with the data, nor a clear obligation to return the data to the user or aid in switching to another CSP. For the CSP, transfer of data (or deletion) implies costs and so helping users transfer data is often seen as an extra service that can be offered for a fee to users in addition to the cloud service itself, rather than an obligation of service.

Time for preservation of data varies considerably. Some providers will retain the data of the user after termination of the contract, (often 30 days) for users to access and retrieve data. Some expert groups considered it essential that cloud providers give advance notice and allocate a sufficient period of time to users to retrieve their data, including free services. As regards free vs. paying CSP, some CSP may have clauses that service can be discontinued and the data can be deleted with no forewarning after a period of inactivity, but this may be considered disproportionate behavior on the part of the CSP, as this triggers a risk for the user to lose their data stored on the cloud.

The format of the data and metadata is also an important issue as there may be changes in format due to the amount of time elapsed between start and completion of the service, and so “standard” formats should be adhered to.

If the termination is due to a breach of contract by the CSP, such as consistently not meeting agreed on SLAs, then there is wide consensus that there should not be costs for the user. There are other situations, while not considered breach, that may lead to the termination of the contract, for example if the CSP is bought by another entity, or changes the terms of the contract, then perhaps the user should be able to decide to continue or not the relationship without penalties for discontinuing.

If the cause is a breach by the user including breach of terms, non-payment or insolvency of the customer or not respecting the Authorized Use Policy, then several groups considered that the CSP has justification to stop the service provision. That said, the DG Justice expert group consider that data should not be held “hostage” in disputes.

Data protection legislation needs to be taken into account in the termination process. After allowing time for the user to recover the data (generally 1-3 months), the CSP has to delete the data or render it unintelligible in order to comply with EU data protection rules. The Cloud standards customer council recommends that the user require written confirmation that their data has been completely removed from the provider’s IT environment and that the CSP agrees not to use the customer data for any reason in the future, including for statistical purposes. If after termination of the contract, the CSP store the data without the customer's consent, they risk being liable under data protection rules (Article 6 (1) (e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 0281)).

In conclusion, the consensus in the literature is that users should be confident on what will happen with their data on termination of the contract while Cloud Providers should not be overburdened with disproportionate obligations

From the questionnaire, we determine that (despite the SLOs given in the next subsections) respondents considered that ISO insufficiently deals with this issue. Comments included: ('[ISO is missing] *Termination of service component: Deleting derived and customer data?*', '*Service cancellation rights for both parties*', '*Agility to integrate a service (or to stop a service). Associated: portability and reversibility*'.

From perspective of CSPs the '*Exit and portability of data'* was considered a complicated point to negotiate, as was '*Termination for Convenience*.'

4.6.1 Service level objectives and commitments

Of the SLOs, via the questionnaire the overall Termination of service component was ranked 11th overall across all users, and relatively higher for CSPs than other respondents, and the return of assets was ranked 19th priority overall. Further we had noted that ISO is missing component of deletion of data.

068 Termination of service component [Overall]
069 Termination of service component [/ Notification of service termination]
070 Termination of service component [/ Return of assets]

SLALOM should seek to cover all of the issues discussed above: duration, exit clauses (when and how a premature exit can be realised by each party), the outcome of the three data types identified in section 4.8, including under what conditions the CSP will store them, provide access to them after termination, ensure portability and so on. SLALOM should consider whether the type of service / business model is relevant. For example in free services is it fair to charge for data portability? SLALOM should also consider whether the data outcomes should be in anyway dependent on the reasons for termination.

Factors on the CSP side include cost, legality (especially the implications of storing or manipulating data after contract termination) and leverage: clearly 'hostage' data provides leverage that can be used both justifiably and egregiously. On the adopter issues such as privacy demand deletion policy, to avoid lock-in requires some portability, and trust and security require the ability to get data out of a cloud

4.7 SUBCONTRACTING and THIRD PARTIES

Subcontracting was an issue that has emerged significantly both in the literature review and the questionnaire. It is a particular concern for adopters. As this is largely untouched by ISO, this was unforeseen by SLALOM and further investigation of the issue may be necessary.

Firstly there was a desire to know who the third parties were. One adopter stated in the questionnaire that this was their biggest MSA pain point: '*Use of 3rd parties by main contractor: who are they and*

where are they?'. Both the DG Justice expert group (in their paper Data "Disclosure and Integrity" [13]) and the C-SIG on the Code of Conduct (in the meeting of 12 February, 2014 [27]) stated that a list of subcontractors should be made available to adopters and kept up to date. The latter stated that all subcontractors should be listed with special regards to those who were not involved in the main data processing but processed data for minor data processing purposes. At the same time they did note that "business flexibility should also need to be taken account". The former also noted that this may be a legal requirement under the data protection requirements of the adopter to their users. They went on to note that "The processing of certain special categories of data may require compliance with specific regulatory provisions, which may not be covered by standards or certifications schemes of general application. Therefore, it should be specified within the service agreement the possible special categories of data that the service is suitable for".

Secondly there was an issue of how much responsibility the CSP would accept for their subcontractors. The questionnaire results highlighted a definite desire by adopters for end-to-end SLAs. Naturally the CSPs resisted calls for end-to-end SLAs based on technical grounds (e.g. reliance on a carrier's connectivity or geographic issues). The CIFs code of Practice 0 has that the CSP should state the extent to which it accepts indirect responsibility for its suppliers, For example: for the technical failure of vendors in the supply chain such as collocation where services are taken off-line. Similarly the CIF COP considers that there should be a statement about the extent to which the organization's suppliers accept indirect responsibility to the CSP's customers. [This covers e.g. the situation of the organization itself going out of business.] For example: if the organization aggregates third-party services that are on-sold to the organization's customers, do the third-party supplier contracts offer reciprocal terms and protections e.g. liability, service level resolution, data protection?

Thirdly, it has been suggested that standardisation and having subcontractors obliged to be certified can help with this issue. The Cloud Security Alliance Control Matrix may address this topic.

Finally, a related issue is the use of third parties within the CSP's group and the uncertainty of what disclosure was necessary or desirable here.

In conclusion, the desire to know who third parties are and where they are based, coupled with a potential legal requirement to do so indicates that the **SLALOM terms should address this issue**. Clearly end-to-end SLAs are highly desirable but have cost and risk associated with them for the provider. Given the market value of this, it could be seen as a differentiating factor for some CSPs. **SLALOM may want to consider this as an optional clause**.

4.8 INTELLECTUAL PROPERTY; CONFIDENTIALITY OBLIGATIONS; DATA PROTECTION;

Issues relating to data protection, confidentiality, privacy, data access, intellectual property rights and data deletion are of top concern to adopters and by far the most written about of any of the chapters of the MSA as presented in this document. According to [28] over 66% of respondents claimed data security was their biggest concern in the cloud. This issue is complex, involving different aspects of law (chiefly data protection), perception, technical and organisational security measures and CSP policy.

It is important to distinguish between different types of data as both what is reasonable and what is mandatory or permitted depends on this. Three broad categories can be considered [13]:

(a) Content supplied to, or generated by, the cloud service by users;

(b) Attributes data or meta-data generated through use of the service, and

(c) Subscriber or user data identifying characteristics of those authorised to use the service.

Depending on the contract, the CSP may act as a *data controller* or *data provider* with respect to this data. As controller or joint controller, the Provider's obligations in respect of data integrity and disclosure are governed by national law implementing Directive 95/46/EC, as well as any contractual obligations accepted or negotiated between the Provider and its customers. Data disclosures require a legitimate basis (arts. 7 and 8); while obligations with regard to data integrity can be found primarily in the principles relating to data quality (art. 6) and the security of processing operations (art. 17). As a processor, the Provider may not necessarily have direct regulatory obligations under Directive 95/46/EC, but must at least be subject to contractual obligations vis-à-vis the controller. Those obligations are to process the data only in accordance with the instructions of the controller and to implement appropriate technical and organizational security measures [13].

4.8.1 CSP's access to data

Probably the biggest subtopic in this chapter, in terms of stakeholder concern, is related to what access to data CSPs and their subcontractors may have. These in turn stem primarily from the conditions of the MSA that permit CSPs to use the data. **Our research shows the need of MSAs to be open and clear about what it will do with each of the data types discussed above**. [13] has commented on the difficulty of deducing data use from relevant security and data protection certifications. This information must be made explicit. Similarly the contract must not try to skew the discussion towards a narrow definition: As the document 'Liability For Non-Performance Including Remedies' [16], prepared by the DG Justice Expert Group, remarked: Data privacy in a cloud context is not just about the protection of the information about the customer's agents in its dealing with the provider (this is the narrow meaning in many existing Service Level Agreements), it also includes the privacy of the information that may be stored about the customer's own customers. The SLALOM questionnaire showed that Adopters are very clear on this point.

Besides confirming the adopter concern (One adopter's main issue with MSAs: *'Where data is stored, who has access to the data?* ', the questionnaire also received comments from CSPs on the subject. One wrote: '[SLALOM should] Clarify exactly what type of access cloud provider has to customer data (e.g. purely for customer support, or also product management to improve product). Some cloud providers gather detailed metrics, even if in aggregate, that customers often are not aware of. I don't think it's a bad thing to collect this data, but customer should be informed'. A second wrote: 'my main problem with MSAs is buyers assuming we can access and see their data. For IaaS, this simply isn't the case.'

Research by the DG Justice group, reported in the document “Control And Use Of Content”[17] showed that while most providers explicitly recognise that the user "owns" their content, most of them ask for more or less broader authorisations to use and control it. Some providers ask for a restricted permission to access the content merely for the technical purpose of providing the service and others also ask for permissions for broadly defined commercial and marketing purposes. Examples from that document include MSAs securing the customer's permission for data use with no time or geographical limitations and extended to a wide range of third party traders. Some contracts remain silent on the question of how the provider will use the customer's content.

From a user perspective the key issue seems to be the extent to which customers have to permit the provider to use their content for reasons other than the provision of the service. In order to access the service the customer has often to permit the use of their content for all purposes intended by the provider [17]. The DG Justice Experts [14] were critical toward contractual clauses granting authorisation to cloud providers to use the user's content for any purposes. These clauses were seen by some experts as potentially unfair as they give too broad rights to the provider. Taking a tougher stance, the Ministry of Justice guidance on Cloud Computing [29] categorically advises cloud adopters to get “assurance that the information will be treated as confidential and not used or disclosed to third parties. You should retain full ownership, in terms of intellectual property, in relation to the data that it is stored on your provider's system. You should have an explicit right to get your data back on demand”.

The experts noted that even detailed terms of service describing the authorization sought by the CSP were often uncertain, in part because they contravene applicable national rules relating to confidentiality, IP rights, consumer or general contract law.

The adopters’ hesitation to sign up for services with unclear data management and use policies is natural because privacy and commercial confidentiality issues are legitimate concerns, and often obligations on the adopter. Furthermore, in some circumstances data on the use an adopter makes of a service may itself betray trade-secrets (data type (b), above), and so it is a legitimate expectation for this to be confidential [30].

A final point raised in discussion of the topic is the frequently reserved right to disclose data in urgent circumstances. This may seem sensible where there is a clear and immediate need to disclose in the public interest or to preserve life. However, as commented in [13], there is a spectrum of approaches to disclosing in other circumstances, from retaining a broad unfettered discretion to obligations to act in ‘good faith’ or on a ‘reasonable’ belief. The relevant interests may generally include the Provider’s own interests as well as those of third parties. That discussion went on to remark: “*Given the publicity over Microsoft recent decision to access a user’s Hotmail account in the course of an internal investigation, it should also be borne in mind that a disclosure to a third party, e.g. a law enforcement agency, may be preceded by unilateral access by the Provider rendered permissible under the terms of service”*. This issue is related to access by law enforcement, which will be discussed in detail below.

The DG Justice subgroup specifically looking at this issue proposed [17] that cloud services could have multiple options relating to CSP data use, avoiding an "all or nothing" approach. This could be useful for specific professions such as health or legal and would probably be premium services.

A final note is on the commitment of the service provider to support of e-discovery (litigation support), potentially with data it has generated (data types (b) and (c)). In Gartner's report for the C-SIG [30] it was suggested that the CSP should be acknowledge whether it will commit to this.

On consideration of the above, the SLALOM terms must ensure that the permitted uses of the three categories of data are crystal clear for both parties. The assignation of data controller and/or processor to the parties should be clear. Any exceptions to the confidentiality clauses should be explicit and not rely on interpretation. Given the wide array of cloud services, of data types and business models, SLALOM should not be prescriptive in denying CSPs the ability to fund a business model off the use of adopter data or metadata, whether as part of a freemium model as hinted by the DG-Justice group, or a CSP's only model.

4.8.2 Data protection

The second major issue in this chapter relates to data protection, regarding the legal obligations of the parties, the security measures necessary and the responsibility for data integrity. Several SLALOM respondents, both Adopter and CSP described this as the key problem with MSAs. One respondent lamented the lack of transparency, and the need for a leap of faith: "*a big binary jump forwards: either you accept that your data are somewhere secure on the providers infrastructures, or.... - you accept the higher price of "on premise" services, with a CAPEX model that creeps in with this "traditional model"*.

The level of protection required varies according to the type of data and the type of user, and in some cases, the profession. There are organisational and technical security measures that must be in place and legal obligations on both parties.

4.8.2.1 Legal obligations

As pointed out by the C-SIG on SLAs [19], adopters, as *data controllers*, must accept responsibility for abiding by the applicable data protection legislation. Notably, the cloud service customer has an obligation to assess the lawfulness of the processing of personal data in the cloud and to select a cloud service provider that facilitates compliance with the applicable legislation.

Consequently, only if the provider informs the customer about all relevant issues, the cloud service customer is capable of fulfilling its obligation as data controller to assess the lawfulness of the processing of personal data in the cloud (e.g. data protection codes of conduct, standards or certification schemes). Moreover, the cloud service provider shall make available the information that enable the customer to provide the data subjects with an adequate notice about the processing of their personal data, as required by law.

The cloud service provider, in its capacity as *data processor*, should inform the adopter, in the most expedient time possible under the circumstances, of any legally binding request for which the provider is

compelled to disclose the personal data by a law enforcement or governmental authority, unless otherwise prohibited, such as a legal prohibition to preserve the confidentiality of an investigation

Notably, transparency in the cloud means 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 (see discussion in section **Error! Reference source not found.**). These points were also raised by [13].

In light of this, SLALOM clauses must ensure that both CSPs and Adopters can fulfil their legal obligations under data protection law, each obliging the other party to disclose any necessary information to adequately assess their compliance.

4.8.2.2 Security

Beyond compliance with the security obligations laid down in national and European legislation, the various literature sources have identified additional data security issues that should be considered. (Note see section 0 for the full discussion on security).

The C-SIG on cloud SLAs guidance [19] recommends that CSP provide "*documentary evidence of appropriate and effective measures that are designed to deliver the outcomes of the data protection principles (e.g. procedures designed to ensure the identification of all data processing operations, to respond to access requests, designation of data protection officers, etc.)".*

The cloud service provider must notify the cloud service customer in the event of a data breach that affects the customer data. To this end, the cloud service provider shall implement a data breach management policy which will specify the procedures for establishing and communicating data breaches".

However, the DG Justice expert group in [13] explains that identifying causes of integrity breaches can be extremely complex, especially in a multi-tenanted environment. It considers that In such situations, *"public law intervention may be required to assist consumers to recover any harm or loss suffered, ranging from the imposition of strict liability to evidential presumptions"*.

Given the importance of simplicity urged upon SLALOM by its respondents, and the complex nature of this issue, the model clauses should avoid a prescriptive solution.

4.8.2.3 Data Integrity

The following sis taken from the Discussion Paper: "Data Disclosure and Integrity" produced by the DG-Justice Expert group [13]:

> *Data integrity is concerned with ensuring that the data processed by a Provider on behalf of a customer, or on the Provider's own behalf, is secured against unauthorised destruction, loss or modification, whether resulting from deliberate, inadvertent or accidental actions of the Provider or a third party, including other users of the cloud service.*

The term data integrity is sometimes used to encompass all forms of security breach, including loss of confidentiality and availability.

In the Cloud Legal Project's 2010 and 2013 surveys [30], it was found that the majority of Providers placed responsibility for the integrity of customer data with the customer.

Some Providers promised to use their 'best efforts' to preserve customer data, but still disclaimed responsibility for data integrity.

Customers are also recommended to take various steps to address data integrity concerns; from the use of encryption to making back-up arrangements (which are sometimes offered by the Provider at additional cost): e.g. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content (AWS).

Providers usually incorporate provisions recognising a general commitment and obligation upon them to implement and maintain 'industry-standard', 'reasonable' or 'appropriate' security measures.

Although this is a data protection obligation on controllers, the appropriate mechanism for dealing with this is through back up and security, which are dealt with in chapters O and O, respectively. SLALOM recommendations will be made in the relevant chapter.

4.8.3 Data Deletion

(see 4.8.7.2 under 'Service level objectives and commitments', below)

4.8.4 Data Location

(see 4.8.7.3 under 'Service level objectives and commitments', below)

4.8.5 Law enforcement access.

(see 4.8.7.1 under 'Service level objectives and commitments', below)

4.8.6 Other issues

A variety of other issues were picked up by the various sources, relating to movements in third party countries and variations of service. One SLALOM respondent (adopter) noted that 'For Public Cloud, Compliance rules: Data Location & Direct audit possibility' was a burning issue. This will be dealt with under the discussion on data location (below) and audits and certifications (section 4.14, compliance). Several questionnaire comments touched on whether much of the issues around data protection were to do with perception. For example, one CSP commented: 'Cloud computing contracts are nothing different from managed services / outsourcing services contracts except that customers are very conscious about data privacy and data security related issues'. Another, as previously mentioned,

complained that adopters incorrectly assumed that (in IaaS) the CSP could access and see all their data, and stated that increased education was necessary. Finally, variability across customers was seen as an issue by one SLALOM respondent in particular. The CSP commented that '*Varied customer requirements for security, incident response, or privacy. Privacy is likely the biggest pain point due to variations in enforcement by different EU countries (e.g., German DPA registration requirements versus other countries).*'

4.8.7 Service level objectives and commitments

One clear feedback from the SLALOM questionnaire was that the data management component of ISO had too many sub-components and that there was a need to rationalise. Another, this time a CSP noted that 'The length of time that potential customers take in looking at, and getting comfortable with, new areas of control within the contract - for example, controls on data access and location of data [is the biggest problem with MSAs]'.

