LEGAL & OPEN MODEL TERMS FOR CLOUD SLA AND CONTRACTS

Cloud Providers' Adoption Assessment

D4.2

Dissemination level: Public version

Work Package	**WP4, Provider Track**
Due Date:	M18
Submission Date:	28/06/2016 // updated 19/09/2016
Version:	1.3 public version
Status	FINAL
Author(s):	Breda Beyer (CIF) David Bicket (CIF) Daniel Field (ATOS)
Reviewer(s)	Julia Wells (ATOS)

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

Contents

This document has the following accompanying annexes:

Annex A: Legal overview document

Annex B: Technical overview document

Annex C: Initial determination of requirements

1 Introduction

1.1 Purpose

This document responds to the contractual deliverable D4.2 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.

The purpose of this document is to summarize:

- the dissemination and promotion activities performed so as to raise awareness of the SLALOM models among the cloud providers;
- the received feedback from the cloud providers with respect to both the legal and the technical SLALOM models during each phase of the project;
- the actions performed to assist the project to address the received feedback; and
- the conclusions based on overall feedback and experience of the project

1.2 Project context

The context of the actions taken is defined in the SLALOM contract project summary abstract. This states:

> *SLALOM is a support action tackling the complexity of cloud computing SLAs and contracts through standardization of the SLA and contract terms and a reference model for SLA management. In doing so it will support the adoption of cloud (SLA complexity is an identified barrier to adoption) and support the exploitation of results from the cloud and SLA research communities, effectively by factoring in advances from the research sector into the SLALOM legal and technical models which will be promoted as industry standards.*
>
> *The project will involve interaction with policy makers, cloud providers, research projects and cloud adopters from various areas. There will be significant interaction with the policy groups set up under the European Cloud Partnership and the working groups of the research community. The project will run for 18 months, focusing on three phases – definition of the models; consensus building; and adoption.*

A major factor which is 'context' for the work done, is the fact that ISO started developing standards related to cloud service agreements and cloud service level agreements subsequent to the SLALOM proposal being prepared and submitted to the EC.

The SLALOM partners recognized that this development impacted significantly on the project. In particular:

- The SLALOM legal and technical models would not be credible in the marketplace if they were developed in a way which was incompatible with the work being done by ISO.
- Ensuring that the SLALOM models were aligned with the work being done by ISO would facilitate market uptake.
- SLALOM had an opportunity to ensure that the standards being developed were 'fit-for-purpose' for SLALOM's purposes by contributing to the ISO development work.

The four relevant standards currently being developed by ISO are:

- ISO/IEC 19086-1: Cloud computing – Service level agreement (SLA) framework — Part 1: Overview and concepts. This standard, although described as being for service level agreements, actually covers most topics related to cloud service agreements, but with more information given about topics relevant to service level agreements.
- ISO/IEC 19086-2: Cloud Computing – Service level agreement (SLA) Framework — Part 2: Metric model. This standard is closely related to the technical model. SLALOM has provided input into this model to ensure that it is 'fit-for-purpose' for specifying metrics with the level of precision (i.e., non-ambiguity) considered necessary by SLALOM. The SLALOM model which is built on it is therefore entirely conformant with the ISO model.
- ISO/IEC 19086-3: Cloud computing - Service level agreement (SLA) framework — Part 3: Core requirements. This standard highlights which of the framework provisions specified in Part 1 are considered 'core' and should be in any CSA or SLA.
- ISO/IEC 19086-4: Cloud computing – Service level agreement (SLA) framework — Part 4: Security and privacy. This standard addresses how specifications for security and privacy can be incorporated into contractual documentation.

SLALOM has had input into Part 1, and continues to have input into Part 2.

Participation in this work as a liaison effectively ensured that SLALOM had the opportunity to liaise with many key provider organisations for the subject matter involved. Note that the ISO standards world, especially for cloud computing, has highly active involvement from almost all of the major cloud providers and stakeholders, including NIST, Amazon, Microsoft, IBM, Oracle, Adobe, and many others.

2 Provider outreach strategies

The main goal of WP4 "Cloud Provider Track" was to reach the consensus of the cloud providers, i.e. key provider groups (SaaS, PaaS and IaaS) with respect to the SLALOM models. To this end, a plan of actions had been defined in SLALOM D1.1 [1] to which all SLALOM team members contributed, based on the targets of each project phase (awareness, consensus and adoption) and the main messages to be delivered. The following sections demonstrate how WP4 members delivered on the plan, including adaptations what were required in response to challenges along the way. Those challenges are set out specifically in Section 6.

2.1 Awareness phase

WP4 members designed the Electronic questionnaire and handout materials to be used to gain stakeholder views about their requirements [2]. These were then shared across the project and updated to ensure that the materials accommodated the other stakeholder types, principally end users, policymakers, consultant and lawyers as well as the provider groups

The methods used by WP4 to promote awareness of the SLALOM project among providers included regular communications to the following groups:

- Cloud Industry Forum email lists (over 13,000 individuals, including 4000 provider contacts – other contacts on this list include adopter, legal and policymakers).
- Other Provider led industry associations (Data Centre Alliance and Eurocloud) who agreed to disseminate information in order to support our efforts to recruit provider stakeholders
- Members of the EC's Cloud Special Industry Group – Service Level Agreement Working Group; participants in the EC's SLA Expert Group (from 2013); members of the ISO group working on SLA standards

CIF published two press releases which generated over a dozen news articles in IT publications during the awareness phase

CIF used its contacts and relationships to secure a number of speaking opportunities for the SLALOM project members at events across Europe, including during the initial awareness phase a presentation at CIF's theatre at Cloud Expo Europe (CEE) in London in March 2015, plus the distribution of SLALOM leaflets at the CIF booth. This was the launch event for distributing the questionnaire and handouts to obtain initial feedback from stakeholders.

CIF also provided regular updates on SLALOM at CIF member meetings with a view to recruiting key provider stakeholders.

2.2 Consensus and Adoption phases

During the consensus phase of the project the main target was to communicate the drafted models (technical and legal) to the cloud provider community so that the latter can provide feedback on adjustments that may be needed

Extensive actions were carried out across the SLALOM team to communicate the legal and technical deliverables to stakeholders, requesting feedback. Some highlights below aim to illustrate the participation of WP4 members in these activities targeting provider organisations. A full report of SLALOM dissemination activities is provided in D1.2 [3].

Presentations at conferences, etc. These included, in particular

Eurocloud Annual Conference, Barcelona 15th October 2015– Atos and CIF attended and spoke at this Event to share the results of the project and to encourage participation by SME provider and adopter organisations across Europe in shaping the output.

Cloud Expo Frankfurt 10th November 2015. The speaking slot was obtained by CIF. The presentation was made by Bird & Bird (Gian Marco Rinaldi)

CloudScape 8-9 March 2016. The project attended this conference, attended by many stakeholders including providers and consultants, and had the opportunity to present the work and recommendations of SLALOM, both to the audience and through informal discussion.

Cloud Expo London 12-13 April 2016. The project presented its results to the audience in one of the seminars, as well as distributing information via the CIF stand.

Webinars CIF organised two live webinar sessions to outline the proposals for both the legal and technical tracks and invite feedback as part of the consultation phase. These were:

11th Nov 2015: Public consultation on Cloud SLAs and Contracts – Have your say. A project introduction and legal results presentation for the consultation phase.

26th Nov 2015: SLALOM helps you define metrics for cloud service agreements. An overview of the technical track for the consultation phase.

Due to technical issues CIF was not able to record the first two webinars but they proved to be an effective method for delivering an overview of the legal and technical tracks of the project. Therefore we organised a further two webinars for the Adoption phase of the project which were recorded and uploaded onto the SLALOM website, enabling stakeholders to view them at a convenient time, and thereby encourage participation.

The first recorded webinar called **"Using metrics to improve Cloud SLAs"** was held on April 26th.
The second recorded webinar, **"Ready to Use Cloud Master Agreement for SLAs"**, was held on May 27th.