The following present an extensive list of SLOs and commitments, compiled across the sources. **SLALOM will have to prioritise and reduce this list in order to comply with the need for simplicity and clarity.**

ISO 066 Protection of personally identifiable information component [Overall]

ISO 107 Data management component [Overall]
ISO 108 Data management component [/ Intellectual property rights component]
ISO 109 Data management component [/ Cloud service customer data component]
ISO 110 Data management component [/ Cloud service provider data component]
ISO 111 Data management component [/ Account data component]
ISO 112 Data management component [/ Derived data component]
ISO 113 Data management component [/ Data portability component]
ISO 114 Data management component [/ Data examination component]

C-SIG: Data portability format
C-SIG: Data portability interface
C-SIG: Data transfer rate
C-SIG: Processing purposes

4.8.7.1 Law enforcement access

ISO 115 Data management component [/ Law enforcement access component]
C-SIG: Number of customer data law enforcement disclosures
C-SIG: Number of personal data disclosure notifications

All providers state that they will disclose customer data in response to a valid court order (Note that valid does not mean legally binding or enforceable) [13][17]. This legal under the exceptions to the data processor obligation, and in some circumstances as a controller.

The DG JUSTICE expert group recognized some of the difficulties with the wording of these clauses. For example: in the case of a clause that would enable CSPs to disclose data "in response to a valid court order". Here, the use of the wording "valid" can be criticized as vague. The experts considered that CSPs in case of law enforcement requests of disclosure cannot be expected to check the lawfulness of the request – they should merely check the procedural compliance of the request [14]. Furthermore the experts identified that the definition of "urgent" is problematic and could be used widely by law enforcement entities.

According to the Discussion Paper: Data Disclosure and Integrity [13], in the case of petitions from third countries, "*considerable controversy exists as to the … 'legal requirement', …[it] is arguably not enforceable against a processor established in a Member State".*

Finally, both the above source and the C-SIG on SLAs [19] consider that "*prior notification of any such legal request, where legally permissible, to enable the customer to take steps to challenge any such request*", and [the CSP]"*should inform the customer, in the most expedient time possible under the circumstances, of any legally binding request for which the provider is compelled to disclose the personal data by a law enforcement or governmental authority, unless otherwise prohibited",* respectively.

Clearly this is a thorny issue for SLALOM and guidance should be sought from the expert groups who have debated the issue. The C-SIG suggested SLOs in this regard seem inappropriate: the objective of both parties is clearly to have no disclosures. If required by law, it would not seem fair to deem the CSP to have breached the SLA, when almost certainly it would be down to suspicions on the adopter.

4.8.7.2 Data Deletion

ISO 116 Data management component - data deletion component [Overall]
ISO 117 Data management component [/ Data deletion process]
ISO 118 Data management component [/ Data deletion notification]
ISO 119 Data management component [/ Data deletion time]
C-SIG: Temporary data retention period
C-SIG: Cloud service customer data retention period
C-SIG: Percentage of timely effective deletions
C-SIG: Percentage of tested storage retrievability
C-SIG: Data retrieval period
C-SIG: Residual data retention
C-SIG: Data deletion type;
GARTNER Data Stewardship
(who controls the different types of data, how will it be managed, how is it secured)

Several sources commented on the importance of clear data deletion policies. However notably only one respondent to the SLALOM questionnaire mentioned this, and then in relation to termination.

The C-SIG on SLA's has proposed an SLO on general data deletion, commenting that the terms are often difficult to extract from MSAs, and that it may be of interest to "*be able to retrieve data after a deletion*

request has been posted and to have SLOs associated with that [19]". They considered it mandatory to have personal data deletion provisions. Furthermore they considered it mandatory that the clause covered all locations and all instances, including previous versions, temporary files, etc. and that those files become irretrievable. Finally they noted that "*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 (See Article 29 WP Opinion, par. 3.4.3.5)*".

Beyond general deletion, most of the literature discussed data deletion at the termination of the contract. This is covered in depth in section 4.6). The emerging consensus among the experts appeared to be that it was unfair to swiftly delete or prevent removal of adopter's data from the service after termination by the CSP, yet at the same time the data should be removed when the adopter terminates the contract. At the same time, it is clear that upon termination the CSP can be exposed to liabilities if they do not delete the data. For example, there is a conflict where the customer stops paying, where the data is alleged to be unlawful or where the provider terminates the service. Many sources suggest a time window prior to data deletion. For example 30 days is recommended in 'Best practice in Cloud Contracts' by DMH Stallard & CIF [28]. Experts commented that data should not be held "hostage" in the case of disputes.

Finding the compromise between what is fair for CSPs and fair for Adopters is complex and probably context dependent. As the majority of the discussion is contained in section 4.6, SLALOM recommendations will be made there.

4.8.7.3 Data Location

ISO 120 Data management component - data location component [Overall]
ISO 121 Data management component [/ Data location]
ISO 122 Data management component [/ Data location specification capability]

Data location was a key area of interest both to expert groups and SLALOM questionnaire respondents. Data location was listed as the main problem with MSAs by several CSPs and Adopters. In some cases the qualification statement implied this was a legislation/compliance issue, with one respondent noting that location was important due to variations in data protection enforcement in different EU countries. In others it seemed more a general concern about losing control ('Where data is stored, who has access to the data? ').

Several literature sources considered it necessary for providers to disclose location (including failover datacenters) [19],0,[28],[30]. Transfer out of the EU was also considered something that should be included contractually. [28] considered this an obligation. The C-SIG on SLAs stated: "*the cloud service customer should verify that the provider guarantees lawfulness of cross-border data transfers, e.g. by framing such transfers with safe harbour arrangements, EC model clauses or binding corporate rules, as appropriate*" [19].

4.9 PENALTIES – SERVICE CREDITS; WARRANTIES AND LIABILITY; INDEMNIFICATION;

There are two broad areas of actuation by the CSP that could incur in liability and breach of services levels; on the one hand the security and confidentiality of the data held on behalf of the user and on the other hand those related to the technical level of service (disruption, server down time, etc.). Associated with this, is the issue of which party bears the burden of proof of SLOs not being met and which penalties and/ or indemnification applies.

4.9.1 Data security and confidentiality breach

The more serious issue is that of liability of data security and confidentiality breach. This type of breach is more difficult to detect by the user than technical disconformities (which will be discussed later in this section). There are different associated liabilities for the provider [19], in bullets and following discussion:

- Liability for authorising an unlawful disclosure;
- Liability for failing to prevent an unauthorised disclosure, or
- Liability for failing to comply with notification obligations consequent from an unauthorised disclosure.

A Provider will usually impose provisions in the contract designed to limit its contractual or tortious liability in all three circumstances above; although a Provider is not be able to transfer any regulatory liability under data protection law. It may try to contractually shift any financial implications consequent from a finding of non-compliance on to other parties in the cloud supply chain.

Regulatory liability arising from the conduct of a receiving controller, e.g. processing for incompatible purposes, would not generally result in any liability on the disclosing controller unless it can be shown that he had some responsibility for the unlawful conduct, e.g. he disclosed data knowing that the receiving controller was intending to engage in unlawful processing[3] . However, the parties may alter the regulatory position through contract, agreeing to be 'jointly and severally liable' for any damage caused to a data subject by any breach; which is the position adopted under the Model Clauses for data transfers between controllers[4] .

The tendency is for CSPs to limit their liabilities through contract terms (in some cases as to seem to have practically zero liability…). The limitations to liability may be either sweeping or focused on certain categories of damages, and usually capping the amount of potential damages, for example in relation to the fees paid by the user over a certain time period [16]. Limitations of liability due to force majeure are common and considered a reasonable practice by the DG Justice expert group.

Despite sweeping clauses limiting liability, users do have recourse for example through the Unfair Contract Terms Directive. For example, a national court rejected a clause excluding liability for loss of

[3] Art. 23(2

[4] Commission Decision 2001/497/EC, 'on standard contractual clauses for the transfer of personal data to third countries', OJ L181/19, 4.7.2001.

data, considering negligence of the cloud provider, and the lack of bargaining power of the user (a small fitness centre). The directive applies only to B2C contracts and only filters out extreme cases, not applying to other unbalanced liability clauses. For this reason, the experts consulted by the EC recommended that the Unfair Contract Terms Directive should be more strictly and systematically enforced to eliminate unfair clauses.

In view of the above, general recommendations include limitations of exclusions of liability, cost of the offered service (free or pay), magnitude and nature of the damages if financial or not (business loss vs temporary inconvenience), and higher penalties associated with security breaches rather than transitory technical problems. Caps on liability are usual practice but a threshold of reparation should also be indicated.

An interesting observation is that providing more advantageous limitation and capping of liability is not a competitive differentiator between cloud providers yet contrary to other service features.

4.9.2 Breach due to failing to meet service levels

Technical disruption of SLO is more easily detected by the user than undue data disclosure or security breaches. Service failures may affect large numbers of users, and so it may be difficult for CSP to foresee financial consequences of such failures. CSP more likely to inform globally to their users in this case in order to avoid adverse publicity associated with lowered service.

As regards remedies for not meeting SLOs, service credits are the most usual means of reparation applied by the CSP as it has a lower operational impact for them as well as strives to maintain the client. This does not always satisfy the user, if the outcome of the deficient service is the decision to change provider rather than continue with the present one. The user may complain that more of the same (bad) service is not satisfactory reparation.

The reparation for deficient service should be defined in the contract, and as far as possible be objective and measurable, with a scale matching the impact of lack of performance of the provider, as well as the procedures for escalating the incidence and applying service level bonuses or penalties [16]. Further, users of free services cannot expect the same levels of reparation as paying users. Some experts differentiate between the impact to the user on issues of convenience or financial loss attributable to the disruption of service.

The DG Justice expert group considered that **Limiting by contract the remedies to service credits could be considered as unfair in the Unfair Contract Terms Directive and so other remedies should be contemplated.** For example, a threshold could be defined beyond which service credit is not sufficient remedy, and refund applied. Remedies should be commensurate with the breach of service.

4.9.3 Burden of proof

Regarding the **detection and report of incidents,** the burden of proof is usually defaulted to the user when the service does not meet a SLO. The manner for detection of these incidents needs to be established, as well as the period for reporting them to the provider and seeking corresponding remedy.

In the study done by ENISA [22], availability tests were done by users 45% of the time rather than the CSP. Further, the process defined in the contract to provide proof of lack of service or deficient quality may require technical skills not held by the end user, who is thus in a disadvantageous position with respect to the provider . **The CSP could take on some of the action of monitoring service levels and informing the end user, without being too burdensome for them. This could be achieved either via (i) reporting by the provider or (ii) by reversing the burden of proof.**

Even though the Cloud providers have access to the necessary information for monitoring, this requires use of time and resources. For this reason, a more cost effective approach for CSP is to report on major problems to users. Alternately, if the burden of proof is reversed (in terms of documentation required of the user to demonstrate loss of service), this reinforces the user position while also preventing overburdening the CSP.

Another alternative is that of independent audit and certification, as described in [29]. For the user, it is important to ascertain that the CSP is willing to undergo audits regarding data quality and security by external audit agencies. Best practice compliance includes:

- ISO 9001 (quality management) standard;
- ISO 27001:2005 (security management) standard;
- ISAE3402 (assurance reporting) standard;
- BS 27999 (business continuity management) standard; and
- the requirements of a Tier 3 data centre set out in the Telecommunications Industry Association's TIA 942 standard

From the questionnaire carried out by SLALOM, there are some items not contemplated or fully contemplated by the current SLOs. For example, CSP respondents listed ‘Warranty (compliance with law and agreement)’ , 'Penalties' and 'Mediation and arbitration', ‘Consequence of default of SLA KPI.' as missing from ISO. Adopters did not identify this with ISO but did bemoan a 'Lack of accountability' and 'Poor resolution of incidents and communication' as key problems of MSAs.

SLALOM should apply the recommendations in the Document: ‘LIABILITY FOR NON-PERFORMANCE INCLUDING REMEDIES’ (DG Justice expert group) [16] as this appears to be the main authority on the issue, and as other sources including the questionnaire have corroborated that this is an issue noted by stakeholders.

4.10 INSURANCE OBLIGATIONS;

No discussion of these obligations arose either from the questionnaire or in the literature search. It is assumed that there are no associated issues of significance.

4.11 SUSPENSION OF SERVICES;

No specific discussion of these obligations arose either from the questionnaire or in the literature search. The topic is related to the section on intellectual property rights, warranties and indemnities.

4.12 FORCE MAJEURE;

No discussion of these obligations arose either from the questionnaire or in the literature search. It is assumed that there are no associated issues of significance.

4.13 NOTICES;

No discussion of these obligations arose either from the questionnaire or in the literature search. It is assumed that there are no associated issues of significance.

4.14 COMPLIANCE;

The following service SLOs have been identified in the literature regarding compliance aspects. Where appropriate we add our findings from the questionnaire and literature search as well:

ISO 082 Governance component [Overall]
ISO 083 Governance component [/ Regulation adherence]
ISO 084 Governance component [/ Standard adherence]

The CSCC [20] supports the need of this SLO stating that " Regulated industries, like government, financial services, and healthcare, are subject to specific and often quite onerous standards which must be addressed in the CSA and implementation"

ISO 085 Governance component [/ Policy adherence]
ISO 086 Governance component [/ Audit schedule]

Regarding audit component, CSPs also expressed their interest through the SLALOM questionnaire in expanding it with audit results while other stakeholders referred to the lack of auditing as something that needs to be dealt.

ISO 087 Governance component [/ Number of failed SLOs]

ISO 123 Attestations, certifications and audits component [Overall]
ISO 124 Attestations, certifications and audits component [/ Cloud service attestations]
ISO 125 Attestations, certifications and audits component [/ Cloud service certifications]

Feedback from a respondent of the SLALOM questionnaire also agrees with the need of the cloud service providers being certified. In particular, he stated that "'The above SLA's" (referring to the

proposed SLA in the SLALOM handout) "should be industrialised, standardised and cloud service providers should be 'certified' to be capable (or not) to provide a high (or medium or low) level of traceability, visibility, monitoring reporting. An industry standard should emerge, like for any other industry..."

ISO 126 Attestations, certifications and audits component [/ Cloud service audits]

Apart from the SLOs proposed by ISO, some more can be found within the work of C-SIG on SLAs [19]:

C-SIG: Certifications applicable
C-SIG: Applicable data protection codes of conduct, standards, certifications

CSP respondents of the SLALOM questionnaire and interview also expressed the need for the SLAs to be aligned with industry specific authorities such as Law Society or SRA requirements.

The Gartner report [31] adds the following two aspects with respect to compliance:

GARTNER: data stewardship

(The terms of which should clearly define the "features that will help the cloud service customer to use the service if there are regulatory compliance needs and applicable details of security certifications (e.g. data location)") and

GARTNER: Compliance and Certification terms

(i.e., details of how the cloud service provider ensures compliance and certification[5]: these should be listed by individual service and region where compliant or certified)

Finally, according to the CIF Code of Practice [23] CSPs should a) list any existing relevant certifications, e.g. ISO 9001, ISO/IEC 27001, PCI DSS, SAS 70 and SSAE 16/ISAE 3402; a statement of the scope of business covered by Certification; and how it corresponds to scope of the Code (of Practice) and b) by whom Certification was performed, if independently certified.

Compliance and external audits are issues that are highly debated in cloud computing. Whilst this area is emerging, it is not clear in whose interest its proponents are acting. Certainly it is in the interest of the bodies producing the certifications and certifying the CSPs. If compliance with a certain regulation or certification is compulsory, it is unnecessary to cover it in the contract as the relevant legislation already ensures it. It the CSP advertises adherence to voluntary codes and yet fails to adhere to them, then this would be covered under legislation on false advertising. Recalling the words of one CSP to SLALOM *'You can be asked to put something under SLA that you would never be asked in traditional process - over-expectation'.* In how many other sectors would you include multiple contractual obligations to oblige the provider to comply with the applicable law?

[5] Examples of relevant compliance and certifications include SSAE 16 audit; ISO 27001; EU Safe Harbor certification; Cloud Security Alliance; European Privacy Seal (EuroPriSe)

4.15 GOVERNING LAW and JURISDICTION;

The aspect of governing law and jurisdiction has been studied primarily through the literature search. The only aspect mentioned through the questionnaire was that of a USA-based CSP with European offices and resulting grey area of jurisdiction. The parties have the right to decide the governing law of the contract following EU regulations and international law. The jurisdiction clause of the contract identifies the court for settlement of potential disputes.

Except where otherwise acknowledged, the following is abridged from the document 'CLOUD COMPUTING AND PRIVATE INTERNATIONAL LAW' prepared by the DG Justice expert group [12].

Regarding relevant governing law and jurisdiction, there are three main existing EU private international law instruments, the Rome I and Rome II Regulations (on the question of the applicable law) and the Brussels I Regulation (on the question of jurisdiction and whether judgments are recognised or enforced), apply to cloud computing services. These instruments also apply to tort cases, such as privacy rights infringements or loss of data [12]**Error! Reference source not found.**. Further, it needs to be taken into account the Data Protection Act 1998 which prohibits the transfer of personal data to countries outside the EEA that do not offer adequate data protection [29].

A consideration for determining governing law and jurisdiction is the contract type of the MSA. Cloud computing contracts can be classed for instance as "lease contracts", "service contracts" ·IT infrastructure contracts¨, "license" or more rarely "sale contracts", or a mixture of different contract types. For the purposes of applying the EU legislative instruments, a characterization as "service contracts" would allow to establish jurisdiction over all disputes relating to the contract in the same court in the EU.

Due to the inter-territorial nature of Cloud computing, there arise questions of private international law and jurisdiction regarding which courts will deal with the dispute and the recognition and enforcement of the judgement in other Member states. Criteria that are being discussed include location of datacentres, location of CSP main offices, network connection of several multi-datacentres, and location of provision of service (customer location). Each of these criteria have weak points, due to the diffuse nature of cloud computing. Further, the criteria to be applied could also depend on the exact nature of the cloud services provided. For example, in case of a cloud communication service, the relevant place would be the place where the service is used (e.g. the place of the consumer). The place of location of the server could also determine the place of provision of the service as it is the place where the contractual obligation (e.g. storage in case of storage service) is executed.

One suggested solution could also be to locate the provision of services at the place of domicile of the service recipient.

From a provider's perspective a key issue seems to be legal uncertainty relating to operating in different EU Member States due to different legislation at national level and this is even more relevant for third countries, notably the US [17].

For CSPs there are two current main approaches in order to mitigate risk of legal disputes. On the one hand, particularly large EU companies take a “local” approach to contacts to adjust to national requirements where they operate or have client base. This is, however, complex and costly and may force providers to limit their offers to selected countries. Another approach is for CSP to set up multi-jurisdiction agreements to comply with different jurisdictions, making any choice of applicable law subject to overriding national mandatory provisions..

This being said, the truth of the matter is that relatively few cases end up in court due to the low value of the claims and the high cost of the legal fees, particularly a barrier to SMEs to seek retribution via this path. Only cases with strategic interests go to court, with others being mediated via out of court mechanisms, due to lower costs and fees.