Both provided examples showing how to practically apply SLALOM to improve current practice. They were also actively announced and promoted within EU Research and Scientific communities.

Online, telephone and physical meetings, in addition to public sessions:

- Circulation to members of the CIF Legal Panel
- Direct 1 on 1 discussions with CIF provider members
- Direct 1 on 1 discussions by ATOS with its own internal organization, and with other providers

There was limited opportunity to obtain adoption assessment feedback on the technical track deliverables from the Provider community in the period to the end of June 2016. This is because the nature of the technical deliverable, meant that the initial deliverables were suited for the research community rather than the provider community.

Interaction with other Research projects

Throughout the Awareness, Consensus and Adoption phases, WP4 members interacted with Research projects to foster consensus and adoption. Some of these projects were initiated through contact with R&D departments of provider organisations participating. Significant interactions included:

- **SLA-Ready**

Informal discussions were held with SLA-Ready experts at various times during the SLALOM project, to coordinate efforts. In particular, the Cloud Security Alliance, an SLA-Ready partner, provided CIF with examples of metric specifications which it had from other projects and sources, and these were passed on to NTUA.

- **CloudWatch2**

CIF reviewed and provided feedback to CloudWatch2 on one of its major deliverables concerning how the IaaS marketplace could become more like a utility. CIF and NTUA personnel also met with CloudWatch2 personnel in London to discuss the two projects.

- **DPSP**

The Data Protection, Security and Privacy (DPSP) in the Cloud Cluster is a group of an EU-funded projects with key objectives on data protection, security and privacy in the cloud. SLALOM established contact with this cluster and collaborated with the organization of the DPSP Workshop 2016 in Napoli (Italy), on 23rd February 2016. This workshop addressed some of the key issues of cloud security and privacy related with EU Digital Single Market strategy as well, and in particular: security level agreements, data sharing agreements, reactive cloud applications, data localization, security of cloud-based public services, secure communication and processing in cloud platforms.

In this regards, SLALOM had an excellent opportunity to present its outcomes in this context. SLALOM was respresented by Gian Marco Rinaldi (Senior Legal Advisor on Cloud SLAs from Bird & Bird) who participated as panelist in the DPSP event discussing on the challenges for (multi-)cloud-based services in Digital Single Market. He emphasized the benefits that SLALOM's legal perspective provides. SLALOM was also represented by David Bicket (CIF). The project delegates established conversations with projects like SPECS, SERECA, MUSA, COCOCLOUD, and CLIPS. It is worth mentiniong that contacts with MUSA project wre initiated here that led to more concrete actions set out below.

- **PICSE**

The European Open Science Cloud envisages a trusted, open environment for storing, sharing and re-using scientific data and results and supporting Open Science practices. The PICSE (Procurement Innovation for Cloud Services in Europe) initiative is relevant for providers as it provides a framework in which they participate. PICSE and SLALOM (driven by ATOS) collaborated in the CloudScape workshop in Brussels, and also in organizing the meeting with DG DIGIT and DG CNCT on 7 March 2016.

- **MUSA-DCA-CSA-CIF Workshop 11 April 2016**

The MUSA Consortium organised a workshop at the premises of CA Technologies in Central London on 11th March 2016 between the Data Centre Alliance (DCA), Cloud Security Alliance (CSA) and the Cloud Industry Forum (CIF).

During this workshop SLALOM outcomes were presented to the MUSA consortium. This also provided an opportunity to communicate with an expert from the Cloud Security Alliance, who is also working in the SLA-Ready project.

3 Initial inputs and position paper (Phase 1 Awareness)

This section summarizes the initial feedback that was received from the cloud providers that responded in the SLALOM questionnaire (awareness phase of SLALOM).

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 providers 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 providers or End-Users. However, they are seen as inhibitors to cost-effective uptake, in particular by SMEs (both provider 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 the provider's perspective, a number of responses indicated their view that inexperience and lack of understanding of potential customers were an issue inhibiting or slowing down cloud uptake. Examples cited by providers include:

- Financial and management concerns of potential customers
- Capex vs opex
- Customer's need to utilize existing infrastructure investment
- Reluctance of IT management to lose control

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.

Based on questionnaire feedback, the proposed approach for the MSA deliverable was 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.

There is a clear prioritization amongst providers 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 providers 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

In relation to components not covered or "missing" from the ISO components, Cloud providers cited the following:

- 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'

Other issues important to Cloud Providers included

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

Full detail of this information is provided in D4.1_5.1 [4] and this was shared across the SLALOM legal and technical tracks to help drive the direction of the proposed models

4 Consensus Phase – Actions addressing the initial feedback (Phase I "Awareness")

This section presents how the received feedback during the awareness and consensus phases has influenced the work of SLALOM and how comments or suggestions have been addressed from the technical and the legal viewpoint.

4.1 From the legal viewpoint

As a result of the extensive promotion activities to encourage feedback, a number of sets of comments were received from providers during the consensus phase and these comments were all passed to the legal track. We discussed with the legal track how we could demonstrate to the reviewers that their comments had been taken into account. As a result of this discussion, the format of the legal deliverable was modified to include a section, for each clause, entitled "Changes to the SLALOM proposed text after feedback".

The Summary below incorporates the analysis of provider's feedback on 2.1 draft legal terms [5] and the adaptations to incorporate such responses. This information is repeated here, only in part, in order to illustrate those clauses where response from providers impacted the subsequent wording of the deliverable.

Each of the Sections below refers to the relevant Section of the Master Service Agreement (MSA) in effect the contractual document which governs the relationship between the parties. This is the document D2.1 to which this provider feedback

Section 2. Provision of Services

Provider's perspective
The Provider could prefer not to establish a clear and precise obligation to provide the services focussing instead on the Adopters obligations relating the use of the services.
Changes to the SLALOM proposed text after feedback
1) In Section 2.1, we replaced the wording "*The Provider shall provide the Services*" with "*The Provider shall make available the Services*" as this wording makes clear that, in most of the cases, the Services are made available for the use of the Adopter and are not unilaterally provided by the Provider regardless of the effective use of the Adopter. The use by Adopter of the Services then has to comply with the Acceptable Use Policy under Attachment 3. The structure of Section 2 should better represent now the usual operating of most cloud computing services.

Section 4. Variation of the Services

Provider's perspective
Depending on the nature of the services, the Provider will be concerned to ensure that:

i) the scope of the services are established at the execution of the cloud computing agreement and cannot be modified or integrated with other systems unless the parties agree on the possible integration and the consequences (financial or operational); and/or

ii) make bug fixes and security patches whenever required; and/or

iii) it has complete discretion to unilaterally develop the services including adding, removing or modifying functionality.

Changes to the SLALOM proposed text after feedback

Further to the feedback received on this Section, we decided to provide significant changes to the relevant provisions.

As the services are very often updated and improved by the providers, the proposed SLALOM model CSA states that the Provider will be entitled to change the services provided that such changes do not determine in any way a reduction of the functionalities or characteristics of the services as they were offered at the effective date of the agreement. If the Provider wishes to reduce the functionalities and characteristics of the services, such changes need to be approved in writing.

As an exception of the above provision, the Provider will be entitled to improve or update the Services in case of improvements or updates necessary to fix defects of the Services or to cure security vulnerabilities of the System (as suggested the DG Justice Group experts, see Deliverable 4.1, Section 4.3); and in case of new laws, regulations acts or orders of the authorities which require changes to the Services. In all these cases, however, if the changes provoke a reduction of the functionalities or characteristics of the Services, the parties must agree a fair and proportionate reduction of the due charges.

We preferred not to provide the right of termination for the Adopter (as suggested by ECP C-SIG group and the CSCC guide, see Section 4.3 of Deliverable 4.1 "Initial Position Paper") in case of changes by the Provider as in many cases this seems not a feasible remedy for the Adopter which could be not in the position to easily change Provider.

As optional clause, which would likely be not applicable for standard services of public cloud Providers, in case of request of variation of the Services by the Adopter, the Provider shall provide the Adopter within a specified deadline an estimate of any potential increases in the consideration due (e.g. fees etc.) together with the potential impact on the delivery and use of the Services and on the applicable Service Levels.

Section 5. Obligations of the Adopter

Provider's perspective

The Provider's concern is to ensure that the Adopter follows the terms and conditions of use of the services as provided in the AUP also considering the possible consequences and damages that the Provider could suffer for the breach of the law or third parties' rights by the Adopter while using the services.

The Provider will also be concerned by any act or content that, though not illegal, might

negatively impact the performance of the services or security for other customers. The Provider will be concerned that a very detailed and specific AUP is provided, aimed at prohibiting any possible conduct of the Adopter which may cause risks for the services and establishing all duties that the Adopter must comply with. If the Adopter breaches the AUP, the Provider shall be entitled to suspend and/or terminate the access of the users to the services or even the cloud computing agreement and remove any infringing content. Finally, in some cases, the Provider will also be keen to impose an obligation on the Adopter to cooperate with the Provider.
Changes to the SLALOM proposed text after feedback
The SLALOM AUP contains specific, non-generic language, setting out the exact obligations that the Adopter must fulfil. The AUP also specifies the rights of the Provider in circumstances where the AUP has been breached. The full SLALOM position can be found in the D2.1 deliverable. In response to feedback, we added an optional clause, the responsibility of the Adopter to back-up its data. It is worth stressing that this provision could have significant consequences in case of loss of data by the Provider, as the Provider can argue that the Adopter, in line with its obligations under the agreement, should be capable to recover the lost data by itself and/or that the Adopter cannot claim damages in relation to such loss because if the Adopter would have fulfilled its obligation to back-up its data, it would have not suffered any damages.

Section 9: Term and Termination

Provider's perspective
Term In certain circumstances, the Provider might want to specify in the agreement a longer term. This would need to be linked to a mechanism allowing for a charges review after a specific period of time to ensure that there is a mechanism to increase the fees (e.g. with a fee scale). Alternatively, the Provider might also prefer a more medium term agreement, whereby the term is re-negotiated prior to expiration along with fee scales. Another option would be to insert an automatic renewal provision with (if possible) a long notice term for preventing the renewal. Similarly, a charges mechanism linked to auto-renewal would also need to be included, allowing the Provider to increase the fees at regular intervals. *Termination* The Provider will be keen to include termination rights in its favour in case of a breach by the Adopter of its payment obligation, or where there's a breach of third party rights, or if the Adopter has breached the law (e.g. by uploading content which is forbidden by law). Another option would be to insert an automatic renewal provision with (if possible) a long notice term for preventing the renewal. Similarly, a charges mechanism linked to auto-renewal would also need

to be included, allowing the Provider to increase the fees at regular intervals.
Changes to the SLALOM proposed text after feedback
1) We have added an optional clause providing the termination for convenience of either Party; 2) we have not provided any right of immediate termination of the CSA for breach of some provisions as we did not receive any feedbacks from the stakeholder requesting such type of provisions; 3) we added the right of termination of either Party where the other Party ceases to carry on business, is unable to pay its debts when they fall due, is declared bankrupt, or an order is made or a resolution passed for the winding up of that other Party or the appointment of an administrator, receiver, liquidator or manager of that other Party. Such clause is against the law in many jurisdictions. Accordingly, we provided that it is applicable to the extent permitted by the law; 4) we added the obligation to notify the termination with registered mail to avoid that such an important communication is given for instance via email among other less important communications.

Section 11: Confidentiality Obligations

Provider's perspective
The Provider is interested in protecting any confidential information relating to the technologies behind its services which have been shared for the performance of the Services, or the information concerning its business which the Adopter could have received.
Changes to the SLALOM proposed text after feedback
1) We reduced the term of the confidentiality obligations after the expiration or termination of the Cloud Service Agreement from 20 years to 6 years; 2) we added an exception in Section 11.9 to the above 6 years term of duration of the confidentiality obligations after the expiration or termination of the Agreement. Such term will not apply indeed in case of trade secrets. Trade secrets are protected under several jurisdictions as intellectual property rights without any time limit until they cease to be secret. If we provide a term of duration of confidentiality obligations on trade secrets, this could be interpreted as an authorization to disclose such trade secrets. Once disclosed, the trade secrets would lose the protection of the law.

Section 12: Warranties and Liabilities

Provider's perspective
Warranties For commercial parties, the Provider will look to receive a warranty from the Adopter that the

representatives executing the cloud computing agreement on behalf of the Adopter have the power to validly bind the company. *Liability* The Provider will require very strict limits on its liabilities. This is likely to result in extensive liability caps on the amounts the Adopter may seek to claim in damages and a number of exclusions of liability (including losses resulting from data use and data loss). The Provider may also try to propose that the payment of service credits is exhaustive of possible damages in relation to the relating services.
Changes to the SLALOM proposed text after feedback
1) In Section 12.1.1.4, we changed the "best effort" by the Provider to ensure that the Services, the Provider Content, the System and the relevant software are free from all viruses into a "reasonable effort". Accordingly, the obligations of the Provider in this respect will be less strong and engaging and more close to the standards of the sector (most of the agreements used in the market indeed does not provide any obligations of this kind); 2) we added the breach of Clause 17 (Data Protection) as one of the cases in which the limitation to liability of the Parties does not apply.

Section 15: Suspension of Services

Provider's perspective
The Provider needs to establish that in some cases (for instance in case of maintenance/update of its servers) it has the right to suspend the services.
Changes to the SLALOM proposed text after feedback
We slightly changed the Section 15.2 to have a clearer wording of the rights and obligations of the parties. Note: The SLALOM proposed text only takes into consideration suspension rights as a result of technical reasons. The suspension for non-fulfilment of obligations by the Adopter is provided under above Sections 5.3 and 5.4. We do not provide the right of suspension of payment for the Adopter. In case the Adopter (due to serious reasons related to its business operating) communicates that the suspension could cause serious damages to its activities, the Parties shall discuss possible postponement of the suspension which cannot be unreasonably refused by the Provider. In this respect, we must consider that the postponement should be not feasible in case of multi-tenancy Systems. For this reason, we have provided the words ""unless such postponement is

not feasible due for technical reasons".

Section 17: Data Protection

Provider Perspective
The Provider is generally interested in achieving high standard of security and protection of the data on one hand, but also in setting out the allocation of responsibilities with the Adopter in such a way to leave on the Adopter a certain number of responsibilities especially in those areas where the allocation of the responsibilities is not clearly defined especially by national data protection rules. Furthermore, sometimes the Providers do not explicitly refer to their role, in the Agreement, as a Processor as they consider treating their infrastructure as Processors may be inappropriate, or they limit their obligations as they consider they do not have access to data held on their cloud infrastructure and the Adopters remain in control over what data is held and for how long. This is inconsistent with most Adopters' expectations (and guidance from regulators) that the Controller-Processor relationship should be set out in writing wherever relevant (or possibly relevant) to avoid any compliance issues, even if these are viewed as unlikely. Alternatively and more recently, global providers (especially large organisations) tend to offer standardised terms and conditions containing significantly more detailed data protection clauses and obligations and some of them, recently, sought and obtained official confirmation by the Article 29 Working Party, that their data processing contractual documentation for the transfer of personal data in the context of some of their cloud services is in line with the principles set out in the EU Model Clauses approved by the EU Commission Decision 2010/87/EU. This is an attempt to harmonise their exposure to data protection compliance risks throughout the entire region where they offer their services (e.g. Europe vs. Americas).
Position proposed by SLALOM and changes proposed after feedback
The core of this clause will focus on the clear definition of the roles of the parties (setting out by default Adopter/controller and Provider/processor)[1] and the obligation of the parties, but notably of the Adopter, to comply with the applicable data protection legislations and the contractual obligations contained in the agreement (including those outlined under Attachment 5). Sample wording provided should be tailored in such a way to reflect details of the processing actually carried out by the Provider. Indeed, although in many instances the Adopter acts as Data Controller, it is less unusual than expected that an Adopter is a data processor itself in relation to the Personal Data to be processed under the Cloud Service Agreement (e.g. because the Adopter is a payroll service provider offering data processing services to its customers using third party SaaS services). In that case the terms and conditions below require substantial changes to properly reflect the data protection obligations that the Adopter agrees when it negotiates with the Data Controller.