Of the cases that have come to court, an issue discussed by experts is the applicable law. For example, in a UK case, Google attempted unsuccessfully to invoke the laws of the state of California, but the UK court applied UK law. In Germany, a case with a non-EU provider was admitted on the criteria of cookies installed on a computer physically located in Germany. One expert stated that usually providers assume that they have to comply with the law where the users reside. So while the elevated costs may deter initiation of legal procedures, consumers still do have access to the court where he has his/her residence. Otherwise, SMEs would likely face difficulties as "choice of court clauses” in some contracts may require SMEs to initiate proceedings abroad and so put a strong deterrent to initiate court proceedings.

Further complications arise when the provider is not EU-based. However, European Commission directives outline that a local presence is not required and that consumers can sue locally despite the absence of a local presence of the CSP. For example, one expert mentioned a case between Google and Apple Safari where the UK court declared itself competent, even though there was a choice of court agreement referring to a US court.

There are no associated SLO for applicable law or jurisdiction

SLALOM could recommend on this point that governing law and jurisdiction should default to the user national law rather than location of the provider or their data centres.

Further, as regards data protection (see section 4.8 on IPR and data protection in this document), it is recommended that the user require the cloud computing provider to store data within the EEA in order to avoid release of said data under other national legislations [29].

4.16 FINAL PROVISIONS

No discussion of these obligations arose either from the questionnaire or in the literature search. It is assumed that there are no associated issues of significance.

4.17 Attachment to the MSA: Business Continuity

This section refers to issues of support, back-up, disaster recovery and so on. It is ordered according to the ISO standard. We add our findings from the questionnaire and analysis from the literature search as well at each appropriate point:

ISO 071 Cloud service support component [Overall]
ISO 072 Cloud service support component [/ Support plans]
ISO 073 Cloud service support component [/ Support costs]

According to Ministry of Justice guidance on Cloud Computing and CJSM [29], there may be additional charges for support services based on e.g., a percentage of the subscription fee.

SLALOM should ensure that support costs are clear in the contract.

ISO 074 Cloud service support component [/ Support methods]

The Ministry of Justice guidance on Cloud Computing [29], advise that support methods don't only necessarily involve answers as soon as the helpdesk is called. The initial response may only include the log of the problem with a further call back to provide substantive support. Another way the CSP may support the cloud adopter is by offering advice on, and support with checking, the necessary equipment and internet connection required for optimum cloud system performance. The CSP may also advise on contingency plans for internet outages.

Given the complex variety of cloud services, as well as variety of business models, it appears unlikely that a standard clause could adequately cover this topic. SLALOM may want to limit scope to providing instruction on how to best describe the methods.

ISO 075 Cloud service support component [/ Support contacts]
ISO 076 Cloud service support component [/ Support hours]
ISO 077 Cloud service support component [/ Service outage support hours]

The Cloud Standards Customer Council (CSCC) [20] and Ministry of Justice [29] also support this component highlighting the need for clarity with respect to time zone used when stating the service support hours. This is particularly important in cases where the cloud adopter may expand their activity in multiple locations. Clarity is also required with respect to the definition of the "week-ends" and/or "holidays" and the variance of their meaning among different countries. CIF Code of Practice [23] takes into account geographical scope for support as well, while CSPs propose - through the SLALOM questionnaire - additional terms related to service desk response time and change of management response time (where applicable).

This is a simple issue for SLALOM, it is merely a question of the clause be well written to be unambiguous.

ISO 078 Cloud service support component [/ Service incident notification]
ISO 079 Cloud service support component [/ Service incident reporting
ISO 080 Cloud service support component [/ Service incident notification time]

The CSCC [20] urge cloud adopters to ensure that a management system is available from the CSP in order to alert them on occurring incidents. Towards this direction, the cloud adopter must first ensure that cloud service failures can be detected. Although such an SLO already exists, the feedback from the SLALOM questionnaire reveals that the resolution of incidents and the respective communication are considered poor.

The same offers guidance on reporting the service incidents: a) the process for reporting failures detected by the customer, b) the process which the provider will follow to address a reported failure, c) the timescales for remedial action and d) the process that the cloud service provider will follow subsequent to a failure to improve the provider's operations to avoid the failure occurring again.

Certainly a-d from the CSCC guide can be considered best practice in customer care. However, to have this as a contractual obligation may be too stringent. Nonetheless it is clear that where the CSP has an obligation of service to the adopter, there needs to be a mechanism through which the adopter can advise of failure. Other SLOs could be seen as part of the value proposition of the CSP.

ISO 081 Cloud service support component [/ Maximum incident resolution time]
ISO 088 Service reliability component - service resilience/fault tolerance component [Overall]
ISO 089 Service reliability component [/ Time to service recovery (TTSR)]
ISO 090 Service reliability component [/ Mean time to service recovery]
ISO 091 Service reliability component [/ Maximum time to service recovery (MTTSR)]
ISO 092 Service reliability component [/ Number of service failures]
ISO 093 Service reliability component [/ Network redundancy]
ISO 094 Service reliability component - customer data backup and restore component [Overall]
ISO 095 Service reliability component [/ Backup method]
ISO 096 Service reliability component [/ Backup interval]

The Ministry of Justice [29] recommends that cloud adopters should be aware of the frequency the cloud provider will back up their data to a separate site and the periods of time that there won't be any data backups so as to make his own to avoid data loss should the cloud system fail. See the discussion in section 4.8.2.3 on the responsibility for data integrity).

ISO 097 Service reliability component [/ Backup verification]
ISO 098 Service reliability component [/ Backup restoration testing]
ISO 099 Service reliability component [/ Backup restoration test reporting]
ISO 100 Service reliability component [/ Retention period for backup data]
ISO 101 Service reliability component [/ Number of backup generations]
ISO 102 Service reliability component [/ Alternative methods for data recovery]
ISO 103 Service reliability component - disaster recovery component [Overall]
ISO 104 Service reliability component [/ Cloud service provider disaster recovery plan]:

The Gartner report [31] suggest that this SLO should define a) the responsibilities for disaster recovery plans and b) the disaster, i.e., events that are included as a disaster, requiring provider response

ISO 105 Service reliability component [/ Recovery time objective (TRO)]
ISO 106 Service reliability component [/ Recovery point objective (RPO)]

Apart from the SLOs proposed by ISO, some more can be found within the work of the C-SIG on SLAs [19]:

C-SIG: Data Mirroring Latency
C-SIG: Maximum Data Restoration time
C-SIG: Percentage of Successful Data Restorations

Finally, Ministry of Justice guidance on Cloud Computing [29] guide the cloud adopters to look for two last business continuity related components in their SLA:

a) Security of Data Centre in terms of i) facility monitoring, ii) controlled access, c) fire detection and suppression system, iv) overheating prevention, v) backup generators to sustain long power outages and vi) backup of everything so there is no single point of failure. Auditing of the facilities of the CSP data centre at least annually is also advisable.

b) Portability of data, i.e., the capability of timeously moving the data back to the cloud adopter premises or to another provider on demand in a usable format. The process to be followed should be tested with a dummy set of data on a regular basis as part of the cloud adopter's ongoing disaster recovery planning. (See related discussion on data portability under sections 4.6 and 4.8).

Overall, the feedback from the SLALOM questionnaire regarding the SLA model for business continuity revealed a good and balanced view of the model, but the concern of turning the SLA into a complex document (due to its level of details) for both the CSPs and the cloud adopters was raised by a CSP.

Indeed the extensive set of SLOs presented in this section seems excessive and potentially impractical as they are unlikely to be applicable in all situations across the spectrum of cloud services. The key issue in this area is clarity over who has the responsibility for back-up and recovery. This is likely to be part of the value proposition of the CSP. If the CSP does offer this as a service it is natural that the terms of this are described with SLOs as per any other part of the service.

4.18 Attachment to the MSA: Security

Security is a major and complex issue, as well as a constantly evolving field. It is one of the major barriers to cloud uptake. Nonetheless the ISO Cloud SLA standard at the time of writing only included one SLO, unlike other sources which suggest more extensive SLOs.

ISO 067 Information security component [Overall]

The Gartner report [31] extends the component of the information security to the physical security as well. In particular, the report suggests that "the terms also reference relevant certifications (e.g, ISO 27001) or explicitly define security measures employed on physical sites, for example biometrics on physical access points, CCTV, security personnel, natural disaster monitoring and multiple power grid feed points.

From the questionnaire point of view, the received feedback is as follows:

CSPs:

- Overall
  - 'Have a quantifiable level of security'
  - 'Security controls for cloud providers needs to be called out (denial of service protection - both volumetric and application layer).'
  - 'DOS attack defence planning'
  - 'Intrusion detection'
  - 'A specific element on security standards, other than that there is far too much, and would push up the cost of cloud computing in Europe if CSPs were forced to build monitoring tools to cover the entirety. The components also fail to recognise that many elements would be service options driven by customer choice - e.g frequency/method of back-up, asynchronous replication across data centres for DR, etc'
  - 'When asked about security practices, don't always have the certifications in place - not always practical for small business. Quality and responsiveness are key to them - e.g. took CIF Code of Practice to demonstrate trustworthiness'
- Security and personal data protection issues
  - 'Varied customer requirements for security, incident response, or privacy.
  - 'Audit and security - in a multi-tenant environment we cannot change or concede for one customer, or we would breach our agreements with our other tenants. Its buyer education again. And trying to keep to standard'
  - 'Many customers don't understand major areas of security vulnerabilities in SaaS applications - mostly in management consoles, by Customer Support, Product Management, etc. Since in many companies, SaaS have lots of access to customer data that the customer may not realize. Yet, the customer contracts try to require very specific security requirements that are archaic (e.g., intrusion prevention devices, instead of newer web application firewalls or privileged account management). '
  - 'Cloud computing contracts are nothing different from managed services / outsourcing services contracts except that customers are very conscious about data privacy and data security related issues'
- Customer need for education / better understanding
  - 'Lack of understanding of Cloud and how to interpret the contract in relation to the provision which leads to big questions that are difficult to answer in layman's terms as things are so new. The What If scenarios which can get a bit unrealistic especially when people hear "gossip" on the news about the latest security breaches. People's lack of understanding.'

Cloud Adopters:

- a set of standard "minimum" security controls
- 'It does not protect against unknown breaches or security incidents as long as the cloud provider is not legally subject to notify them.'
- 'The lack of a standard set of Security Controls (or just the "family" of the topic).'
- 'Completeness of SLA: how far to go, what is acceptable by the provider, take it or leave it approach if the provider has a dominant position on its market.'

Apart from the SLOs proposed by ISO, some more can be found within the work of C-SIG on SLAs [19]:

C-SIG: User authentication and identity assurance level
C-SIG: Authentication

According to the C-SIG [19], authentication and authorization are key elements of information security which apply to the use of cloud services. The Gartner report [31] also supports the existence of such a component and identity aspect as a whole stating that i) user management, ii) authentication mechanisms, iii) management of the authorization of users and iv) federation services for integration with other identity and access management solutions are the controls for information protection that SaaS cloud terms of service need to provide. Ministry of Justice guidance on Cloud Computing [29] draws the attention of the cloud adopters to the importance of them understanding the measures he can take to protect the security of your data (e.g., through the mandatory use of strong passwords, automated routines for password updates, etc.). The guidelines also proposes two-factor authentication to reduce the impact of human security weaknesses (such as writing the password down and keeping it near the computer). With two-factor authentication, a password ("something you know") is coupled with a second authentication mechanism such as a smart card or device that generates a single-use PIN ("something you have").

C-SIG: Mean time required to revoke user access
C-SIG: User access storage protection
C-SIG: Third party authentication support
C-SIG: Cryptographic brute force resistance:

It is necessary for the SLA to describe specifics relating to encryption methods in order for the cloud service customer to evaluate a cloud service fully, since few certifications require the use of specific encryption methods. In Gartner report [31] terms, cloud terms of service relating to data stewardship should clearly define i) how data is encrypted, ii) how data isolation/segregation is enforced and iii) how data is secured to protect it from being revealed inadvertently.

C-SIG: Key access control policy
C-SIG: Percentage of timely incident reports

How information security incidents are handled by a cloud service provider is of great concern to cloud adopters

C-SIG: Percentage of timely incident responses
C-SIG: Percentage of timely incident resolutions
C-SIG: Percentage of timely vulnerability corrections
C-SIG: Percentage of timely vulnerability reports
C-SIG: Reports of vulnerability corrections

Finally, the Gartner report [31] adds the following two aspects with respect to security:

a) In terms of security breaches, the cloud terms of service should provide information with respect to i) responsibilities for identifying and reporting security breaches to cloud service customer, ii) timescales for reporting security breaches to cloud service customer and iii) processes to respond to security breaches.

b) Tenant isolation: The way isolation and protection of the cloud adopter is ensured should be defined.

Security is a complex issue and an evolving field that would require significant expertise and resources to standardise. As commented by the CSPs, there is a danger of focussing on the wrong ("archaic") issues and leaving an exposed front with respect to the latest cyber threats.

SLALOM should consider parallel work in both the areas of certification and compliance, and in security standards. It is unrealistic and senseless for SLALOM to attempt to repeat this work in any way, and hence should defer to them for the standards. In terms of the contract SLALOM should focus on ensuring that the adopter is clear of what security is being offered, such as through reference to security standards.

5 Component and Metric Prioritisation

5.1 Component prioritisation

This spreadsheet shows the relative prioritization of components listed in the first Committee Draft of ISO/IEC 19086-1, based on the SLALOM questionnaire responses.

Component	CSP Avg Val	CSP Rank	End-User Avg Val	End-User Rank	Other Avg Val	Other Rank	All Avg Val	All Rank
067 Information security component [Overall]	4.95	1	4.9	1	4.75	10	4.91	1
042 Availability component [Overall]	4.89	2	4.82	5	5	1	4.88	2
066 Protection of personally identifiable information component [Overall]	4.84	3	4.8	7	4.75	10	4.82	3
033 SLA definitions component [Overall]	4.74	6	4.82	5	5	1	4.79	4
050 Cloud service performance component - cloud service response time component [Overall]	4.72	8	4.73	16	4.75	10	4.73	5
104 Service reliability component [/ Cloud service provider disaster recovery plan]	4.68	9	4.89	2	4.5	21	4.73	5
103 Service reliability component - disaster recovery component [Overall]	4.78	5	4.8	7	4.25	38	4.72	7
032 Covered services component [Overall]	4.63	11	4.73	16	5	1	4.71	8
034 Service monitoring component [Overall]	4.58	14	4.73	16	5	1	4.68	9
094 Service reliability component - customer data backup and restore component [Overall]	4.79	4	4.7	20	3.75	61	4.64	10
068 Termination of service component [Overall]	4.63	11	4.67	24	4.5	21	4.63	11
120 Data management component - data location component [Overall]	4.74	6	4.6	30	4	41	4.61	12
107 Data management component [Overall]	4.56	15	4.78	9	4.33	31	4.6	13
109 Data management component [/ Cloud service customer data component]	4.42	24	4.89	2	4.75	10	4.59	14
123 Attestations, certifications and audits component [Overall]	4.53	18	4.6	30	4.75	10	4.58	15
082 Governance component [Overall]	4.56	15	4.7	20	4.33	31	4.58	15
093 Service reliability component [/ Network redundancy]	4.42	24	4.89	2	4.5	21	4.57	17
088 Service reliability component - service resilience/fault tolerance component [Overall]	4.56	15	4.7	20	4.25	38	4.56	18
035 Service monitoring component [/ Monitoring parameters]	4.44	21	4.6	30	4.67	17	4.52	19
070 Termination of service component [/ Return of assets]	4.47	19	4.67	24	4.33	31	4.52	19
116 Data management component - data deletion component [Overall]	4.42	24	4.78	9	4.25	38	4.5	21
125 Attestations, certifications and audits component [/ Cloud service certifications]	4.37	32	4.56	35	5	1	4.48	22
117 Data management component [/ Data deletion process]	4.37	32	4.75	14	4.5	21	4.48	22
083 Governance component [/ Regulation adherence]	4.42	24	4.78	9	4	41	4.48	22
100 Service reliability component [/ Retention period for backup data]	4.42	24	4.78	9	4	41	4.48	22
078 Cloud service support component [/ Service incident notification]	4.37	32	4.56	35	5	1	4.47	26
069 Termination of service component [/ Notification of service termination]	4.39	30	4.56	35	4.67	17	4.47	26
108 Data management component [/ Intellectual property rights component]	4.28	41	4.67	24	4.75	10	4.45	28
097 Service reliability component [/ Backup verification]	4.37	32	4.63	28	4.5	21	4.45	28
115 Data management component [/ Law enforcement access component]	4.41	29	4.56	35	4.33	31	4.45	28
122 Data management component [/ Data location specification capability]	4.63	11	4.22	59	4	41	4.45	28
071 Cloud service support component [Overall]	4.47	19	4.7	20	3.75	61	4.45	28
121 Data management component [/ Data location]	4.68	9	4.33	51	3.33	65	4.45	28
039 Accessibility component [Overall]	4.37	32	4.55	41	4.5	21	4.44	34
113 Data management component [/ Data portability component]	4.28	41	4.75	14	4.5	21	4.43	35
098 Service reliability component [/ Backup restoration testing]	4.32	38	4.67	24	4.5	21	4.43	35
075 Cloud service support component [/ Support contacts]	4.32	38	4.44	44	5	1	4.42	37
037 Roles and responsibilities component [Overall]	4.26	43	4.55	41	4.75	10	4.41	38
057 Cloud service performance component - cloud service capacity component [Overall]	4.32	38	4.73	16	4	41	4.41	38
084 Governance component [/ Standard adherence]	4.44	21	4.5	43	4	41	4.41	38
079 Cloud service support component [/ Service incident reporting]	4.39	30	4.33	51	4.5	21	4.38	41

Component	CSP Avg Val	CSP Rank	Adopter Avg Val	Adopter Rank	Other Avg Val	Other Rank	All Avg Val	All Rank
077 Cloud service support component [/ Service outage support hours]	4.16	53	4.56	35	4.5	22	4.3	47
062 Cloud service performance component - elasticity component [Overall]	4.21	46	4.56	35	4	45	4.29	48
124 Attestations, certifications and audits component [/ Cloud service attestations]	4.21	46	4.44	47	4.33	35	4.29	48
076 Cloud service support component [/ Support hours]	4.21	46	4.22	64	5	1	4.29	48
038 Roles and responsibilities component [/ Responsibility list]	4.16	53	4.4	53	4.67	17	4.28	51
036 Service monitoring component [/ Monitoring logs]	4.26	44	4.3	63	4	45	4.25	52
040 Accessibility component [/ Accessibility standards]	4.21	46	4.4	53	4	45	4.25	52
118 Data management component [/ Data deletion notification]	4.11	58	4.63	28	4	45	4.24	54
086 Governance component [/ Audit schedule]	4.21	46	4.44	47	3.5	68	4.23	55
102 Service reliability component [/ Alternative methods for data recovery]	4.16	53	4.44	47	4	45	4.23	55
073 Cloud service support component [/ Support costs]	4.11	58	4.33	55	4.67	17	4.23	55
099 Service reliability component [/ Backup restoration test reporting]	4.21	46	4.22	64	4	45	4.2	58
095 Service reliability component [/ Backup method]	4.16	53	4.33	55	4	45	4.2	58
101 Service reliability component [/ Number of backup generations]	4.16	53	4.33	55	4	45	4.2	58
059 Cloud service performance component [/ Limitation of available cloud service resources]	3.95	67	4.56	35	4.5	22	4.17	61
063 Cloud service performance component [/ Elasticity]	4	64	4.33	55	4.67	17	4.14	62
112 Data management component [/ Derived data component]	3.94	68	4.57	33	4	45	4.11	63
072 Cloud service support component [/ Support plans]	4.11	58	4.11	67	4	45	4.1	64
110 Data management component [/ Cloud service provider data component]	4.06	63	4.33	55	3.5	68	4.1	64
111 Data management component [/ Account data component]	4	64	4.33	55	4	45	4.1	64
041 Accessibility component [/ Accessibility policies]	4.11	58	4	70	4.33	35	4.09	67
074 Cloud service support component [/ Support methods]	4	64	4.11	67	4	45	4.03	68
058 Cloud service performance component [/ Number of simultaneous cloud service connections]	3.72	69	4.44	47	4	45	3.97	69
114 Data management component [/ Data examination component]	3.71	70	4.57	33	4	45	3.96	70

5.2 Metrics Prioritization

This spreadsheet shows the relative prioritization of metrics listed in the first Committee Draft of ISO/IEC 19086-1, based on the SLALOM questionnaire responses.