[1] Suggestion given by the Minutes of the 5th meeting of the Cloud Select Industry Group (C-SIG) on Code of Conduct 12 February 2014.

This clause may also provide a sample of privacy notice given by the Provider to the Adopter in relation to the processing of the Adopter's personal data, if applicable(in most countries information related to legal entities, or businesses is not at all – or it is only under very limited circumstances, e.g. in the EU - within the scope of the data protection, or data privacy, laws), describing how the Provider will process – as data controller, for this limited purpose – the Adopter's personal data to execute the agreement.
Changes to the SLALOM proposed text after feedback
- We added a drafting note in the Section 17.2 to encourage the drafting parties to enclose specific wording (or reference to other documentation contained in the Agreement or in its annexes) to describe what this monitoring tools are; - we have slightly amended the Section 17.3 to clarify this is an obligation (and not a warranty) for the Provider, and to adapt the wording to make it potentially more acceptable for the Providers specifying that it is the Providers obligation to implement the security requirements of the applicable Data Protection Laws and Regulations as apply to the Provider in its capacity as a data processor, whilst the Adopter will retain all liabilities in case of breaches caused by the Adopter's failure to its own obligations; - in line with the changes introduced under Section 17.3, we added a new Section 17.5 to expressly clarify that the Adopter is responsible for any instruction it delivers to the Provider in case they result in omissions or inappropriate actions by the Processor to comply with the data protection laws; - we slightly simplifies Section 17.6; - a new Section 17.7 was added to expressly cover the recovery right for the party that paid the compensation to the data subjects on the basis of a joint liability with the other party - Section 17.8 was slightly supplemented with a warranty to be given by the Adopter about having obtained valid consent from the Data Subjects, if so required by the law, to have their Personal Data processed for the purpose of the agreement.

4.2 From the technical viewpoint

Based on the feedback during the awareness phase, including the questionnaire responses, the proposed approach of using the ISO structure was considered good overall but with a number of comments and recommendations for improvement.

The most important ISO metrics for Cloud Service Providers based on feedback are:

i. Availability component [/total downtime]
ii. Availability component[/Availability]
iii. Availability component[/Uptime]
iv. Availability component [/Allowable downtime]

v. Availability component [/Availability percentage]
vi. Service reliability component [/Recovery Time Objective (TRO)]
vii. Service reliability component [/Maximum time to service recovery (MTTSR)]
viii. Service reliability component [/Recovery point objective (RPO)]
ix. Cloud service performance component [/response time observation]
x. Service reliability component [/Time to Service recovery (TTSR)]
xi. Availability component [/Downtime]
xii. Availability component [/Uptime percentage]

This information was useful to SLALOM in helping to prioritise and focus on key components and metrics. Given the need for common understanding and consensus among the stakeholders, the prioritization list that was exploited when scheduling the work in SLALOM for the definition of the technical specification and the respective examples of metrics, was based on the feedback of both adopter and provider stakeholders

5 Cloud Provider's feedback (Phase II – III Consensus and Adoption)

This section provides a summary of the key considerations and feedback SLALOM received from providers in relation to the legal and technical tracks during the consensus and adoption phases of the project. It provides some key insights into the challenges facing service providers in managing the relationships and technical implementation of cloud computing operations in customer scenarios.

Subcontracting

The most significant issue raised was subcontracting, and this was cited by multiple reviewers. There is clause 16 on subcontracting in the legal deliverable. However, the concerns raised relate to contractual issues overlapping with service level issues, and to the overall complexity of controlling subcontracting. In our view, this issue goes beyond what can be addressed just with model terms and conditions, and with the definition of metrics. Rather, what is likely needed is separate guidance on the issues involved in subcontracting, and how to address them.

The context for this issue is that it is likely that the majority of SME providers, and of SaaS providers in general, subcontract their services to IaaS providers. While this is the most obvious subcontracting situation, there are many others, and all providers are believed to subcontract some services, such as for communications. In general, there are typically many layers of subcontracting. One source compared it to a Russian wooden nesting doll, with additional layers repeatedly being found as you look inside each one.

Some specific examples were given of the types of issues which exist:

- The adopter's main provider may not accept responsibility and liability for the performance of its subcontractors and their service levels, especially if the main provider is a smaller provider with limited financial capacity, and the subcontractor is one of the larger providers of infrastructure services.
- There is a practice described as 'clause floating' in which a clause (e.g. for limitation of liability) from one subcontractor in the stack is 'floated' up through all intervening subcontractors until it gets to the adopter where it must be accepted.

- Responsibilities may be specified in a way which is highly challenging for the adopter, but designed to protect the providers. A concept called 'stop the clock' is an example. The main provider may have agreed a 24 hour maximum response time for incident resolution or response. However, if the incident was not under the control of the main provider, but rather the responsibility of the subcontractor (or possibly a subcontractor to that subcontractor etc.), then the main provider reports the incident to the subcontractor. At this time the main provider's response time clock is stopped, and the subcontractor's response time clock starts – which may be for a different period of time than that of the main provider. A series of clocks may be started and stopped as the incident resolution request is bounced down and up the subcontractor chain. None of the providers suffers undue exposure as a result, but the adopter does.
- The situation is potentially much more complicated with respect to subcontracting when personal data is involved, because of the need to ensure compliance with data protection legislation in various countries. There may be a need for the adopter (the 'data controller' for data protection purposes) to be able to demonstrate adequate controls through the entire subcontracting stack.

The issue of subcontracting is also related to the next issue of market harmonization and commoditization.

Market harmonization and commoditization

The issue of market harmonization and commoditization is being addressed in particular by the CloudWatch 2 project which has discussed its issues with SLALOM personnel from CIF and ATOS. The issue has also been raised by one other organization.

The challenge is that cloud infrastructure services are now effectively commodity services, yet the market does not yet reflect that fact. For example, pricing information is not generally available; service levels and their metrics are generally defined differently; and contractual terms and conditions make it difficult for resellers to offer equivalent alternative infrastructure services.

SLALOM's approach of having model contractual terms and conditions, and agreed metric definitions, would greatly facilitate market harmonization, and the commoditization at least of the infrastructure layer.

It might be possible for the market overall to evolve in this direction, especially if large adopter organizations (such as governmental bodies) require common metrics and also common terms and conditions. However, it might also be necessary for there to be legislation and regulation, comparable to what exists in many utility industries, to achieve effective commoditization and interoperability.

Exploitation of SLALOM results in Research Community

The SLALOM project collaborated with various research projects in order to get their vision of Cloud technologies and also to push our findings in technical SLA aspects. Contributions have been, so far, very important for the project.

This is the list of projects that are either both contributing or being helped with SLALOM practical approach to SLAs:

- Cloud Teams Project

- Cloud Scale Project
- Artist Project
- CoherentPaaS Project
- MODAClouds Project
- Cactos Project
- Ascetic Project

Risks associated with SLALOM models

Concerns have been expressed about possible risks associated with the SLALOM models. In particular, there is concern, as with any new text or deliverable, that there may be unintended or unexpected 'loopholes' which can be exploited. The example which was given is one which had already been raised in feedback to the first draft of the legal deliverable, and we consider it already to have been addressed in the final version. However, to give the example by way of explanation, the concern was that the original provision allowing an adopter to cancel a contract if the service was varied by the provider, would give the adopter an unfair opportunity to cancel if the provider had no choice but to make the variation, e.g. if it was required by legislation or regulation, or to fix a bug. As mentioned, this particular issue was already addressed in the final legal model. However, there may be more such cases which will only be identified over time, requiring amendments to the SLALOM models to remain clearly fair and balanced.