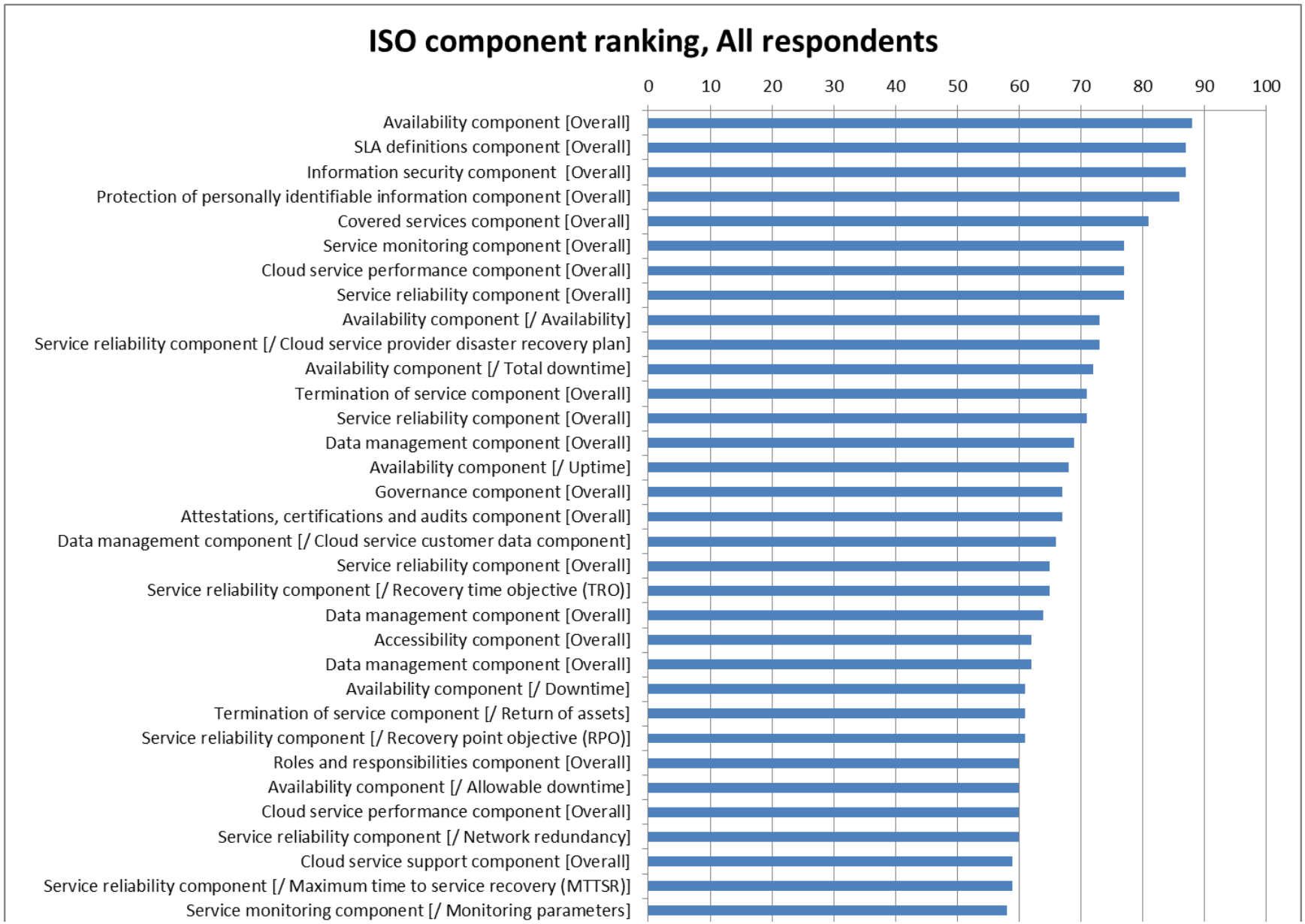
Metric	CSP Avg Val	CSP Rank	End-User Avg Val	End-User Rank	Other Avg Val	Other Rank	All Avg Val	All Rank
043 Availability component [/ Total downtime]	4.79	1	4.8	2	4	21	4.72	1
044 Availability component [/ Availability]	4.74	2	4.6	12	4.67	3	4.69	2
046 Availability component [/ Uptime]	4.74	2	4.5	18	4.33	18	4.63	3
105 Service reliability component [/ Recovery time objective (TRO)]	4.53	5	4.78	3	5	1	4.63	3
091 Service reliability component [/ Maximum time to service recovery (MTTSR)]	4.47	7	4.78	3	4.5	7	4.57	5
106 Service reliability component [/ Recovery point objective (RPO)]	4.47	7	4.78	3	4.5	7	4.57	5
051 Cloud service performance component [/ response time observation]	4.44	10	4.7	7	4.5	7	4.53	7
089 Service reliability component [/ Time to service recovery (TTSR)]	4.42	11	4.78	3	4.5	7	4.53	7
048 Availability component [/ Allowable downtime]	4.58	4	4.6	12	3.67	30	4.5	9
092 Service reliability component [/ Number of service failures]	4.47	7	4.67	9	4	21	4.48	10
049 Availability component [/ Downtime]	4.42	11	4.7	7	4	21	4.47	11
045 Availability component [/ Availability percentage]	4.53	5	4.4	23	4	21	4.44	12
047 Availability component [/ Uptime percentage]	4.42	11	4.5	18	4.33	18	4.44	12
080 Cloud service support component [/ Service incident notification time]	4.32	14	4.56	14	4.5	7	4.4	14
081 Cloud service support component [/ Maximum incident resolution time]	4.21	17	4.56	14	4.5	7	4.33	15
061 Cloud service performance component [/ Cloud service bandwidth]	4.16	21	4.67	9	4.5	7	4.33	15
119 Data management component [/ Data deletion time]	4.21	17	4.63	11	4	21	4.31	17
055 Cloud service performance component [/ Cloud service response time over threshold]	4.17	19	4.56	14	4.5	7	4.31	17
090 Service reliability component [/ Mean time to service recovery]	4.26	16	4.44	20	4	21	4.29	19
056 Cloud service performance component [/ Delay duration time]	4.11	22	4.44	20	5	1	4.28	20
052 Cloud service performance component [/ response time mean]	4.17	19	4.33	24	4.67	3	4.27	21
060 Cloud service performance component [/ Cloud service throughput]	3.95	25	4.89	1	4.5	7	4.27	21
087 Governance component [/ Number of failed SLOs]	4.32	14	4.13	28	4	21	4.24	23
059 Cloud service performance component [/ Limitation of available cloud service resources]	3.95	25	4.56	14	4.5	7	4.17	24
063 Cloud service performance component [/ Elasticity]	4	23	4.33	24	4.67	3	4.14	25
065 Cloud service performance component [/ Precision]	3.95	25	4.33	24	4.67	3	4.11	26
064 Cloud service performance component [/ Speed]	4	23	4.2	27	4.33	18	4.07	27
053 Cloud service performance component [/ response time variance]	3.89	28	4.11	29	4.5	7	4	28
058 Cloud service performance component [/ Number of simultaneous cloud service connections]	3.72	29	4.44	20	4	21	3.97	29
054 Cloud service performance component [/ Nth percentile of response time]	3.47	30	4.11	29	4	21	3.71	30

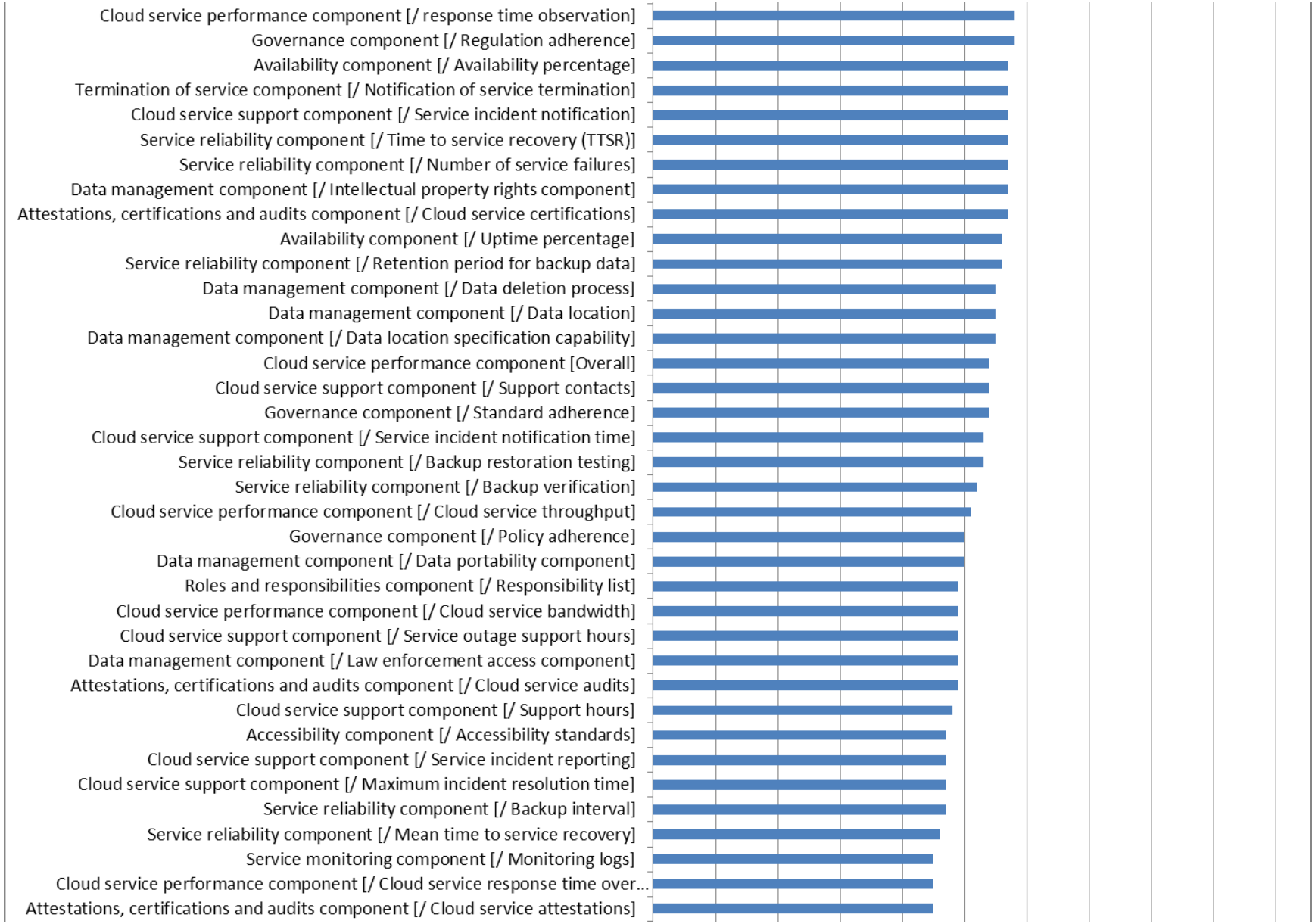
5.3 Graphical representation

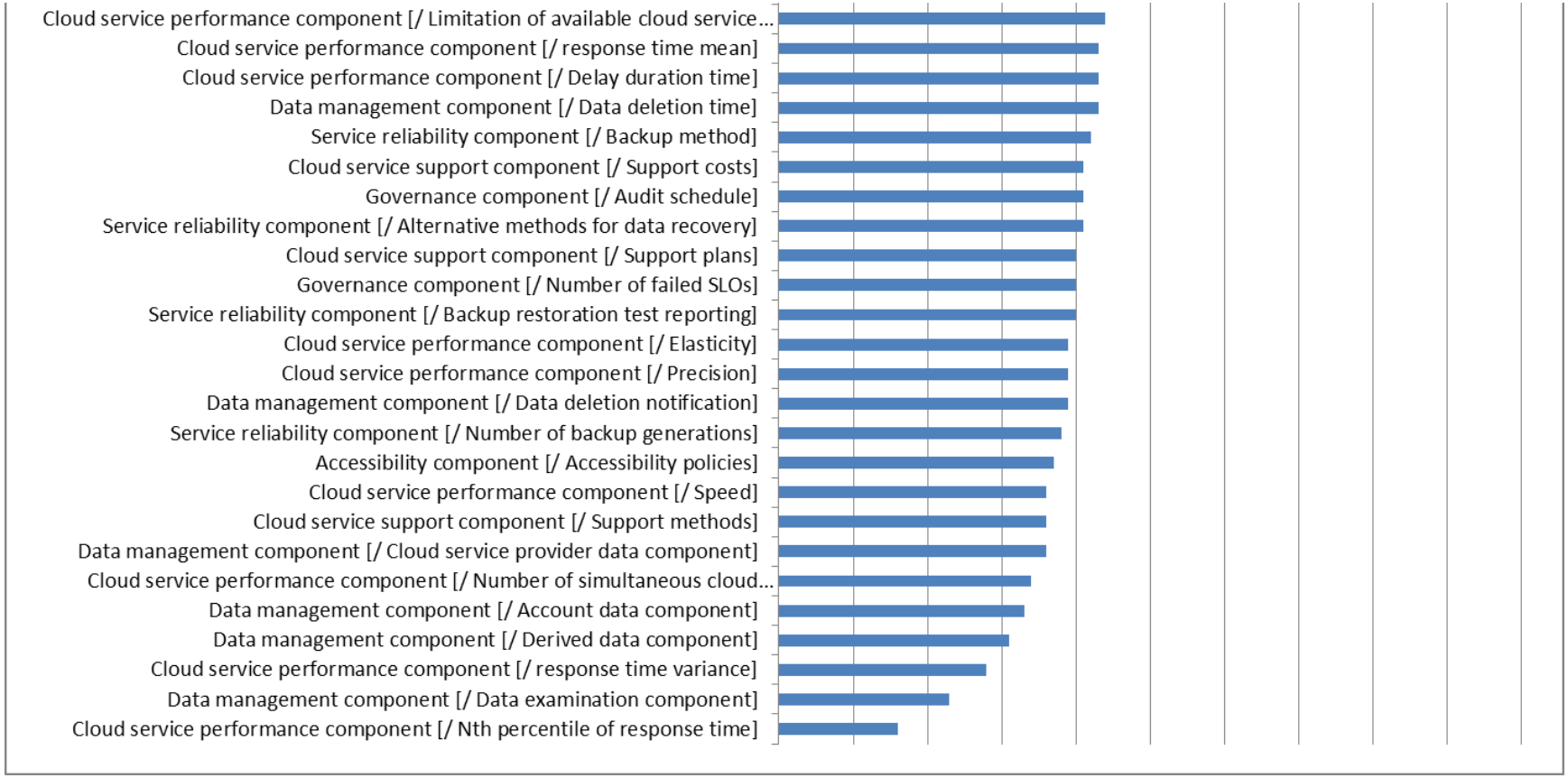
5.3.1 Ranked importance of ISO components and metrics

The following chart shows the relative importance of ISO components and metrics. A multiplicative factor was applied to distance the ranking, as shown below:

Rating	Value
highly important (core requirement)	3
somewhat important	1
Somewhat unimportant	-1
Blank	0

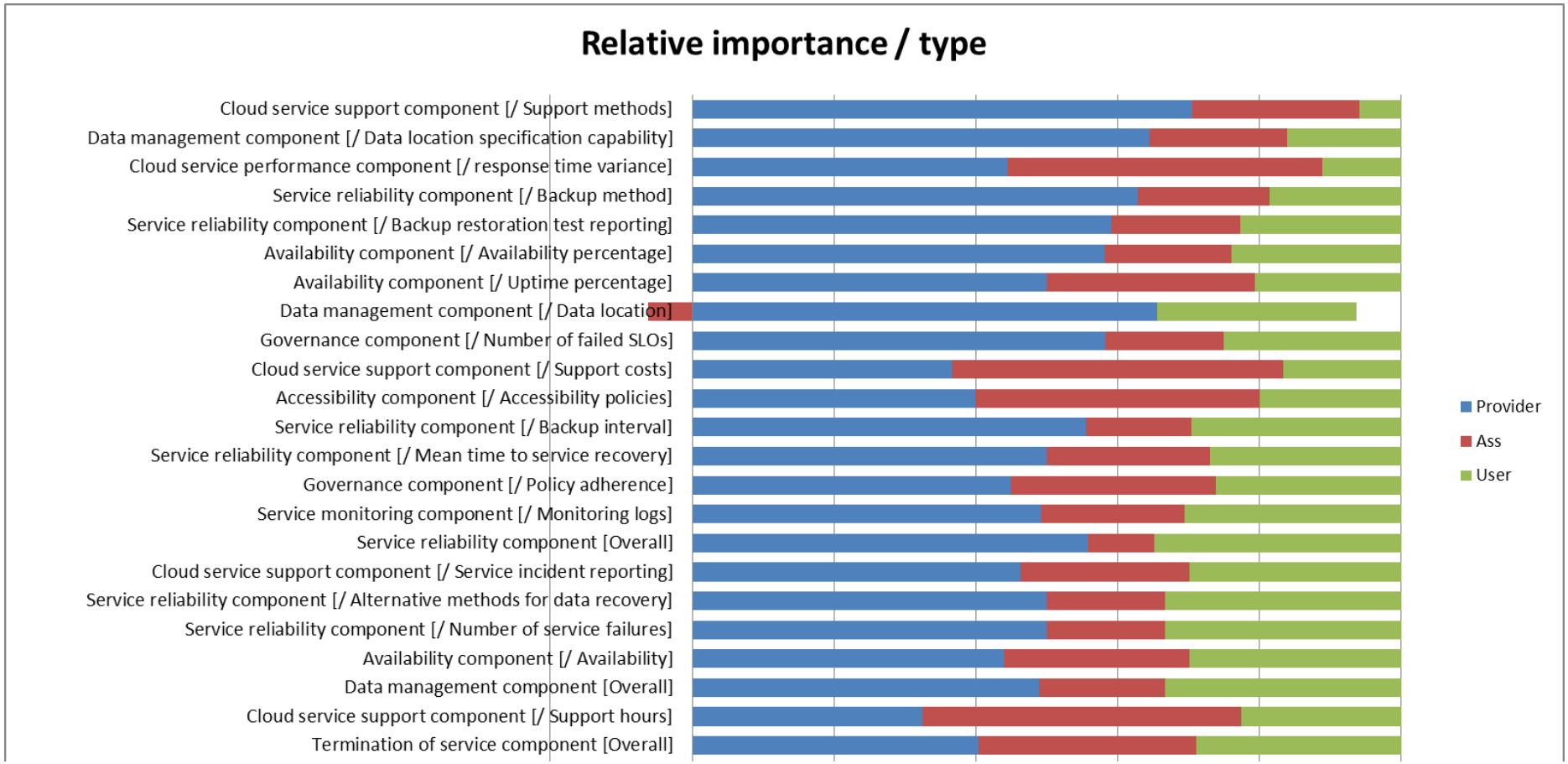


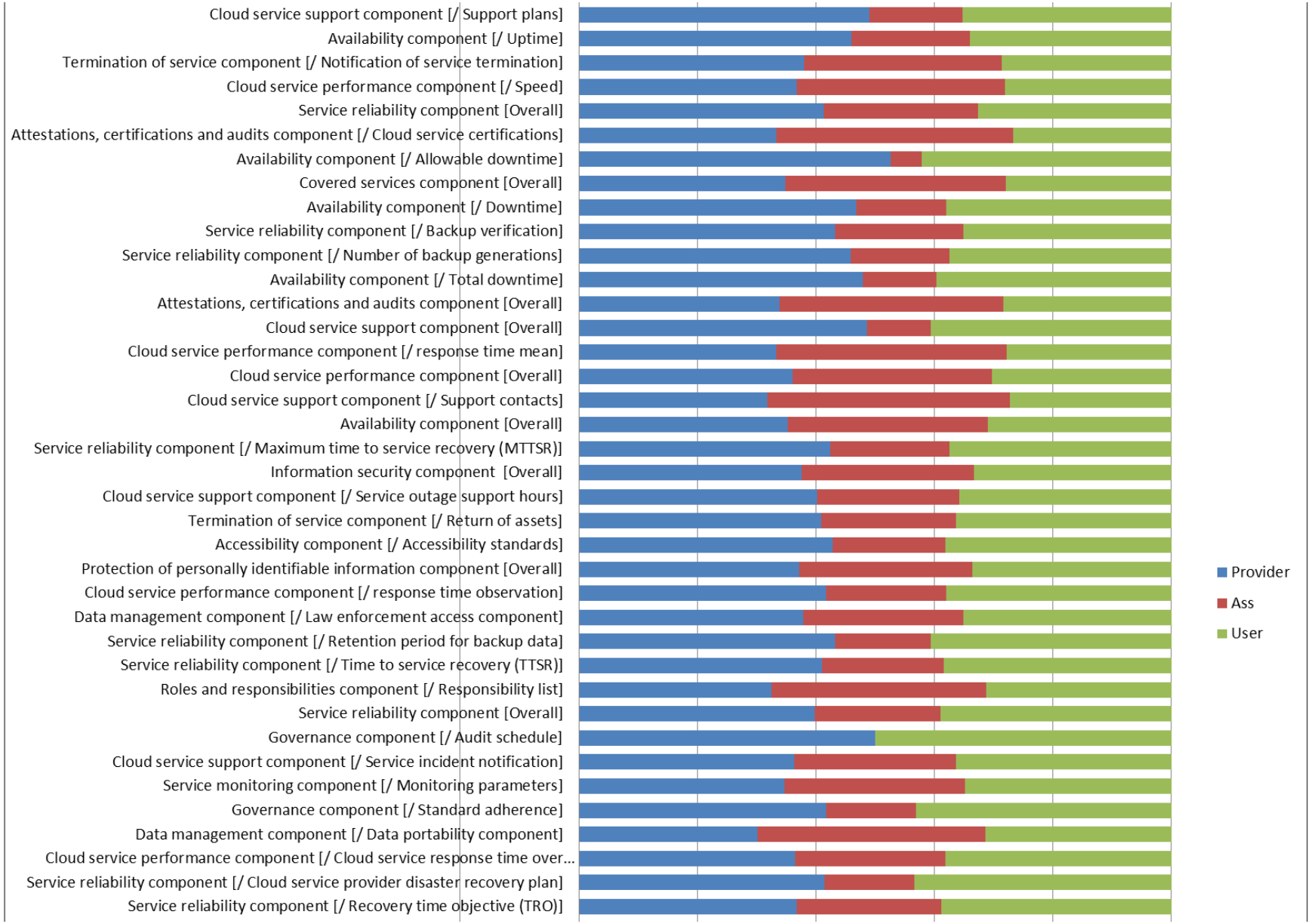


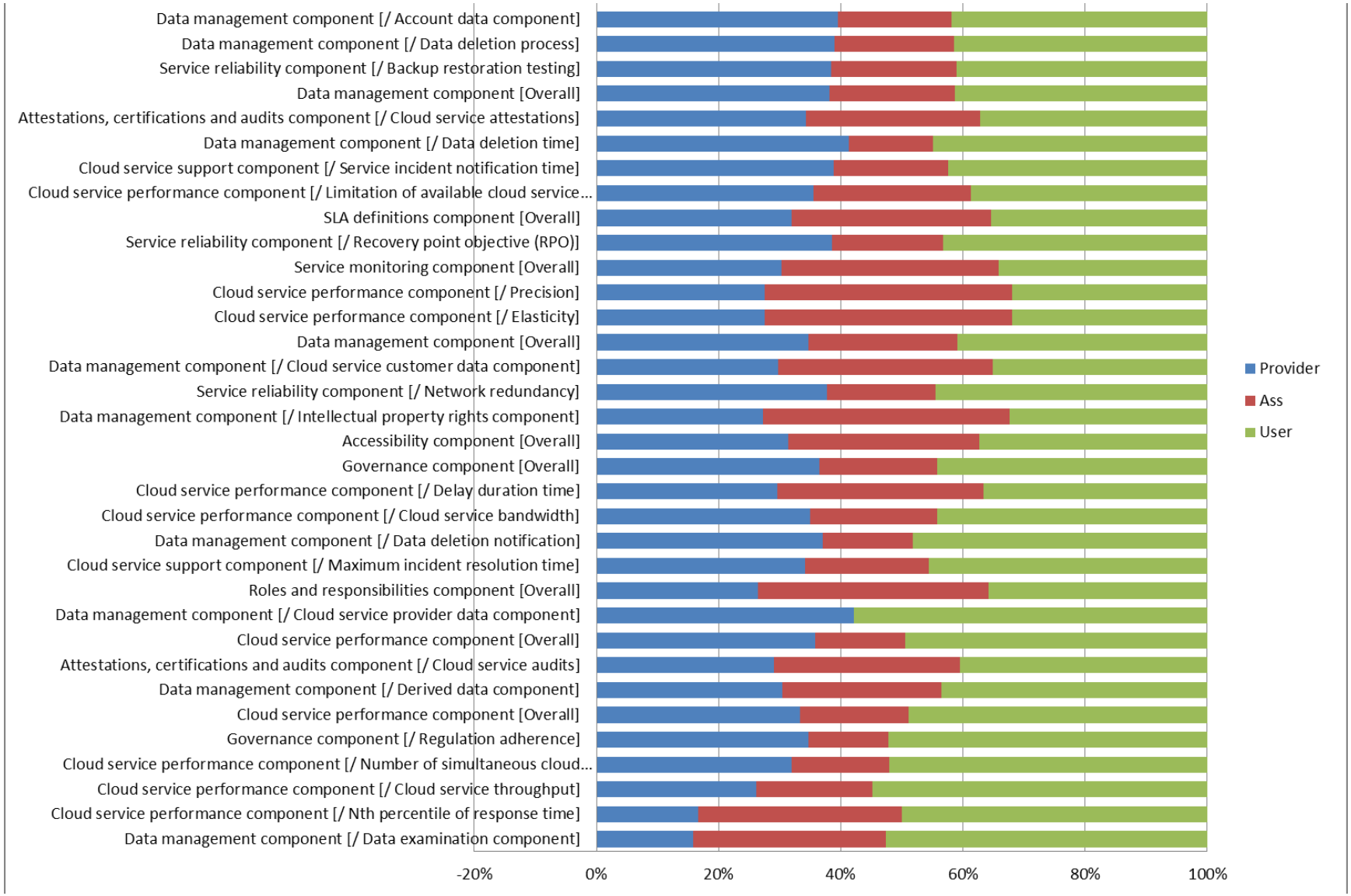


5.3.2 Relative importance of ISO components and metrics per stakeholder type

The following graph shows the relative importance of the metrics per stakeholder type. In order to calculate the values, the above multiplicative factors were applied to distance the rankings, and then a correction factor was applied to correct for the total number of respondents per stakeholder type to the questionnaire. They are sorted with according to discord between providers and adopters.







6 Service level research

The questionnaire presented five scenarios emerging from the SLA research community (from projects funded by EC unit E.2 over recent years). Overall, feedback supports including coverage of the five listed research areas in the final deliverable. 'SLAs at different levels' was the most highly rated with CSPs and Adopters. Automated SLA renegotiation was lowest rated for CSPs and Others, whereas Multi-level SLA interaction was lowest rated for Adopters. 'Others' consistently rated SLA research topics the highest, overall as 'highly important' for 3 of the 5 topics listed. A number of additional topics for research have also been suggested by CSPs, Adopters, and Others.

6.1 Supporting questionnaire analysis

Quantitative Assessment of Research Topics

	CSP	Adopter	Other	Total
135 SLAs at different levels	4.32	4.2	5	4.34
136 Multi-level SLA interaction model	3.94	3.6	5	3.93
137 SLA negotiation across multiple layers	3.81	3.9	4.67	3.93
138 Automated SLA re-negotiation	3.69	3.8	4.33	3.79
139 Proactive SLA violation detection	4.22	3.7	5	4.13
Note: 5 = highly important; 4 = somewhat important; 3 = somewhat unimportant				

Qualitative Assessment of Metrics Model Approach

From the perspective of CSPs:

- Consumer education - the cloud service market is very diverse, evolving rapidly, with niche providers offering solutions to the commonly thought of cloud challenges. Customers need to understand how to identify the right cloud service, rather than homogenising cloud service, which will inhibit the market, and cloud take-up
- For enterprise consumers, how is availability defined?
- Expansion of SLA at different levels - should be split out by geographic location due to high variability in user experience based on country. For example, Russia & China users have up to 10x worse performance than US users. This is a much larger impact on performance than anything else in the cloud provider's infrastructure.
- Where the client's cloud service requirement is jurisdiction-critical (e.g. banking/ investment management; legal; health), regular audit reports for the Supplier to the Client to enable the Client to comply with its Quality Management/ Licencing audit requirements

From the perspective of Adopters:

- Combined effects of location of data centers, local laws and security.

From the perspective of Others:

- Cloud orchestration standards
- Technical Cloud Brokerage standards (interfacing, API's...)
- Cloud Management Portals standards
- Cloud Services Monitoring & Reporting Standards
- SLA auditing and monitoring process for public Clouds SLAs: 3alib SLA auditing component (http://www.artist-project.eu/tools-of-toolbox/209)
- Translating SLA terms to necessary resource management actions (http://users.ntua.gr/gkousiou/publications/MOCS2011.pdf)

7 Conclusions

Given the nature and purpose of this document, it is complex, and rather ineffective to summarise all of the prior discussion. Each chapter summarises and concludes the pertinent considerations. Often this summary is in itself the conclusions of more extensive research and discussion, particularly in the case of sections covered predominantly by the DG Justice expert group. Each section includes conclusions for SLALOM, which can also be considered as best practice or recommendations by other readers.

Nonetheless, it is worth considering the feedback from the questionnaire that explicitly evaluated the SLALOM approach and provided recommendations for the project.

7.1 MSA model approach - conclusions and proposals for SLALOM

- Overall, the proposed approach is considered good. Concerns primarily relate to the worries about a 'one-size-fits-all' approach. Assuming that sufficient flexibility can be built into the proposed model MSA terms and conditions, yet without throwing everything open to endless negotiation, it should help drive the speed of cloud contracting.
- Re additional components, the following are suggested based on feedback to the proposed ISO structure:
    - Warranty (compliance with law and agreement)
    - 'Payment section (payment terms, indexation, consequence of non-payment)'
    - 'Penalties'
    - 'Service cancellation rights for both parties'
    - 'Termination of service component: Deleting derived and customer data?'
    - 'Mediation and arbitration'
    - Subcontracting'
    - Agility to integrate a service (or to stop a service). Associated: portability and reversibility'
    - Scalability (to ramp up or ramp down) of a service
    - 'Generic definitions. Availability is used for example, but there are many different definitions of it. Specific formula should be included'
    - 'Cost reporting! daily, weekly, monthly, wtd, mtd, ytd, forecasting...etc...'
- There is considerable overlap in the proposed ISO SLA standard ISO/IEC 19084-1 between measurable metrics and overall contractual content (or 'service commitments'), and SLALOM should give consideration to what it lists as needing to be covered. SLALOM shall prioritise based on this document and additional market research as necessary.

Quantitative Assessment of MSA Approach

Org Type	No of Responses	Average Rating
CSP	5	4 – Good
Adopter	4	4.25 – Good
Other	3	3.33 - Poor

Qualitative Assessment of MSA Approach

From the perspective of CSPs:

- Overall assessments given ranging from good to poor
    - Good: 'excellent'; 'very useful examples'
    - Negative: 'I believe SLALOM is not addressing the problem from the correct perspective. Some cloud providers pitch service directly to consumers, and terms will need to be different from terms meant for enterprise, where there will tend to be greater scope for negotiation. In either case, SLALOM should be looking at the really key issues - controller, processor relationships, writing terms that serve the many available consumption models, DP compliance, etc. - what is proposed is too simplistic, and assumes all CSPs are like Facebook!'
- Concern/disagreement about specific terms proposed

From the perspective of Adopters:

- Overall assessments good: 'useful'; 'I will use them today'
- Suggestion for improvement: 'Maybe broader examples, organized for each kind of sector/industry'

From the perspective of Others:

- Overall assessments given ranging from good to very poor
    - Negative: ' The "Model Terms" are either dictatorial (lengthy pages of terms and conditions that the Customer is required to accept to enable swiftly the cloud based services OR they are open to debate, with lengthy negotiations which reach agreements that are still highly in favour of the provider.
- Suggestion for improvement: ' The comparisons of good and bad terms are informative, but we also need a straight-forward list of recommended terms.'

7.1.1 Prioritization of components

Section 5 shows the ranked priorities of the different ISO components for CSPs, Adopters, Others, and overall, with the top priorities for each highlighted. The following may be noted:

- The 'information security component' is top priority for both CSPs and Adopters.
- The 'availability component' and 'personally identifiable information' component (i.e. personal data protection) are priorities 2 and 3 for CSPs; and in the top ten for Adopters.
- Network redundancy ranks high for Adopters (2) but lower for CSPs (24).
- The 'cloud service audits' component ranks high for Adopters (9) but quite low for CSPs (58).
- The 'data location' components rank high for CSPs (9 & 11), but fairly low for Adopters (55 & 64).
- 'Others' ranked a number of components highly which were not ranked highly by CSPs or Adopters.

7.2 Service level agreements - Conclusions for SLALOM

- Overall, feedback supports proceeding with the proposed metrics model approach. There are significant challenges because we do not yet have any practical worked examples; and ISO is still developing its proposals for how metrics should be specified, which is what we propose to follow. However, the goal of having something which can be automated is an important one.
- Although there are potentially a large number of metrics which can be incorporated into SLAs:
    - The number of measurable metrics (for use with service level objectives) is significantly less than the number of components which are identified in CD1 of the ISO SLA standard 19086-1. This issue about the distinction between SLOs and 'service commitments' (effectively contractual clauses with commitments which are not measurable in the sense of service levels) is not yet resolved within ISO (SC38 WG3).
    - There is a clear prioritization amongst CSPs and Adopters for specific metrics, or groups of metrics, as follows:
        - Availability (e.g. uptime and downtime, planned and unplanned) – consistently the highest priority metric
        - End-to-end responsiveness/throughput [particularly wanted by Adopters, but seen as difficult by CSPs because of third-party providers beyond effective control, with geography a significant factor]
        - Response time for service support issues [e.g. time to provision; to respond/resolve to service interruptions or to support requests]
    - There is repeated emphasis on the need to keep things simple; and that too many metrics are unrealistic and impractical
- We noted that the CD1 draft of ISO/IEC 19770-1 has no measurable service level metrics defined for the service support component, although it does define a number of 'statements' which should be included in the SLA or other contractual documentation. It is suggested that more focus should be put on such metrics in future drafts, especially given their importance as demonstrated by the questionnaire responses.
- There is furthermore support for using a data exchange format (such as XML) for metric specifications
- It is therefore proposed, for the purposes of SLALOM's final deliverables, that detailed specifications are developed for only a limited number of core metrics, principally in the three priority categories cited above.

Quantitative Assessment of Metrics Model Approach

Org Type	No of Responses	Average Rating
CSP	5	3.8 – Good
Adopter	4	4.25 – Good
Other	3	3 - Poor

Qualitative Assessment of Metrics Model Approach

From the perspective of CSPs:

- Overall assessments are highly variable, ranging from 'overall quite good' to 'meaningless and unusable'. Examples were (understandably) wanted. ['It is difficult to understand exactly how these would work…'] Given continuing significant evolution of ISO approach to specifying metrics, which we propose following, some negative comments are to be expected.

From the perspective of Adopters:

- Support for automation

From the perspective of Others:

- Recognition of issue of communication barrier between technical specifications and non-technical business users: 'Detailed metrics specifications using this template may be precise, but still difficult to understand. For example, it is not clear how the rules will be shown/specified.'