Concerns about overall SLALOM project

There has also been feedback expressing concerns about the overall SLALOM project. We cite it here for information and understanding.

One size fits all. We have heard the criticism on several occasions that the SLALOM approach is a 'one-size-fits-all' approach. The SLALOM position is that the SLALOM models are not 'one-size-fits-all' solutions, but are baselines which are intended to be used as templates which should be modified to meet each organization's specific requirements.

Uncoordinated with other projects by the EC. We have heard a number of criticisms about the way highly similar projects such as SLALOM and SLA-Ready can be approved by the EC without coordination, and that it is left to the projects to find out about each other and do what they can to coordinate after their scopes and schedules have already been set. This is beyond SLALOM's ability to control, and we have done what we could to coordinate with other projects, including SLA-Ready. Two of the significant challenges of such coordination are that (a) the projects typically have different completion dates, meaning that they are rarely at corresponding stages in their work; and that (b) the time when the major deliverables are available from one project may not work for the second project, meaning that cross-working between projects is often not realistic.

Project overreach. We have heard the comment on a number of occasions that the SLALOM project represents 'scope creep' and overreach on the part of the EC. This is mentioned in particular concerning the fact that the title of the project specifically mentions 'service level agreement' or SLA, whereas the scope as implemented includes the full cloud service agreement, or CSA, which is above the SLA. The SLA is seen as being more technical, whereas the CSA is primarily contractual.

The factual observation about the project including the CSA is correct. However, the issue of how the term SLA is used is not limited to the SLALOM project. It is a common issue in the industry, and indeed the exact same issue exists in the ISO group working on the ISO/IEC 19086 family of standards which are all labelled as being for 'service level agreement', but the scope clearly includes the CSA, which is covered in the first part of that family, ISO/IEC 19086-1.

While it would be desirable to have better accuracy in the use of the terms SLA and CSA, SLALOM is reflecting industry practice. Indeed, we raised this issue ourselves in the ISO working group, but without success. Furthermore, the individual who initially developed the proposal for the 19086 family of standards clarified that this had been debated when the proposal was initially made, and the decision had been made to label it as it now is.

Analysis by provider type

One of the requirements of the SLALOM contract for this report) is:

> *The provided information will be provided stating information with respect to the category the cloud provider (in terms of e.g., the jurisdiction in which he provides his services, the type of the services provided, etc.) …*

We have identified the following areas where provider characteristics are significant in discussing the results of the work performed:

- **Likelihood of uptake of deliverables.** We determined that SME providers are more likely to adopt the legal model than large providers. On the other hand, the uptake of the technical deliverables (metric specifications) is more likely to be driven by large adopters, such as governmental organizations, which will drive adoption by all providers.

- **Types of services provided.** Infrastructure and platform services (IaaS and PaaS) are more likely to be provided by large providers, whereas SME providers are largely providing software as a service, using the infrastructure services supplied by large providers.

- **Relevance in subcontracting and market harmonization.** The way the market is largely split (see previous point on types of services provided) has significant implications for the issues of subcontracting and market harmonization.

We did not identify any other significant issues which depend on provider characteristics, including the country or jurisdiction of the provider, with the exception of country-specific legislation affecting cloud computing contracts such as are addressed in the report on jurisprudence and case law which is contractual deliverable D2.3. [6] It is also recognized that there may be special requirements by sector, such as for the financial and health care sectors, but that has been outside the scope of this present work, and is rather an area which might be addressed in future work.

6 Challenges

The purpose of this section is to set out some of the challenges encountered in the project, and how we adapted to meet them.

6.1 ISO involvement in subject area of project

As already discsussed, ISO started developing standards specifically related to cloud service agreements and service level agreements subsequent to the SLALOM proposal being prepared and submitted to the EC.

This presented SLALOM with two types of challenges: (a) establishing a mechanism for working with ISO; and (b) working in the way required by ISO.

We successfully addressed the first of these challenges and established a formal liaison relationship with ISO (SC38 WG3), and actively participated so as to achieve the objectives stated in 1.2.

The second challenge, of working in the way required by ISO, was primarily a challenge for SLALOM members other than CIF, since CIF was already involved with ISO and used to its way of working. Other members found it bureaucratic yet with demanding deadlines which were largely immovable. CIF mentored the other SLALOM members through this process; taking the following actions in particular, in addition to general discussions with technical track personnel:

- Reviewed the initial SLALOM technical deliverables, before the ISO liaison was established, to provide specific feedback and recommendations to NTUA concerning conflicts between the early versions of each.
- Drafted the initial version of the technical deliverable now called “Cloud SLA Metrics Based on the SLALOM Specification and Reference Model”. This takes the work which had been done on the SLALOM technical model, and applied it to specific metrics which should be immediately usable by providers and adopters alike, using a structure similar to that used for the legal model.

The general view now within SLALOM is that it was a successful effort, and will be continued beyond the end of the funded project.

6.2 Coordination with other projects

We recognized that there were significant overlaps in interest between SLALOM and a number of other EC-funded projects. As a result, we took actions to liaise with many of these projects, to mutual benefit.

6.3 Stakeholder feedback fatigue

It proved to be a challenge to obtain good feedback from commercial stakeholders, for free, to such lengthy documents as were produced by the SLALOM project. The amount of effort required by reviewers, without obvious immediate commercial benefit, was itself a major barrier. The fact that there are many demands on these commercial players for participation in other surveys and reviews, including from commercial IT research organizations, mean that there is significant feedback fatigue amongst the commercial stakeholders, and in particular amongst the providers from whom we had requested feedback.

We tried to address this issue by making direct one-on-one requests to individuals with whom CIF personnel had personal relationships, and this was successful, but the number of individuals who will help in this way is limited, and our ability to repeatedly make use of such personal relationships is also limited.

It is CIF's view that some alternative approaches may be more effective in the future, in similar situations. One possible alternative approach is to make use of small incremental deliverables. The SLALOM project had multiple versions of deliverables, but they were all of deliverables which were quite long, and inherently quite demanding on reviewers. Producing smaller, more 'digestible' deliverables more quickly could facilitate getting people to review those deliverables, and also get them involved in the project so that they would have a higher level of commitment to reviewing later possibly larger deliverables.

6.4 Dryness of the subject matter

Another challenge of the SLALOM project was the fact that the subject matter was not very exciting. It is incredibly important, but it does not have the cachet of many other subjects, such as security breaches. In the vernacular, it is not 'sexy'. The subject matter may also be commercially sensitive, especially for larger providers, and where they are willing in principle to contribute, their internal control processes for managing comments about such topics to external parties can be so onerous as to effectively prevent their helping.

There is little we can do which will make the subject matter more exciting. However, we can be vigilant to ensure that our deliverables communicate as clearly as possible.

7 Ongoing Actions (Phase II – III Consensus and Adoption)

There was limited opportunity to gain feedback or adoption assessment on the technical track deliverables from the Provider community in the period to the end of June 2016. This is because the nature of the technical deliverable, however, meant that the initial deliverables were suited for the research community rather than the provider community.

The deliverable which applied that work in a way which was directly usable by the provider community only became available on 16 June 2016, during the last two weeks of the project, meaning that there was no realistic opportunity for obtaining feedback on its contents. We developed a questionnaire [7] which continues to be available for assessment of the deliverable by Cloud Providers and Adopters. This is an activity which will be continued into the sustainability phase of the project.

SLALOM will continue to promote the availability of the legal and technical models and the National Technical University of Athens, responsible for the technical stream, have confirmed they will remain involved in ISO. We are therefore taking appropriate steps to ensure that the liaison relationship between ISO (SC38 WG3) and SLALOM continues.

8 Conclusions

In the course of collecting the feedback and views of the provider segment, it became apparent many suppliers believe that the issues of contracting require continued education efforts so that both providers and users share common understanding. We identified more openness to potentially using the legal terms from SMEs and micro-businesses in the provider sector. We know of at least one such organization which has already adopted the legal terms.