Suggestions for Improvement in Metric Model Approach

From the perspective of CSPs:

- Need for simplicity
    - 'Simplify'
    - 'Make them less complex and perhaps targeted at types of provider. We operate a simple availability and responsiveness test which is as much as the majority of clients can track.'
    - 'Keep contract text simple.'
    - 'Clarity is key'
- Need for relevance
    - 'Make relevant to the nature of cloud services'
    - 'More details on performance - measured in networks that the SaaS provider controls, and by geography for areas that are not under the SaaS Providers control (e.g., if hosted in Singapore - that's one metric. But access from China, Japan, Australia, Russia are all going to be very different).'
- Other
    - 'Make metrics accessible via API.'
    - 'Consistency with other model documents to ensure that they all work together'
    - 'Make sure it is completely platform agnostic'

From perspective of Adopters:

- Other
    - 'Take into account the Cloud Security Alliance Control Matrix. It has some good ideas on disposition that could also be part of the model.'
    - 'Alignment with future regulation/directive on data protection (security by design)'

- 'Support for automation'
- 'Support for designing (co-operative processes) processes between customer and supplier and third parties'
- 'A standardization accepted by EU level'

From the perspective of Others:

- Need for simplicity
  - KISS = Keep it Simple and Stupid... Seriously, just like TCP/IP is not perfect, but it works for everyone worldwide. Let's find the simple & standard approach to implement and deploy Cloud services.
- Other
  - Standard, transparent and traceable SLA contracts that are legally imposed and that balance the risk for both the Customer and the provider.
  - We need worked examples especially for some of the most important metrics.
  - Potentially standardized classes of contracts

Quantitative Assessment of Using Data Exchange Format

Org Type	No of Responses	Average Rating
CSP	6	4 – Good
Adopter	4	4 – Good
Other	3	4.33 - Good

Qualitative Assessment of Using Data Exchange Format

From perspective of CSPs:

- 'Highly recommended - this would make such metrics actually usable. Otherwise, customer has too many SaaS vendors to deal with to calculate things manually.'
- 'There may need to be some flexibility in the values i,e, dependent on usage or times of day or days of week, or exceptions.'
- 'Who is this aimed at? The majority of clients will be in the S & M [SME] bracket and won't require this level of detail'

From the perspective of Adopters: No comments

From the perspective of Others:

- 'Can be machine readable and processable, however an actual text should be there also. standardized fields should exist for generic processing tools to be created'

8 REFERENCES

[1] COM(2012) 529 final: "Unleashing the power of cloud"
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[2] The European Cloud Partnership
https://ec.europa.eu/digital-agenda/en/european-cloud-partnership

[3] ETSI: Cloud Standards Coordination
https://ec.europa.eu/digital-agenda/en/etsi-cloud-standards-coordination

[4] The Cloud Select Industry Group on Service Level Agreements
https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements

[5] The Cloud Select Industry Group on Certification Schemes
https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-scheme

[6] The Cloud Select Industry Group on Code of Conduct
https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

[7] Cloud Computing Expert Group on Research
https://ec.europa.eu/digital-agenda/en/cloud-computing-expert-group-research

[8] Expert Group on Cloud Computing Contracts
http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

[9] ISO
http://www.iso.org/iso/home.html

[10] Cloud Standards Customer Council
http://www.cloud-council.org/

[11] Cloud Industry Forum
http://cloudindustryforum.org/

[12] Document: 'CLOUD COMPUTING AND PRIVATE INTERNATIONAL LAW' (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/final_synthesis_30_april_6th_meeting_en.pdf

[13] Discussion Paper: Data Disclosure and Integrity (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/data_disclosure__integrity_en.pdf

[14] Meeting DG Justice 30/04 (synthesis)
http://ec.europa.eu/justice/contract/files/final_synthesis_30_april_6th_meeting_en.pdf

[15] Document: 'AVAILABILITY' (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/expert_groups/availability_working_paper_en.pdf

[16] Document: 'LIABILITY FOR NON-PERFORMANCE INCLUDING REMEDIES' (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/expert_groups/liability_working_paper_en.pdf

[17] Document: 'CONTROL AND USE OF CONTENT' (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/expert_groups/control_use_working_paper_en.pdf

[18] Working paper on 'Switching - Transfer and deletion of data after the end of the relationship' (DG Justice expert group)
http://ec.europa.eu/justice/contract/files/expert_groups/switching_working_paper_en.pdf

[19] Cloud Service Level Agreement Standardisation Guidelines (C-SIG on SLAs)

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

[20] Practical Guide to Cloud Service Agreements Version 2.0 CSCC
April 2015 http://cloud-council.org/CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf

[21] SLALOM Questionnaire and analysis

[22] ENISA: Survey and analysis of security parameters in cloud SLAs across the European public sector
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector 2011-12-19 ENISA

[23] Cloud Industry Forum Code of Practice COP Detailed Overview
cloudindustryforum.org/code-of-practice/code-of-practice

[24] Dimension data best practices
http://cloud.dimensiondata.com/sites/default/files/comparing_public_cloud_service_level_agreements_0_0.pdf

[25] NIST - 'Cloud Service Level Agreements - Meeting Customer and Provider needs' (National Institute of Standards and Technology)
https://www.nitrd.gov/nitrdgroups/images/3/34/SLA_Overview_FASTER_20140128.pdf

[26] C-SIG Code of Conduct - Dec. 10th, 2013 minutes
https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

[27] C-SIG Code of Conduct - Feb. 12th, 2014 minutes:
https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

[28] DMH Stallard & CIF - Best practice in Cloud Contracts
http://www.dmhstallard.com/site/publications/pressreleases/DMH_Stallard_Best_Practice_guide_cloud.html

[29] Ministry of Justice guidance on Cloud Computing and CJSM
http://www.lawcloud.co.uk/security/law-society-cloud-guidance

[30] Cloud Computing law, edited by Christopher Millard, Oxford University Press, 2013, Chris Reed and Alan Cunningham, Ownership of Information in the Cloud, p. 144, p. 146

[31] Deliverable 6: Cloud Service Provisions Final Report, Gartner
(21/02/2014, engagement 330017337 for the EC).

[32] http://www.northbridge.com/2013-future-cloud-computing-survey-reveals-business-driving-cloud-adoptioneverything-service-era-it

9 ANNEX 1 – Work Done

9.1 Summary

There have been three main thrusts to the work done to determine the requirements in this document:

1. **Assessment of the opportunity for alignment between SLALOM and ISO.** An ISO working group on SLAs (ISO/IEC JTC1 SC38 WG3 Cloud Computing Service Level Agreements) was set up after the proposal for SLALOM was submitted to the EC. Given the strong overlap in content, it was imperative that we assessed the opportunity for alignment, although this alignment work was not anticipated in the proposal. Although the ISO work is still in progress in developing the ISO/IEC 19086 family of standards for cloud computing SLAs, our initial assessment of what SLALOM needed to do was reflected in the electronic handout which is included as ANNEX 2 to this document, and which was the basis for the questionnaire (see sub-point 2) asking for market feedback. The handout itself was also designed as an integral part of the direct feedback process.
2. **Obtaining direct feedback from the marketplace (both CSPs and Adopters).** This was done by direct and telephone interviews, and via questionnaire. See 9.2 below.
3. **Reviewing previous work done.** A comprehensive review of existing work was performed, especially that which has been conducted by the EC or by groups or projects related to it. The full list of sources used is available in section ?. See 9.3 below.

Names of individuals have also been collected who wish to be kept informed about SLALOM, and participate in the feedback phase starting in September 2015.

9.2 Direct feedback from the marketplace

- **Electronic handout.** To facilitate the process of obtaining direct feedback from the marketplace (both CSPs and Adopters), it was essential to have a document which explained the SLALOM project, its objects, scope, and the essential issues about which we needed market guidance. This included in particular the issue about alignment with ISO. The resulting electronic handout is attached to this document as ANNEX 2.
- **Questionnaire.** A comprehensive questionnaire was created to obtain feedback from all types of respondents, using the electronic handout as the basis of many of the questions asked. This was a highly demanding questionnaire, typically requiring 45 minutes or more to complete its 150 questions, in addition to having read the electronic handout. Once we had a number of responses to the full questionnaire, but not as many as we wanted, we produced a shorter version of the questionnaire which did not rely on having read the handout. The list of questions in both questionnaires is given in ANNEX 3. Note that the longer version of the questionnaire gave us particularly useful feedback about SLALOM's proposed final deliverables. Both versions of the questionnaire gave us useful feedback about overall challenges and requirements of the

marketplace, and also about the prioritization of metrics and other contractual provisions. Fifteen responses were received to the full questionnaire, and 21 to the shorter version, for a total of 36 responses.

- **Cloud Expo Europe – March 2015.** A session was given on the SLALOM project at Cloud Expo Europe (the largest cloud computing event worldwide), in the Cloud Industry Forum theatre. Information on SLALOM was also available at the CIF booth. SLALOM consortium members also discussed the project with many other individuals in the Expo and in the CIF awards event for the UK Cloud Awards.
- **Promotion of questionnaire.** The questionnaire was promoted extensively, including to:
    - The CIF membership
    - The CIF Legal panel
    - The CIF provider contact list (over 400 individuals)
    - The full CIF contact list (over 3,000 individuals, both cloud providers and cloud Adopters)
    - Members of the EC's Cloud Special Industry Group – Service Level Agreement Working Group
    - Participants in the EC's SLA Expert Group (from 2012)
    - Several EC project funded under unit E.2
    - The cloud-concertation mailing list maintained by the CloudWatch project
    - A number of adopters identified through the Cloud Expo or generally known to be large adopters (e.g. CERN, ESA)
    - The Internet Research Task Force (IRTF)
    - 25 Top providers identified through internet search.
- **Telephone interviews.** CIF conducted detailed telephone interviews with a number of CIF SME CSP members. The results were included in the questionnaire results.

9.3 Work done – literature review

An extensive desk research of third party material discussing cloud computing contractual and SLA issues was conducted. The majority of the Internet hits were dismissed as 'click-bait', press-releases, amateur blogs and news articles that tended to reproduce key conclusions of other studies. An initial list of 100+ sources were identified for further reading. This was reduced to approximately 25 after initial analysis. Relevant material from these sources was extracted and sorted according to the structure of the MSA. The findings of each source was contrasted and summarised per MSA chapter and contrasted with the findings of the SLALOM questionnaire. The material extracted included perceptions, evidence from the market, hard recommendations to practitioners and proposed Service level objectives and commitments, notably from ISO, the C-SIG on SLAs and the Gartner study on SLAs for the European Commission.

9.4 Profiles of questionnaire respondents

Figure 3 below shows the main breakdown of respondents to the questionnaire by stakeholder category, namely Cloud Service Provider (CSP), Adopter (also referred to as End-User or Cloud Service Consumer), and a third category of 'Other', which was expected to be primarily for associations or other organizations concerned with cloud service agreements in a primary capacity not directly as a provider or consumer.

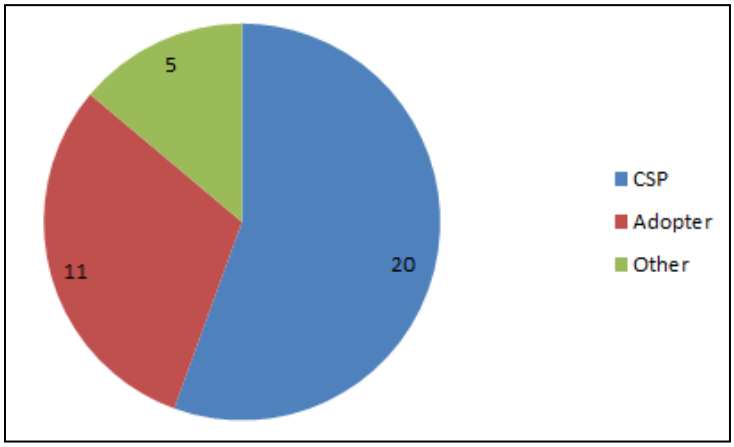


Figure 3: Questionnaire Respondent Types

Figure 4 below shows the breakdown by number of employees of CSP respondents. It may be noted that the majority of respondents are Small and Medium Enterprises (SMEs), with one respondent just above the size of an SME, and with only one CSP respondent which is enterprise-sized.

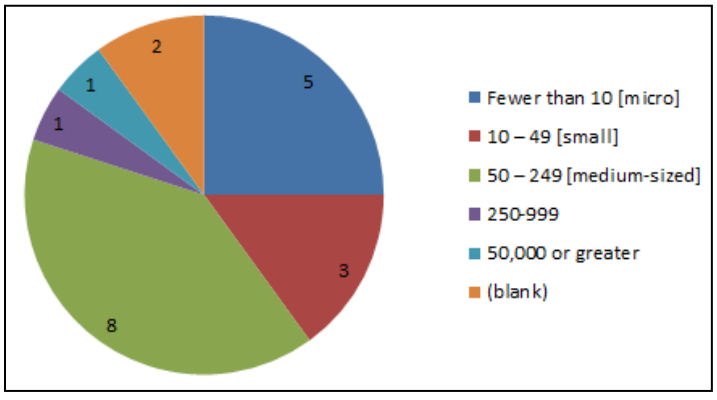


Figure 4: CSP Respondents by Size

Figure 5 below shows the breakdown by number of employees of Adopter respondents.

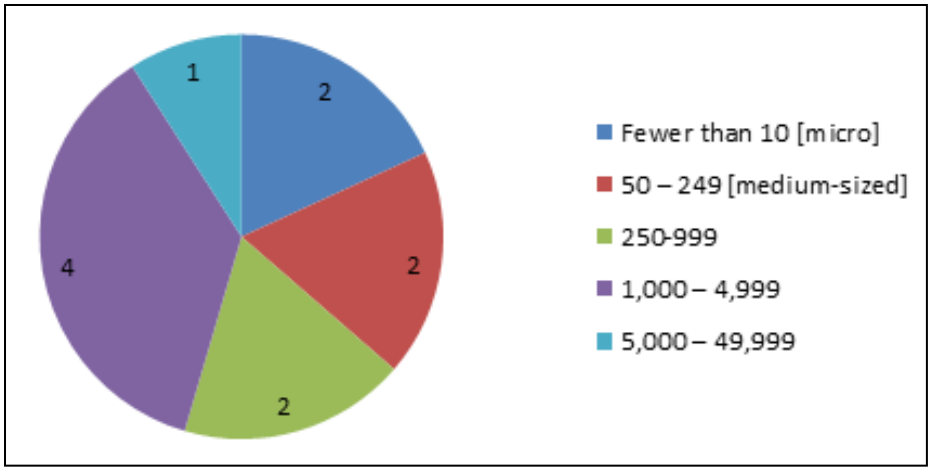


Figure 5: Adopter Respondents by Size

10 Annex 2: The Handout

Note: The link to this electronic handout (not guaranteed for long-term accessibility) is http://bit.ly/SLALOMeHandout

SLA Model Terms and Specifications:

SLALOM Project Overview and Request for Feedback

SLALOM is an initiative aligned with the European Cloud Strategy [1]. The first phase of the initiative is an 18-month, EC-funded project[6] whose objective is to create a Service Level Agreement (SLA) reference model consisting of model contractual terms and model technical specifications.[7] It seeks to provide clarity and reassurance to the market through establishing a baseline of fair and balanced provisions for cloud SLAs. They can be adopted by most cloud service providers and consumers without great expense yet providing a high level of trustworthiness. The benefits to industry include greater uptake of cloud computing by reducing the recognized [2] barrier to adoption of lack of trust and consequent risk.

The purpose of this document is to give an overview and provide examples of the proposed model terms and specifications, and to ask for market feedback in order to confirm or modify the proposed work. The on-line questionnaire accompanying this document will be available at bit.ly/SLALOMWantsToKnow until 31 March 2015.

Some of the key issues about which market feedback is requested are:

[6] SLALOM ("Service Level Agreement - Legal and Open Model") is a support action project funded by the European Commission through the Horizon 2020 research programme, with Grant agreement no: 644270. Its consortium comprises: ATOS SPAIN (project lead), Bird & Bird (responsible for the legal track), the National Technical University of Athens (responsible for the technical track), the Cloud Industry Forum (responsible for liaison with the Cloud Service Provider community), and the University of Piraeus (responsible for liaison with the Cloud Adopter community). The project runs for 18 months from 01/01/2015.

[7] The brief of SLALOM is provide two SLA reference models for cloud computing. The first is a set of common legal clauses to cover cloud SLAs and contracts. The second is a standard technical SLA specification. The models cover both current market practice and scenarios emerging from research. The project will find consensus between stakeholders and determinedly promote the models' adoption. The project will use its position to proactively support all community projects researching either cloud computing or cloud-related SLAs.

- Structure and format of models: How can the project deliverables be presented so that they are as practical and easy to use as possible? Can improvements be made on the structure and format of the examples presented?
- Core coverage: How broad should core coverage be? What is considered core? How can it be prioritized? To what extent might "core" depend on the market sector and type of cloud used?
- Coverage of scenarios emerging from research: There are a number of topics arising from research which could be addressed including in hybrid, federated and 'fog' clouds, as well as automated SLA management frameworks. What are the market views about these topics and the amount of coverage they should be given?

1 Contents

1.1 Scope

SLALOM is a long-term initiative to develop model contractual terms and technical specifications for all cloud computing areas, including emerging and future developments.

The current (and initial) phase of SLALOM is an EC-financed project with the following scope:

- Model contractual terms for cloud computing contracts at the Master Service Agreement (MSA) level, i.e., a legal scope for cloud computing contracts in general.
- Model contractual terms and technical specifications for Service Level Agreements (referred to by the MSA), i.e., a more extensive remit but just for Service Level Agreements.

It should be noted that SLALOM is much more than just SLAs, both in this current project and long-term. Consequently, its scope exceeds that of the proposed ISO/IEC 19086 family of standards for Cloud SLAs. However, for the purpose of SLAs, its scope is closely aligned to these standards. See the section on 'Alignment to ISO' for further details.

1.2 Model terms

Model terms are planned at least for the following areas at the Master Service Agreement level (the list is not exhaustive):

- Obligation to Provide Services
- Quality of Service (Reference to SLA Attachment)
- Obligation of The User
- Consideration
- Intellectual Property
- Liability 0f The Parties
- Term and Termination
- Confidentiality Obligations
- Warranties
- Indemnification
- Data Protection
- Law of the Contract
- Jurisdiction

The intention is to draft a template for each section. This will provide the necessary clauses which will be drafted in accordance with legal practice and balancing the rights of each party, taking into consideration the work of expert groups that have debated the issues, such as the group managed by the Justice Directorate of the European Commission. [3]

The following examples show how SLALOM will approach each of the model contractual terms, identifying deficiencies in current practice and establishing a new, fair and unambiguous definition. All examples are from the Master Service Agreement level.

1.2.1 Example 1: Provision of Services

Many cloud computing Master Service Agreements include a clause along the following lines:

> "***Provision of Services"***
>
> *The client may access and use the Service in accordance with this Master Service Agreement*

It could appear there is not an obligation in charge of the provider to supply the services.

A SLALOM-type of clause would be as follows:

> *"**Provision of Services"***

1. *The Provider shall provide the Services to the User for the Term in accordance with the SLA under Attachment [●] and the terms and conditions of this Master Service Agreement.*
2. *The User shall access and use the Services in compliance with all applicable laws and regulations, the Acceptable Use Policy and according to the terms and conditions of the present Master Service Agreement".*

1.2.2 Example 2: Liability including for non-performance against SLA requirements

Several Master Service Agreements provide a wording similar to the following concerning liability issue:

> *"The Provider will not be liable to the User for any direct, indirect, incidental, special, consequential or exemplary damages (including damages for loss of profits, goodwill, use, or data), even if the Provider has been advised of the possibility of such damages. The Provider will not be responsible for any compensation, reimbursement, or damages arising in connection with: (a) User's inability to use the Services, including as a result of any (i) termination or suspension of this Master Service Agreement or User's use of or access to the Service offerings, (ii) Provider's discontinuation of any or all of the Service offerings, or, (iii) without limiting any obligations under the SLA, any unanticipated or unscheduled downtime of all or a portion of the Services for any reason. In any case, the Provider's aggregate liability under this Master Service Agreement will be limited to the amount the User actually pays to the Provider under this Master Service Agreement for the Service that gave rise to the claim during the 12 months preceding the claim".*

1.2.3 SLALOM can provide different liability clause options:

1° Class Liability: full liability of the provider. Sample clause:

"*The Provider will be liable to the User for the claim, damages and consequences deriving from the breach by the Provider of its material obligations under this Master Service Agreement*".

2° Class Liability: medium liability of the provider (areas of exclusion/limitation to the amount of damages):

> "*The Provider will be liable to the User for any direct damages deriving from the material breach by the Provider of the following obligations under this Master Service Agreement: section [●]. The Provider shall be liable to the User for any direct damages deriving from the material breach of its obligations under Section [●], it being understood that the Provider's aggregate liability deriving from the breach of aforesaid obligations will be limited to the amount the User actually pays us under*

this Master Service Agreement during the 3 months preceding the claim. In any case the total aggregate liability of the Provider under the present Master Service Agreement shall not exceed the amount the User actually pays to the Provider under this Master Service Agreement during the 12 months preceding the claim".

3° Class Liability: total exclusion of liability of the provider except payment of provided penalties.

"*To the extent permitted by the law, the Provider, save for the payment of the penalties deriving from the failure in fulfilling the SLA, shall not liable to the User for any consequences, claim, damages suffered by the User deriving from the breach by the Provider of its obligations and warranties under this Master Service Agreement*".

The Provider and the User will be able to clearly know the "Class of Liability" they are selling/buying

1.2.4 Example 3: Intellectual property rights

SLALOM MSAs will establish a clear set of rules for distinguishing between:

1) IP of the Provider (OS of the platform; SaaS);

Sample clause:

"The Provider and its licensors shall remain the exclusive owners of any and all Intellectual Property Rights ("IPR") connected, deriving or relating to the Services, including without limitations, the Software and the Operating System and all relevant improvements or changes related thereto developed or produced during the execution of this Master Service Agreement"

2) IP of the Users (uploaded data and new works created on the cloud);

Sample clause:

"The User shall remain the exclusive owner of any and all IPR connected, deriving or relating to the Content uploaded by the User on the Provider's server through the use of the Services, as changed, implemented and developed by the User during the Term of the Master Service Agreement. The User authorises the Provider, its officers and employees, to store, copy, transmit and use such Content with the exclusive purpose to provide the Services. The Provider, its officers and employees, shall not be entitled to use above Content for any other scope or purpose"

3) IP of Third-Party (contents, software installed on PaaS or IaaS)

Sample clause:

> *"The User guarantees that the Provider shall have title to use, copy and transmit the User Software or the Third-Parties Software installed on the Provider's servers upon request of the User to provide the Services in accordance with the terms and conditions of the Master Service Agreement. Any other use of the User Software or Third-Parties Software shall be prohibited."*

…providing punctual notification of transfer of IPR from one to the others.

Sample of notification:

> *"This Content/Software is exclusive property of [●]. You will have title to use it for [●] days for the following purpose [●], according to the following modalities [●]".*

1.2.5 Example 4: Protection of personally identifiable information component

SLALOM can provide model rules to cover most of the many multi-jurisdiction privacy and data protection compliance needs, also offering multiple-choices to cover:

1) Sector specific requirements
2) Potential secondary purposes
3) Security related requirements

One of the major issues with privacy and data protection compliance for cloud service customers - especially if based in highly privacy and data protection regulated countries (like the European Countries or some APAC Countries) - arises from cross-border transfers that are a typical way to operate in distributed computing models. Indeed, cloud service customer may be subject to restrictions about the physical location of the cloud service customer data, especially if the location of the personal identifiable information is in third countries that do not offer adequate protection.

It is still quite common to read Master Service Agreements that do not cover explicitly the place where the data centers are or that offer options similar to the following:

"Location of Personal Identifiable Information"

> *"The Provider informs the User about the place(s) of the Provider's data center(s) [and the User can select from which data center the Services will be provided]. The User acknowledges and agrees that the Provider can offer the Services with global resources resident in any of its premises in the world. The User declares and warrants that the Personal Identifiable Information accessible to the Provider in connection with the execution of the Services does not require any export license or that there are no restrictions to the transfer of the Personal Identifiable Information to the Provider's global resources."*

Or

"… The User agrees that the Provider may transfer the Personal Identifiable Information outside the country, both inside and outside the [European Union], to the entities and countries listed in Annex [x] if the Provider so deems it appropriate or useful to provide the Services…"

The cloud service customer should be offered being informed in advance in case of possible transfer of the Personal Identifiable Information and be materially offered the possibility to keep control over the data and taking the necessary steps preventing breaches of its privacy and data protection obligations:

"Location of Data Centers" (sample)

"For the purposes of the provision of the Services, the Provider shall store the User's data in the countries and on the infrastructures identified in the Annex [x], unless the User requests in writing that the data center(s) delivering the services are based in [y].

If the Provider initiates a change to the then-current storage location(s) resulting in a new or additional country of storage of User's data, the Provider will inform the User by advance notice of [x] days, unless the location change has been requested, authorized, or elected by the User, and provided that the User is in the position to obtain the prior authorizations/license from the competent authorities, if so required by the applicable law, or to terminate the Agreement.

The transfer of the User's data out of the European Union/APAC shall be governed by the Standard Contractual Clauses or any equivalent legal basis (BCRs/CBPR/EU-US Safe Harbor or EU-Swiss Safe Harbor)."

1.2.6 Example 5: Expiration and Termination – Exit Process

Sample clause:

"*The Master Service Agreement commences on the Effective Date and will remain in force for [●] years unless terminated in accordance with this clause.*

Each Party shall have the right to terminate the Master Service Agreement or some specified Service, at any time for convenience upon 15 days written notice to the other Party.

A Party may terminate this Master Service Agreement for cause: (i) upon 20 days written notice to the other Party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the Provider fails to respect the SLA under Point [●] of Attachment [●] more than twice in a month; (iii) if the other Party ceases or threatens to cease its business activity.

At the termination or expiration of the Agreement, the Provider shall continue to store and make available to the User the Content for 60 days after the expiration or termination date, allowing the User to download or retrieve them.

Upon request of the User, the Provider shall assist the User in the migration of the Content or Third-Party Software in order to enable the User to have the Services provided by a third party provider or to manage/use them autonomously. As consideration for such assistance, the User shall pay the Provider the due amount in accordance with the hourly rate under Attachment [●] to the Master Service Agreement".

1.3 Model specifications

Technical specifications related to SLAs will typically be defined in a separate document from the Master Service Agreement (MSA). Nonetheless, they will usually be included in the agreement by reference, and therefore have equivalent force (unless overridden by clauses in the main agreement).

Because of the highly technical nature of such specifications, how they are defined in terms of content can be challenging. Significant reliance must be placed on clear definitions of terms. Because SLALOM intends to align its work with ISO, it is intended to use ISO definitions wherever they exist or are being developed.

Because of the early stage of SLALOM's work, we do not yet have worked examples of technical specifications (i.e. of metric definitions) to show. The most likely approach we will adopt is that defined in the working draft of ISO/IEC 19086-2 (metrics) [4]. We are asking for feedback (via the questionnaire) about the usefulness of this proposed approach.

Note that if a well-structured approach is followed rigorously, then it should be possible to implement metric specifications in a way which supports automation, such as using XML.

The working draft of ISO/IEC 19086-2 defines the following templates for cloud service level metrics[8]:

1.3.1 Abstract Metric Definition Template

Abstract Metric (required)

name (required)

referenceId (required)

unit (required)

scale (required)

[8] Text from the working draft of ISO/IEC 19086-2 is © 2015 ISO/IEC

expression (required when underlying AbstractMetrics are used)

definition (required)

note (optional)

Abstract Metric Rule Definitions (optional)

name (required)

referenceId (required)

definition (required)

note (optional)

Abstract Metric Parameter Definitions (optional)

name (required)

referenceId (required)

parameterType (required)

definition (required)

note (optional)

underlyingAbstractMetrics (required when AbstractMetric is composed)

name (required)

referenceId (required)

1.3.2 Concrete Metric Definition Template

Metric (required)

name (required)

referenceId (required)

note (optional)

Primary Abstract Metric (required)

name (required)

referenceId (required)

Metric Rules (required if primaryAbstractMetric is associated with RuleDefinitions)

value (required)

ruleDefinition - referenceId (required)

note (optional)

Metric Parameters (required if primaryAbstractMetric is associated with RuleDefinitions)

value (may be set during use of the Metric)

parameterDefinition - referenceId (required)

note (optional)

1.4 Alignment to ISO

1.4.1 General

SLALOM will align its work to the extent practical to the ISO standards currently under development for Cloud Service Level Agreements. This section of the questionnaire asks for feedback about the overall structure and content of ISO's work as proposed. It is not necessary to know anything about ISO to give meaningful feedback. Indeed, it is particularly valuable to have feedback from people who are not knowledgeable about ISO work to validate that the proposed structure and content make sense from an ordinary commercial perspective.

ISO has created a working group specifically for Cloud Service Level Agreements, which is currently working on three Cloud SLA standards.[9] It is the intention of SLALOM to make its SLA work consistent

[9] ISO/IEC JTC1 Subcommittee 38 Working Group 3 (SC38 WG3) Cloud SLAs. The three standards currently being worked on are:

- ISO/IEC 19086: SLA framework and terminology – Part 1: Overview and concepts, at the Committee Draft stage

with this ISO work, and SLALOM has applied for a liaison relationship with that working group to facilitate this alignment.

SLALOM proposes to use the structure of the proposed ISO/IEC 19086-1 as the basis for its SLA work. While the draft standard makes it clear that this structure is not required for SLAs or contracts, nonetheless it provides a reasonable basis for SLALOM's SLA reference models, one which will be internationally recognized.

SLALOM will diverge from the ISO/IEC 19086 family of standards as regards the full scope of model terms at the Master Service Agreement level, notwithstanding that many of these terms do apply to SLAs. Some of this MSA-level SLA coverage furthermore goes beyond what is proposed in ISO/IEC 19086, e.g. in the following areas:

- Cloud SLA management, including the consequences of violation of SLA provisions (payment of penalties, termination of the MSA, etc.)
- Liability (with respect to service level issues)

Additional such issues may be identified during the course of SLALOM's work.

SLALOM also proposes to use relevant ISO definitions where they exist, with particular emphasis placed on ISO/IEC 17788:2014 Cloud computing — Overview and vocabulary; and on parts 1, 2, and 3 of ISO/IEC 19086: SLA framework and terminology. We will propose additional definitions where needed, but with the expectation that ISO definitions will eventually take their place.

Market feedback on this structure will be given to ISO and well as being used by the SLALOM project.

1.4.2 Structure

The ISO SLA structure is given in the drafts of the ISO/IEC 19086 family of standards.[10] The structure given in Committee Draft 1 of ISO/IEC 19086-1 is shown below in **bold**. Those additional components or details which are identified as 'core' in the draft ISO/IEC 19086-3 are shown in *italics*. Note that 19086-3 is at an earlier draft stage, and more likely to evolve, but 19086-1 is also expected to evolve further, in particular to take account of issues recognized during the development of 19086-3.

The questionnaire accompanying this document asks for feedback on which components are 'core', which are the most important, and which are possibly excessive.

- **Covered services component**
- **SLA definitions component**
- **Service monitoring component**

- ISO/IEC 19086: SLA framework and terminology – Part 2: Metrics, at the Working Draft stage
- ISO/IEC 19086: SLA framework and terminology – Part 3: Core requirements, at the Working Draft stage

[10] The text shown from the drafts of ISO/IEC 19086-1 and ISO/IEC 19086-3 is © 2015 ISO/IEC.

- *Monitoring parameters*
- *Monitoring logs*

- **Roles and responsibilities component**
  - *Responsibility list*
- **Accessibility component**
  - *Accessibility standards*
  - *Accessibility policies*
- **Availability component**
  - *Total downtime*
  - *Availability*
  - *Availability percentage*
  - *Uptime*
  - *Uptime percentage*
  - *Allowable downtime*
  - *Downtime*
- **Cloud service performance component**
  - *Cloud service response time component*
    - *Cloud service response time observation*
    - *Cloud service response time mean*
    - *Cloud service response time variance*
    - *Nth percentile of response time*
    - *Cloud service response time over threshold*
    - *Delay duration time*
  - *Cloud service capacity component*
    - *Number of simultaneous cloud service connections*

        - *Limitation of available cloud service resources*
        - *Cloud service throughput*
        - *Cloud service bandwidth*
    - *Elasticity component*
        - *Elasticity*
        - *Speed*
        - *Precision*
- **Protection of personally identifiable information component**
- **Information security component** *[o/s to be defined]*
- **Termination of service component**
    - *Notification of service termination*
    - *Return of assets*
- **Cloud service support component**
    - *Support plans*
    - *Support costs*
    - *Support methods*
    - *Support contacts*
    - *Support hours*
    - *Service outage support hours*
    - *Service incident notification*
    - *Service incident reporting*
    - *Service incident notification time*
    - *Maximum incident resolution time*
- **Governance component**
    - *Regulation adherence*

- *Standard adherence*
- *Policy adherence*
- *Audit schedule*
- *Number of failed SLOs*

- **Service reliability component**
  - *Service resilience/fault tolerance component*
    - *Time to service recovery (TTSR)*
    - *Mean time to service recovery*
    - *Maximum time to service recovery (MTTSR)*
    - *Number of service failures*
    - *Network redundancy*
  - *Customer data backup and restore component*
    - *Backup method*
    - *Backup interval*
    - *Backup verification*
    - *Backup restoration testing*
    - *Backup restoration test reporting*
    - *Retention period for backup data*
    - *Number of backup generations*
    - *Alternative methods for data recovery*
  - *Disaster recovery component*
    - *Cloud service provider disaster recovery plan*
    - *Recovery time objective (TRO)*
    - *Recovery point objective (RPO)*

- **Data management component**

- *Intellectual property rights component*
- *Cloud service customer data component*
- *Cloud service provider data component*
- *Account data component*
- *Derived data component*
- *Data portability component*
- *Data deletion component*
  - *Data deletion process*
  - *Data deletion notification*
  - *Data deletion time*
- *Data location component*
  - *Data location*
  - *Data location specification capability*
- *Data examination component*
- *Law enforcement access component*

- **Attestations, certifications and audits component**
  - *Cloud service attestations*
  - *Cloud service certifications*
  - *Cloud service audits*

1.5 Coverage of scenarios emerging from research

One of the provisions of the original SLALOM proposal was that it would include coverage of scenarios emerging from research. We need feedback to assess the importance the market attaches to different areas of research to determine the relative emphasis we should place on these areas in our final deliverables. Some of the major areas of SLA research which are not (clearly) reflected in the ISO structure above are:

- SLAs at different levels
- Multi-level SLA interaction model

- SLA negotiation across multiple layers
- Automated SLA re-negotiation
- Proactive SLA violation detection

Short descriptions of these research areas / outcomes along with potential uses are summarized in the following paragraphs.

SLAs at different levels

Anastasia - focused on the media domain - would like to obtain a cloud service but as a non-technical user, she can only specify terms at a “high-level” (i.e. not related to resource attributes such as CPU or memory). She wants to specify terms at her own “understandable language” level (e.g. frames per second) so that these terms will be translated to the corresponding technical ones.

The IRMOS EU project has proposed two types of SLAs, namely application and technical along with a mechanism for performing the required translation between these agreements.

Multi-level SLA interaction model

Irene is a data analyst in a financial trading company. She aims at utilizing resources / services offered from two different providers, as her service is both computational- and data-intensive and different providers offer the corresponding “best” services. To this end, a model for cloud federations is required. The model is based on automated SLA offer generation and enables the user to negotiate an SLA with the federation and the federation looks for the best way to satisfy it by negotiating SLAs with one or more providers (on behalf of the user).

The CONTRAIL EU project has proposed an approach for SLAs in multi-provider environments, including a scheme for SLA splitting, which allows for service-, resource-, or performance-based SLA splitting and revenue sharing / compensation provision.

SLA Negotiation across multiple layers

Yannis is a doctor and would like to deploy his eHealth application in a cloud environment. The application requires workflow management that highlights the need for software-layer negotiation on top of the infrastructure-layer negotiation. What is more, the negotiation process across these two layers should be transparent, while domain-specific (i.e. medical) knowledge should also be incorporated in the SLA lifecycle without additional human intervention.

The SLA@SOI EU project implemented a framework that enables different protocols to be injected through an engine, so as to facilitate the interaction between the different layers and entities. Since the protocol will be used for specific interaction, it may include domain specific content.

Automated SLA re-negotiation

Michael is an entrepreneur who has developed a new tourist service that mixes virtual and augmented reality. As an interactive real-time application, there are specific requirements (towards the cloud

infrastructure that hosts it) which however change during runtime based on the number of end-users. His goal is to sign a contract with a provider, which will allow automated re-negotiation during runtime without human intervention. The re-negotiation should also address cases where the causes and origin of an agreement violation could be addressed by establishing again a process of negotiation.

The IRMOS EU project has developed an SLA re-negotiation mechanism that can be triggered either by the user (e.g. change in application parameters), by one of the providers (e.g. detection of potential SLA violation) or by the application (e.g. elasticity rules). The mechanism allows for automated re-negotiation during runtime without human intervention.

Proactive SLA violation detection

Gabriel is a computer engineer at the operation center of a publication transportation company. The operation center software has been deployed and is running on a cloud infrastructure. There are specific requirements for downtime (near zero) and availability of these mission critical services. Therefore, he sets explicit values for the aforementioned terms and requires “proactive” mechanisms that will protect his application from any performance degradation or failure.

The VISION Cloud EU project has proposed a proactive SLA violation detection mechanism that bases estimations on the analysis of monitoring data. The analysis enables discovering of repetitive patterns and identification of potential relationships between the different parameters to identify dependencies that may affect the evolution of the parameter values during runtime.

Feedback on these, and on any other unmentioned areas of SLA research, is requested via the questionnaire.