The most immediate results in terms of uptake of the technical model is the collaborations with other research projects who have confirmed their interest in making use of the models in the context of their ongoing work. SLALOM has also provided guidance documentation "Do's and Don'ts of Cloud SLAs for Research"

Useful and quality deliverables

Overall we have had positive feedback from reviewers and the marketplace to the SLALOM deliverables. We consider that the SLALOM project has produced deliverables which are useful for the cloud marketplace, and are of appropriate quality. They are immediately useable by all stakeholders, including providers, adopters, the legal profession, consultants, policy makers, and the research community. They also provide a good basis for incremental improvement.

Opportunity for adoption

Based on the feedback we have had, we consider that it is likely there will be reasonable uptake and use of the SLALOM deliverables. There has been little time for the market to consider and start to use the SLALOM deliverables, but the signs are positive. In particular:

- **Legal model adoption.** It is considered that SME providers will be the earliest users of the legal model (i.e. the cloud service agreement model terms and conditions) because they have the most flexibility with respect to their legal contracting, and it may be seen as a competitive advantage for them to have contractual terms and conditions which are independently created with the intent of being fair and balanced. There is already at least one SME provider which has used the SLALOM legal model. (See http://www.taxcalc.com/cloudServiceAgreement.). On the other hand, we have feedback that large organizations – both providers and adopters – will likely find it more difficult to adopt the legal model largely as it is because they have years, or decades, of contracting experience with resulting contractual terms and conditions which have evolved in response to that experience, and these will not quickly be replaced. Nonetheless, there could be a willingness to benchmark their own contractual terms and conditions to those of the SLALOM legal model.

- **Technical model adoption.** It is considered that large adopters will be the earliest users of the technical model, and in particular of metric definitions proposed by SLALOM based on that model. One large government procurement organization has already indicated that it is interested, in principle, in using the SLALOM metric definitions in its tendering processes, and we have had feedback that the same may apply to at least one other governmental procurement organization, and potentially more. While not all providers will respond to such requirements, enough will (and do), and such behaviour can move the market by making the use of these metrics generally available. On the other hand, it is unlikely that small adopters will have the commercial clout to require the use of the SLALOM metrics from providers which do not currently provide them. Likewise small SME providers, which are typically dependent on larger providers for underlying services, will not have the commercial clout to require their supplier providers to use the SLALOM metrics.

- **Use of SLALOM models as baselines.** Regardless of whether there is full adoption or not of the SLALOM legal and technical models, we have had feedback from several organizations including providers that they are considering using both SLALOM models for benchmarking against their current practices. This is likely to influence those practices, even if the SLALOM models are not

adopted as such.

- **Publicity.** We have had good initial reactions and publicity concerning the release of the SLALOM legal and technical models, and there are further on-going developments. Indications are that there could be further commercial uptake as more people and organizations learn about the SLALOM legal and technical deliverables.

- **Research community uptake.** There has also been feedback that various research projects are considering making use of the SLALOM legal and technical deliverables. While this does not imply direct commercial uptake, it reflects the fact that all stakeholders see value in the SLALOM deliverables.

REFERENCES

[1] SLALOM deliverable D1.1, “Stakeholder analysis and initial communication plan”
[2] SLALOM Online questionnaire, “SLALOM: Ready to Use Cloud SLA”, available at http://bit.ly/28JFmPh [last accessed: June 2016]
[3] SLALOM deliverable D1.2, “Outreach Year 1 report and plan for the adoption phase”
[4] SLALOM deliverable D4.1_5.1, “Initial Position Paper Reflecting Cloud Service Provider and Cloud Adopter Requirements”, available at http://bit.ly/SLALOMD4-1D5-1 [last accessed: June 2016]
[5] SLALOM deliverable D2.1, “First draft of the terms for discussion in the consensus groups”, available at http://bit.ly/291ZPB1 [last accessed: June 2016]
[6] SLALOM deliverable D2.3, “Report on Jurisprudence and case law”, available at http://bit.ly/28WlIjt [last accessed: June 2016]
[7] SLALOM Online questionnaire, “SLALOM: Project Deliverables Assessment”, available at http://goo.gl/forms/Wl3wCRb3855dm2p42 [last accessed: June 2016]

License

Annex A: Legal overview document

Overview

SLALOM Cloud Service Agreement Model Terms & Conditions

The SLALOM project[2] (www.slalom-project.eu) has two main deliverables, namely a cloud legal model, and a cloud technical model. This document provides a short overview of the structure of the SLALOM cloud legal model. The SLALOM cloud legal model is a set of model terms and conditions for cloud service agreements. The full legal model is available at www.slalom-project.eu/downloads.

The SLALOM cloud service agreement (CSA) model terms and conditions have been developed primarily by the SLALOM consortium member and legal firm Bird & Bird with assistance by the University of Piraeus Research Center (UPRC), and incorporating extensive feedback from cloud stakeholders. These model terms and conditions are intended to be:

- **A practical baseline.** The SLALOM legal model can be used by anyone to assess or develop their own CSA terms and conditions. It has been produced under a Creative Commons license which allows anyone to use it and modify it in any way they wish.

- **Fair and balanced.** The SLALOM legal model should give reasonable assurance that there is no bias towards either the cloud service provider or the cloud service adopter (i.e. customer).

The SLALOM legal model covers the following areas:

Section Title in SLALOM Legal Model	Comment
Introduction	
Cloud Service Agreement	
Section 1: Definitions - Interpretations	
Section 2: Provision of services	
Section 3: Service levels	There is limited coverage in the SLALOM legal model, with coverage rather expected in the SLALOM technical model.
Section 4: Variation of the services	
Section 5: Obligations of the Adopter	
Section 6: Charges	

[2] The SLALOM project is co-funded by the European Commission through the H2020 Programme under Grant Agreement 644720.

Section 7: Service credits	
Section 8: Intellectual property	
Section 9: Term and termination	
Section 10: Consequences of termination and expiration	
Section 11: Confidentiality obligations	
Section 12: Warranties and liability	
Section 13: Indemnification	
Section 14: Insurance obligations	
Section 15: Operational suspension of services	
Section 16: Subcontracting	
Section 17: Data protection	
Section 18: Force majeure	
Section 19: Notices – Parties' team leaders	
Section 20: Governing law	
Section 21: Disputes - jurisdiction	
Section 22: Final provisions	
Section 23: Attachments	
Attachment 1 to the Agreement: Services Description [Ref'd from S2]	No detailed text is given by the SLALOM legal model, since this depends on the specific service being offered.
Attachment 2 to the Agreement: Service Level Agreement – Service Credits [Ref'd from S3]	There is limited coverage in the SLALOM legal model, with coverage rather expected in the SLALOM technical model.
Attachment 3 to the Agreement: Acceptable Use Policy (AUP) [Ref'd from S5]	A detailed proposal is given by SLALOM.
Attachment 4 to the Agreement: Charges [Ref'd from S6]	No detailed text is given by SLALOM, since this depends on the specific commercial terms which apply.
Attachment 5 to the Agreement: Data Protection Attachment [Ref'd from S17]	A detailed proposal is given by SLALOM.
Attachment 6 to the Agreement: Security Policy [Ref'd from S11]	No detailed example is given by SLALOM.

The areas addressed by the SLALOM legal model are organized as follows:

General description of the section	
Standard clauses used in the market	
Provider's perspective	Adopter's perspective
Position proposed by SLALOM	
Changes to the SLALOM proposed text after feedback	
SLALOM proposed text	

There may be future updates of the SLALOM legal model, based on further feedback received, and possibly also to address sector-specific or jurisdiction-specific issues. Further information when available will be found at www.slalom-project.eu.