1.6 Annex A: About SLALOM

SLALOM: Building a common model for cloud computing SLAs

Slalom is a new European initiative that seeks to remove uncertainty in cloud computing SLAs through standard models. The initiative was launched in January 2015 with the mission to help drive the uptake of cloud services with service level agreement (SLA) model legal clauses and technical specifications.

Industry analysts repeatedly point to uncertainty around legal issues as a major barrier to cloud adoption. Questions such as *who owns my data when I place it in the cloud? What happens if the service provider goes bust? What happens to my applications and data if I miss a payment?* And *which jurisdiction governs my contract*? are common and legitimate questions posed by businesses every day, and these issues are the tip of the iceberg. Furthermore trying to compare providers can become complex when metrics are not uniformly defined. Without like-for-like comparisons, it is difficult to determine the true value proposition, which providers are selling.

A number of groups at European and International scale, such as the European Cloud Partnership and ISO are working towards the standardization of cloud SLAs, debating the distribution of responsibilities between the actors and identifying critical issues that should be addressed. SLALOM is going further, by generating an open and ready-to-use set of model SLA contractual terms and technical specifications for metrics. Adopters will have significant assurance because of using a trustworthy base, which is practical, fair, and understandable, while saving time and resources.

> *"SLALOM will take theory to practice, providing a trusted verifiable starting point for providers and business users to negotiate SLAs for doing business in the Cloud in a simple, fair and transparent way."*
>
> Daniel Field, Project Coordinator, Atos

The initiative is backed by the European Commission and the first stage of the initiative is financed through the H2020 programme, running for 18 months with a budget of 700,000 Euros. The initial members of the SLALOM consortium are global service provider ATOS (project lead), legal firm Bird and Bird (responsible for the legal track), the National Technical University of Athens (responsible for the technical track), the Cloud Industry Forum (responsible for the cloud service provider liaison track) and the University of Piraeus (responsible for the cloud adopter liaison track). External collaborators and contributors are welcome.

For more information on the initiative contact the coordinator Daniel Field (daniel.field@atos.net), or visit our website slalom-project.eu. SLALOM is funded by the EC under Grant agreement 644270.

1.7 Annex B: Reference materials and further reading

A number of (non-exhaustive) further avenues are listed below for readers who wish to better understand the gamut of initiatives taking place in this area within the European Commission. Additionally readers interested in collaborating or becoming involved in this work are invited to contact the SLALOM consortium directly.

The European Strategy on Cloud Computing

In September 2012, the EC published a document entitled "Unleashing the Potential of Cloud Computing in Europe" [1], which identified what the potential impact of cloud on the economies of Europe was, and then identified some steps which should be taken to capture the benefits.

The European Cloud Partnership

One of the actions of this strategy was to establish the European Cloud Partnership [5]. This is a board of executives and representatives from member states.

The ECP produced a report [6], entitled "Establishing a Trusted Cloud Europe", which identified two groups of actions:

- creation of a flexible common framework of best practices, and
- systematic consensus building.

The Cloud Select Industry Groups

The ECP also established a number of Cloud Select Industry Groups (C-SIGs). The C-SIG on SLAs has produced a sequence of 3 reports:

- A short report, produced by Atos, describing 11 key SL indicators;
- A much more comprehensive document from Gartner, including many details derived from their standard texts on cloud service levels;
- A smaller Task force of 5 organisations, each addressing particular aspects of the subject: Performance, Security, Data Management, Personal Data Protection;
- A detailed set of guidelines for SLA standardisation published in June 2014.

A further EC expert group is working on cloud computing contracts, debating the fairness and conflicting perspectives on the clauses regularly found in cloud contracts [3].

ETSI actions on cloud standards

As a further action under the EC cloud Strategy, the European Telecommunications Standards Institute (ETSI) was tasked with "cutting through the jungle of standards", and map existing cloud computing

standards in collaboration with all relevant stakeholders. That working group produced a useful analysis [7] of the applicable standards within the arena of cloud.

European Projects

Over recent years a number of European research consortia have investigated and applied SLA lifecycle management frameworks in the context of cloud computing. An expert group was formed by the European Commission to survey the research outcomes stemming from these projects, and to discuss how these outcomes address the complete SLA lifecycle. Their conclusions were published in June 2013. This report also provided a set of recommendations to support the on-going policy work on SLAs of the Cloud Select Industry Group (SIG), while identifying the research outcomes that can be exploited for the implementation of the recommendations [8].

Additionally, a number of grants have been awarded to research consortia to investigate specific aspects legal, security and data protection in Cloud computing. These include:

The **CIRRUS** project, which delivered recommendations on cloud security standards, certification schemes, as well as international cooperation. In addition a CEN workshop agreement on cloud security assurance has been launched, with an eye on future cloud trends and models. The CIRRUS Green paper is used as the input to several EU trusted cloud initiatives: http://www.cirrus-project.eu/

SLA-READY is a project initiated in January 2015. The consortium aims to make cloud customers, especially small- and medium-sized enterprises (SMEs), SLA-aware, educating and advising them on SLAs. SLA-Ready gives businesses “pain relief” from the SLA challenge, reducing risks and creating certainties. http://www.sla-ready.eu/

The **CUMULUS** Initiative, which collects multiple types of evidence regarding security, including service testing and monitoring data and trusted computing proof. It has models for hybrid, incremental and multilayer security certification with different levels of automation in the certification process steps. http://www.cumulus-project.eu/

The **Coco-Cloud** project, which is delivering machine readable data sharing agreement (DSA) that can define how user data is used, for which purpose and in which context. The main achievement is, however, the automated enforcement of these agreements in the cloud, as well as the contribution to automated evidence-based audits of privacy policies. http://www.coco-cloud.eu/

WITDOM, a group whose research goal is to protect sensitive data in cloud cryptographically, by applying the privacy-by-design paradigm. WITDOM's data protection methods will be tailored to the risks associated with different classes of data. http://www.witdom.eu/

1.7.1 References

[1] Unleashing the potential of Cloud Computing in Europe, COM(2012) 529 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[2] IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake.
http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

[3] http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

[4] ISO/IEC 19086: SLA framework and terminology – Part 2: Metrics, SC38 WG3 N56, version with WG3 comments on CSA expert contribution on 19086-2, uploaded 23 January 2015.

[5] http://ec.europa.eu/digital-agenda/en/european-cloud-partnership

[6] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

[7] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

[8] http://ec.europa.eu/digital-agenda/en/news/cloud-computing-service-level-agreements-exploitation-research-results

12 Annex 3: The questionnaire

This is a list of all questions in both the full and short questionnaires, and an associated reference number which is used to facilitate reference to the questions in the analyses. The type of answer which could be given is shown. An asterisk ('*') indicates that the answer could have been chosen from 'highly unimportant', 'somewhat unimportant', 'somewhat important', 'highly important (core requirement)', or left unanswered. Where a question is only in the full or short questionnaire, this is also indicated.

Questions preceded by 'FULL' or 'SHORT' were only asked in the full or shortened questionnaire, respectively.

005 What type of organization is yours, primarily, with respect to cloud services? [choice]

006 If your organization is a cloud service provider, which best describes your channel? [choice]

007 If yours is an end-user organization, in which sector does it primarily operate? [choice]

008 How many employees are there in your immediate organization (determined from the perspective of reasonably independent control in providing or using cloud services)? [choice]

009 FULL: If your organization is part of a larger organization or group, how many employees does the overall organization have? [choice]

010 What is the ownership of your organization? [choice]

011 FULL: With which of the following do you have experience? [choice]

012 FULL: If other cloud-based services please specify` [free-format comment]

013 FULL: Please classify your personal level of experience/expertise concerning cloud Master Service Agreements? [choice]

014 FULL: Please classify your personal level of experience/expertise concerning cloud Service Level Agreements? [choice]

015 Geographically where are you, personally, based? [drop-down choice]

016 How critical are the cloud services you are concerned about? [choice]

017 What are your organization's key constraints for its increased provision/use of cloud computing? [free-format comment]

018 To what extent do you consider contract and SLA-related issues as inhibiting your organization's increased provision/use of cloud computing? [free-format comment]

019 FULL: Please provide a quantitative assessment of the appropriateness and usability of the presentation of model terms given in the examples. [choice: v good, good, poor, v poor]

020 FULL: Please provide an overall assessment of the appropriateness and usability of the presentation of model terms given in the examples. [free-format comment]

021 What is your biggest 'pain point' regarding cloud computing contracts? [free-format comment]

022 FULL: What is your second biggest 'pain point' regarding cloud computing contracts? [free-format comment]

023 FULL: Please provide a quantitative assessment of the appropriateness and usability of the metrics template shown. [choice: v good, good, poor, v poor]

024 FULL: Please provide an overall assessment of the appropriateness and usability of the metrics template shown. [free-format comment]

025 What is your biggest 'pain point' regarding SLAs? [free-format comment]

026 FULL: What is your second biggest 'pain point' regarding SLAs? [free-format comment]

027 FULL: Please provide your highest priority recommendation for improvement in model specifications. [free-format comment]

028 FULL: Please provide your 2nd highest priority recommendation for improvement in model specifications. [free-format comment]

029 FULL: Please provide a quantitative assessment of the potential value of model specifications using a data interchange format such as XML. [choice: v good, good, poor, v poor]

030 FULL: Please provide any comments you may have about the idea of model specifications using a data interchange format such as XML, and about the relative desirability of any other data interchange formats. [free-format comment]

031 SHORT: Before commenting on the ISO proposals, please summarize which, in your view, what are the most important service level metrics for you and for cloud computing overall? [free-format comment]

032 Covered services component [Overall] [choice *]

033 SLA definitions component [Overall] [choice *]

034 Service monitoring component [Overall] [choice *]

035 Service monitoring component [/ Monitoring parameters] [choice *]

036 Service monitoring component [/ Monitoring logs] [choice *]

037 Roles and responsibilities component [Overall] [choice *]

038 Roles and responsibilities component [/ Responsibility list] [choice *]

039 Accessibility component [Overall] [choice *]

040 Accessibility component [/ Accessibility standards] [choice *]

041 Accessibility component [/ Accessibility policies] [choice *]

042 Availability component [Overall] [choice *]

043 Availability component [/ Total downtime] [choice *]

044 Availability component [/ Availability] [choice *]

045 Availability component [/ Availability percentage] [choice *]

046 Availability component [/ Uptime] [choice *]

047 Availability component [/ Uptime percentage] [choice *]

048 Availability component [/ Allowable downtime] [choice *]

049 Availability component [/ Downtime] [choice *]

050 Cloud service performance component - cloud service response time component [Overall] [choice *]

051 Cloud service performance component [/ response time observation] [choice *]

052 Cloud service performance component [/ response time mean] [choice *]

053 Cloud service performance component [/ response time variance] [choice *]

054 Cloud service performance component [/ Nth percentile of response time] [choice *]

055 Cloud service performance component [/ Cloud service response time over threshold] [choice *]

056 Cloud service performance component [/ Delay duration time] [choice *]

057 Cloud service performance component - cloud service capacity component [Overall] [choice *]

058 Cloud service performance component [/ Number of simultaneous cloud service connections] [choice *]

059 Cloud service performance component [/ Limitation of available cloud service resources] [choice *]

060 Cloud service performance component [/ Cloud service throughput] [choice *]

061 Cloud service performance component [/ Cloud service bandwidth] [choice *]

062 Cloud service performance component - elasticity component [Overall] [choice *]

063 Cloud service performance component [/ Elasticity] [choice *]

064 Cloud service performance component [/ Speed] [choice *]

065 Cloud service performance component [/ Precision] [choice *]

066 Protection of personally identifiable information component [Overall] [choice *]

067 Information security component [Overall] [choice *]

068 Termination of service component [Overall] [choice *]

069 Termination of service component [/ Notification of service termination] [choice *]

070 Termination of service component [/ Return of assets] [choice *]

071 Cloud service support component [Overall] [choice *]

072 Cloud service support component [/ Support plans] [choice *]

073 Cloud service support component [/ Support costs] [choice *]

074 Cloud service support component [/ Support methods] [choice *]

075 Cloud service support component [/ Support contacts] [choice *]

076 Cloud service support component [/ Support hours] [choice *]

077 Cloud service support component [/ Service outage support hours] [choice *]

078 Cloud service support component [/ Service incident notification] [choice *]

079 Cloud service support component [/ Service incident reporting] [choice *]

080 Cloud service support component [/ Service incident notification time] [choice *]

081 Cloud service support component [/ Maximum incident resolution time] [choice *]

082 Governance component [Overall] [choice *]

083 Governance component [/ Regulation adherence] [choice *]

084 Governance component [/ Standard adherence] [choice *]

085 Governance component [/ Policy adherence] [choice *]

086 Governance component [/ Audit schedule] [choice *]

087 Governance component [/ Number of failed SLOs] [choice *]

088 Service reliability component - service resilience/fault tolerance component [Overall] [choice *]

089 Service reliability component [/ Time to service recovery (TTSR)] [choice *]

090 Service reliability component [/ Mean time to service recovery] [choice *]

091 Service reliability component [/ Maximum time to service recovery (MTTSR)] [choice *]

092 Service reliability component [/ Number of service failures] [choice *]

093 Service reliability component [/ Network redundancy] [choice *]

094 Service reliability component - customer data backup and restore component [Overall] [choice *]

095 Service reliability component [/ Backup method] [choice *]

096 Service reliability component [/ Backup interval] [choice *]

097 Service reliability component [/ Backup verification] [choice *]

098 Service reliability component [/ Backup restoration testing] [choice *]

099 Service reliability component [/ Backup restoration test reporting] [choice *]

100 Service reliability component [/ Retention period for backup data] [choice *]

101 Service reliability component [/ Number of backup generations] [choice *]

102 Service reliability component [/ Alternative methods for data recovery] [choice *]

103 Service reliability component - disaster recovery component [Overall] [choice *]

104 Service reliability component [/ Cloud service provider disaster recovery plan] [choice *]

105 Service reliability component [/ Recovery time objective (TRO)] [choice *]

106 Service reliability component [/ Recovery point objective (RPO)] [choice *]

107 Data management component [Overall] [choice *]

108 Data management component [/ Intellectual property rights component] [choice *]

109 Data management component [/ Cloud service customer data component] [choice *]

110 Data management component [/ Cloud service provider data component] [choice *]

111 Data management component [/ Account data component] [choice *]

112 Data management component [/ Derived data component] [choice *]

113 Data management component [/ Data portability component] [choice *]

114 Data management component [/ Data examination component] [choice *]

115 Data management component [/ Law enforcement access component] [choice *]

116 Data management component - data deletion component [Overall] [choice *]

117 Data management component [/ Data deletion process] [choice *]

118 Data management component [/ Data deletion notification] [choice *]

119 Data management component [/ Data deletion time] [choice *]

120 Data management component - data location component [Overall] [choice *]

121 Data management component [/ Data location] [choice *]

122 Data management component [/ Data location specification capability] [choice *]

123 Attestations, certifications and audits component [Overall] [choice *]

124 Attestations, certifications and audits component [/ Cloud service attestations] [choice *]

125 Attestations, certifications and audits component [/ Cloud service certifications] [choice *]

126 Attestations, certifications and audits component [/ Cloud service audits] [choice *]

127 FULL: Please provide a quantitative assessment of the appropriateness and usability of the above structure. [choice: v good, good, poor, v poor]

128 FULL: Please provide a written assessment of the appropriateness and usability of the above structure. [free-format comment]

129 Please identify the top component you consider to be missing from the above structure. [free-format comment]

130 FULL: Please identify the second component you consider to be missing from the above structure. [free-format comment]

131 FULL: Please identify the third component you consider to be missing from the above structure. [free-format comment]

132 Please provide your highest priority recommendation for improvement in the above structure. [free-format comment]

133 FULL: Please provide your 2nd highest priority recommendation for improvement in the above structure. [free-format comment]

134 FULL: Please provide your 3rd highest priority recommendation for improvement in the above structure. [free-format comment]

135 Please provide a quantitative assessment of the importance you attach to the following topics being covered in the SLALOM model terms and specifications: [SLAs at different levels] [choice: v good, good, poor, v poor]

136 Please provide a quantitative assessment of the importance you attach to the following topics being covered in the SLALOM model terms and specifications: [Multi-level SLA interaction model] [choice *]

137 Please provide a quantitative assessment of the importance you attach to the following topics being covered in the SLALOM model terms and specifications: [SLA negotiation across multiple layers] [choice *]

138 Please provide a quantitative assessment of the importance you attach to the following topics being covered in the SLALOM model terms and specifications: [Automated SLA re-negotiation]

[choice *]

139 Please provide a quantitative assessment of the importance you attach to the following topics being covered in the SLALOM model terms and specifications: [Proactive SLA violation detection] [choice *]

140 Please provide your highest priority recommendation for another area of research which should be included, and a reference to where more information can be found. [free-format comment]

141 FULL: Please provide your 2nd highest priority recommendation for another area of research which should be included, and a reference to where more information can be found.

142 Where did you learn about this questionnaire? [choice (FULL); free-format comment (SHORT)]

143 FULL: Cloud Industry Forum (please specify e.g. email, website, press release) [free-format comment]

144 FULL: Press Publication (please specify) [free-format comment]

145 FULL: Social Media (LinkedIn, Twitter, …) [free-format comment]

146 FULL: Other (please specify) [free-format comment]

147 Please indicate if you would like to be informed of future developments of the SLALOM project.

148 Name (*) [free-format comment]

149 eMail address (*) [free-format comment]

150 Name of your employer (full organization name) [free-format comment]

151 Any other comments [free-format comment]

13 License

14 Confidential Annex 4 Possible suggestions for ISO

The following annex is relevant to the SLALOM review process but is termed confidential as it is not appropriate to circulate possible suggestions to ISO to a wider audience. SLALOM will decide how and when to present these suggestions to ISO and it is up to ISO to manage them as deemed fit by them.

As a result of the work which has been done by SLALOM, the following types of suggestions could be made to ISO/IEC JTC1 SC38 WG3 for consideration in the development of the 19086 family of standards. This is a summary only, and it will probably be necessary to submit comments using the official commenting template, possibly including a document with alternative text.

- Definitions:
  - Define the term 'service level'. See 3.4.3 for details.
  - Redefine the term 'service level objective' in terms of the definition for 'service level'. See 3.4.3 for details.
- Scope: [See 3.4.3] Clarify in the draft 19086-1 and in related standards the scope differences between
  - Cloud service agreement structural components (covering all aspects of cloud service agreements, including general provisions [covered services, definitions] and potentially optional provisions [e.g. service commitments], and not just components specific to cloud service level agreements); and
  - Measurable service levels and their related service level objectives
- Service support: [See **Error! Reference source not found.**] Define service levels and metrics (not just service commitments) for service support purposes (e.g. time to provision; to respond/resolve service interruptions or to support requests)
- Aligning names with content: Consider renaming both the ISO/IEC 19086 family standards, and also SC38 WG3, from 'Cloud Computing Service Level Agreements' to 'Cloud Computing Service Agreements'