Annex B: Technical overview document

Overview

Cloud SLA Metrics

Based on the SLALOM Specification and Reference Model

The SLALOM project[3] (www.slalom-project.eu) has two main deliverables, namely a cloud legal model, and a cloud technical model. This document provides a short overview of the structure of the document entitled "Cloud SLA Metrics Based on the SLALOM Specification and Reference Model", which includes examples that can be used "as is" by cloud providers and cloud adopters. The full document is available at www.slalom-project.eu/downloads. A more detailed document, SLALOM deliverable D3.6 "SLA specification and reference model - c", will be released by the end of June 2016 through the SLALOM website and will include updates of the SLALOM technical model, including in particular for the suggested metrics, based on feedback received.

The SLALOM technical model has been developed by the SLALOM consortium member National Technical University of Athens (NTUA), incorporating revisions to reflect work which SLALOM has done with the ISO committee responsible for cloud standards. The SLALOM technical model is intended to be:

- **Unambiguous.** The SLALOM technical model allows for the unambiguous specification of cloud metrics, to avoid the common problem with many current metrics that they are unclear and can be contested (i.e. the results can be easily repudiated).

- **Fair and balanced.** The SLALOM technical model and its proposed metrics should give reasonable assurance that there is no bias towards either the cloud service provider or the cloud service adopter (i.e. customer). This is not only because of the way the metrics are specified, but also because of the metrics which are proposed.

- **Readily usable.** Although the proposed SLALOM metrics are technical in nature, they are described in ways which may be understood by individuals with limited technical expertise, and these descriptions may then be expressed in unambiguous ways (e.g. in XML or JSON) by individuals with those more specific expertise sets.

The suggested metrics based on the SLALOM technical model currently cover the following:

Section Title

[3] The SLALOM project is co-funded by the European Commission through the H2020 Programme under Grant Agreement 644720.

Metrics: General
Availability (Accessibility) Metric
Availability (Functionality) Metric
Response Time (Transactional) Metric
Response Time (Incident) Metric
Incident Resolution Time Metric
Performance of Virtual Cores Metric

The different aspects describing the metrics based on the SLALOM technical model are organized as follows:

General description of the metric	
Standard metric provisions used in the market	
Provider's perspective	Adopter's perspective
Position proposed by SLALOM	
SLALOM proposed metric parameters	
Indicative SLO definition for the above metric based on the SLALOM reference model	

There may be future updates of the SLALOM technical model, and in particular for suggested metrics, based on further feedback received. Further information when available will be found at www.slalom-project.eu.

Annex C: Initial determination of requirements

The information in this annex is from the initial determination of requirements conducted by CIF.

1. General observations

1.1 Industry views of model terms and specifications

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.

1.2 Implications of counterparty size: SME to enterprise

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 providers providing input for SLALOM were SMEs.

2. Industry views about the importance of the work being done

2.1 Importance of the work - conclusions and proposals for final deliverable

- 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 providers 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 providers or End-Users. However, they are seen as inhibitors to cost-effective uptake, in particular by SMEs (both provider 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).

2.2 Supporting questionnaire analysis

Column 17 – Overall factors inhibiting cloud uptake

From perspective of providers:

- Only one mention relevant to SLALOM scope: 'legal issues'
- Minimal mention of 'traditional' cloud issues
    - Data location
    - Security
    - Resilience
    - Robustness
    - Availability
- Most are marketing and education related
- Some relate to fast-changing technology and ability to keep up
- Some reflect financial and management concerns of potential customers
    - Capex vs opex
    - Need to utilize existing infrastructure investment
    - Reluctance of IT management to lose control
- Some reflect particular concerns of small SMEs
    - Funding
    - One cites exposure to government policy changes (for provider serving government)
- Some reflect supply chain issues
    - Licensing

From perspective of adopters:

- Limited mentions relevant to SLALOM scope
    - 'difficulty of comparing providers'
    - Availability (2 mentions)
- Main concern is regulatory compliance
    - Personal data protection
    - Data location
- Security is second-highest concern
- Variety of other single mentions
    - Vendor lock-in
    - Feasibility
    - Performance
    - Storage
    - Redundancy
    - Threat deterrents
    - Accessibility
    - Direct audit possibility

From perspective of others:

- Only 2 mentions
    - Cost
    - Need for technical cloud brokerage platforms/portals

Column 18 – Legal terms and SLAs inhibiting cloud uptake

From perspective of providers:

- There were few comments about general contractual issues unrelated to SLAs, except as detailed below (e.g. data location)
- Overwhelming view is that SLAs do not inhibit cloud uptake
    - 10 responses, 2 non-responses
- A limited number (4) say they want standardization, but do not say if they inhibit cloud uptake
    - 3 SMEs
    - 1 just above: 250 – 999 employees
- One says SLAs are important, but does not indicate if they inhibit cloud uptake
- Several mention issues related to SLAs
- Most important for
    - Enterprise sector
    - Public sector
    - Local government
    - Charities
- Other issues mentioned are
    - Data location
    - Availability (difficulty of achieving high levels)
    - 'Off-shore or third party administrative roles in service assurance' [apparently = issue of subcontracting]
    - Customer confusion
- View expressed that SLAs are not important for run-rate (= standardized, high-volume, low cost) services
- View expressed that there are no meaningful SLAs by public cloud providers

From 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
    - Variances of the same terms between vendors
- Only two strong comments
    - "Very significant. Too much time reviewing contracts for potential privacy liability risk assessment with no ability to negotiate limitation clauses'
    - "Lack of control about personally identifiable information outside of our doors"

From perspective of others:

- Only 2 limited responses
    - "basically"
    - "Significant"
- One extensive comment: " .. should be structured by strong, standard, simple and agile SLAs and contracts…"

3. Alignment to ISO

3.1 ISO structure feedback - conclusions and proposals for final deliverable

- 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, it is a moving target. 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.
- Based on the questionnaire responses, the proposed approach of using the ISO structure is considered good overall, but with a number of comments and recommendations for improvement.
    - Even some of those commenting that it is 'good' consider that it is too detailed to be practical.
- Re structure, it is suggested that the data management component has too many sub-components. Consider further breakdowns.
- Re 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.

3.2 Supporting questionnaire analysis

Column 127 – Quantitative Assessment of ISO Structure (Full Questionnaire Only)

Org Type	No of Responses	Average Rating
Provider	5	4.16 – Good
Adopter	4	4.2 – Good
Other	3	4 - Good

Column 128 – Qualitative Assessment of ISO Structure (Full Questionnaire Only)

From perspective of providers:

- Balance of views is positive.
- Qualifying comment from provider giving assessment of 'Good' is 'Probably excessively complex in operation. Few S&Ms [=SMEs] will pay the extra for the additional work and structures involved.'
- One negative comment from provider giving assessment of 'Poor' is 'Tries to shoe-horn the old world into the new.'
- One comment refers to missing components (should be in column 129): "There seems to be no warranty section. Cloud user must use the system in compliance with the law and the agreement. There seems to be no payment section, payment terms, indexation, and consequence of non-payment. Any commercial incentive of penalty for lack of service."

From perspective of adopters:

- Only question raised in comments is 'Process view should be included somehow?'

From perspective of others:

- Although balanced view is 'good', qualifying comment from provider giving assessment of 'Good' is 'It is too detailed in some points and probably overambitious, eg. in terms of MTTR, 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' is '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...'

Columns 129-131 – Missing Components

From perspective of providers:

- Additional major components
    - 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'
- Specific provisions under existing components
    - '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 defense 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?'
- Further comments about proposed additional scope:
    - 'Expand performance by geographic location and tie with user experience due to high variability (e.g., Russia & China may have 10x worse performance than users in USA).'
    - 'Alignment with industry specific authorities such as Law Society or SRA requirements may be a consideration.'
- 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 providers 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.'

From perspective of adopters:

- Additional major components
    - Managing subcontracting and ensuring standardisation of obligation in this context. Please see Cloud Security Alliance Control Matrix that addresses this topic.
- Specific provisions under existing components
    - a set of standard "minimum" security controls
    - Role and responsibility list (role list is missing)

From perspective of others:

- Additional major components
    - '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'
    - 'Penalties'
    - 'Cost reporting! daily, weekly, monthly, wtd, mtd, ytd, forecasting...etc...'

Columns 132-134 – Suggestions for Improvement

From perspective of providers:

- Philosophy of work
    - 'Simplify'
    - 'Simplify, simplify, simplify. The biggest adopters are not large organisations; these standards are aimed at enterprise customers'
    - 'Think about who the consumer is - a private consumer won't give two hoots other than "is my service available" and would resent paying for a service in order to have an SLA they won't understand, and won't care about.'
    - 'Speak to real cloud users and real cloud providers, rather than the old guard, and learn from them'
- Specific content recommended to include
    - 'Implement a quantifiable level of security'
    - 'How to measure availability of service as a whole'

    - '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.'
    - 'Process of payment'
- Reiteration of existing content
    - Detailed security controls for cloud providers should definitely be called out, since denial of service, or web application vulnerabilities have the highest impact.
    - The roles and responsibilities of each party should be clear.
    - The importance of common language and expectation setting between provider, reseller and end user.

From perspective of adopters:

- Specific content recommended to include
    - Subcontracting
    - Process view should be included somehow?

From perspective of others:

- Structure
    - Data management component has too many sub-components. Consider further breakdowns.
- Specific content recommended to include
    - Costs monitoring/reporting
    - Cloud based orchestration Tools, services, monitoring, reporting... (Cloud Management Portal services)

4. Master service agreements (MSAs)

4.1 MSA model approach - conclusions and proposals for final deliverable

- 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.
- For presentation, the 'comparisons of good and bad terms are informative, but we also need a straight-forward list of recommended terms.'
- Potentially, there could be 'broader examples, organized for each kind of sector/industry'
- Re additional components, the following are suggested based on feedback to the proposed ISO structure (see 3.1 ISO structure feedback - conclusions and proposals for final deliverable.)
    - 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...'
- Our provider interviewing process identified that the Council of Bars and Law Societies of Europe has issued the "CCBE Guidelines on the Use of Cloud Computing Services by Lawyers", including a section on contractual issues. (http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf). There are a number of other references for legal practitioners relating to their own use of cloud computing at http://www.lawcloud.co.uk/security/law-society-cloud-guidance.
- 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 3.1(ISO structure feedback - conclusions and proposals for final deliverable).
- The EC DG Expert Group on Model Cloud Terms has considered many of the clauses considered important for cloud computing agreements. See the References at the end of this document.
- The proposed MSA detailed organization for contents to be produced for the final SLALOM deliverable is given in Annex 1.

4.2 Supporting questionnaire analysis

Column 19 – Quantitative Assessment of MSA Approach (Full Questionnaire Only)

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

Column 20 – Qualitative Assessment of MSA Approach (Full Questionnaire Only)

From perspective of providers:

- 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 providers are like Facebook!'
- Concern/disagreement about specific terms proposed

From 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 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.'

Columns 21 (all Questionnaires) & 22 (Full only) – MSA Pain Points

From perspective of providers:

- Security and personal data protection issues
    - 'Data protection and location of data'
    - '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).'
    - '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). '
    - '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.'
    - 'Buyers assuming we can access and see their data. For IaaS, this simply isn't the case.'
    - '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'
    - 'Consequence of default of SLA KPI.'
    - 'Termination for Convenience.'
    - 'Jurisdiction issues, caused by intentional confusion sown by [name omitted] etc. who try and sell as if they are not US corporations simply because they have a European office.'
    - 'These can be long and difficult to understand or they can be short with not enough detail'
- Other
    - 'Complexity'
    - 'What's a good standard'
    - 'Exit and portability of data'
    - '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'
    - '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 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.'
    - '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.'
    - 'Where data is stored, who has access to the data? '
    - 'For Public Cloud, Compliance rules: Data Location & Direct audit possibility'
    - '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?"'
    - 'Limitation of liability... specifically the provider wanting to partner with skin in the game about ownership and dollars. Most want to tie this to their revenue as opposed to the potential losses.'
    - '99.99% uptime may be the guarantee, but if it's down, the only option is a credit (which oftentimes does not equal the employee/business impact)'
- Other
    - 'Customer's rights'
    - 'Service security, availability and quality'
    - 'Use of 3rd parties by main contractor who are they and where are they?'
    - 'Private cloud versus public cloud.'

From perspective of others:

- Security and personal data protection issues
  - 'the opt out option and data privacy'
- 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
    - either 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 providers.'
- Other
  - 'user interaction respond time'

Columns 32-126: Prioritization of components

The following may be noted:

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

5. Service level agreements (SLAs)

5.1 Conclusions and proposals for final deliverable

- 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 providers 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 providers 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.

5.2 Supporting questionnaire analysis for metrics model approach

Column 23 – Quantitative Assessment of Metrics Model Approach (Full Questionnaire Only)

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

Column 24 – Qualitative Assessment of Metrics Model Approach (Full Questionnaire Only)

From perspective of providers:

- 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 perspective of adopters:

- Support for automation

From 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.'

Columns 25 (all Questionnaires) & 26 (Full only) – SLA Pain Points

From perspective of providers:

- Customer expectations
  - 'Customers expecting the ability to bespoke - huge cost attached to this'
  - '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.'
  - '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'
- Standardization issues
  - 'The fact that no one set of SLAs will meet the needs of different customers/cloud options'
  - 'Defining "availability"'
  - 'To the most part lacking of common language and definitions.'
  - 'how to measure SL's according to standard'
- Technical challenges
  - 'That there is no contrast and compare mechanism available to gauge actual performance.'
  - '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.'
  - 'The reliability of third party service - such as connectivity.'
  - 'Admin and tools to monitor internally that we are meeting our SLA's. IN saying that few people ask us to provide these measures.'
- Contractual issues
  - 'That the quality part should be emphasised rather than the forfeit.'
  - 'Consequence of default of SLA KPI.'
  - 'Termination for Convenience.'
- Other
  - 'Resource to meet them.'
  - 'They can protect the provider rather than the customer'
  - 'End to end penalties measurements and reporting.'

From perspective of adopters:

- Meeting adopter requirements
  - 'I do not think the provider is able to provide all core metrics I have identified'
  - 'managing subcontracting : the controls the provider has on its subcontractors and the leveling of controlling/reporting between all involved parties since the SLA are already in place when a new customer signs the agreement with the main provider'
  - 'Mapping user needs and SLA'
  - 'Ensuring the correct SLA's are in place to ensure they match the service we need, the contractor delivering the SLA we signed up for. The business area understanding we no

longer have the same control that we once had when we provided the service internally.'

- Other
    - 'making them simple for all parties to agree to and review as a partnership.'
    - 'Lack of accountability'
    - 'Poor resolution of incidents and communication'
    - 'Since we're mainly based in Europe, for Public Cloud, the European offer is not so developed and competitive as in the US. The possibility of using US facilities is constrained by the need of usage of sufficient bandwidth that often offset the economic benefit of the offer itself. '

From perspective of others:

- Technical challenges
    - 'The difficulty to track the veracity of the SLA reports provided by the Cloud services provider.'
    - 'The lack of 'end to end'' SLAs'
- Contractual issues
    - 'Complexity of contractual definitions, and all of the exceptions which undermine their usefulness.'
- Other
    - 'Lack of comparability between different providers.'
    - 'Lack of auditing'

Columns 27 & 28 (Full Only) – Suggestions for Improvement in Metric Model Approach

From perspective of providers:

- 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 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

Column 29 – Quantitative Assessment of Using Data Exchange Format (Full Questionnaire Only)

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

Column 30 – Qualitative Assessment of Using Data Exchange Format (Full Questionnaire Only)

From perspective of providers:

- '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'

5.3 Supporting questionnaire analysis for prioritization of metrics

For the short questionnaire, a leading question was added which stated "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?" Because this was answered with comments, the responses were not easily combinable. Nonetheless, it was clear that the most cited metrics fell into the following groupings:

- Availability (e.g. uptime and downtime, planned and unplanned) – consistently the highest priority metric
- Response time for service support issues [e.g. time to provision; to respond/resolve to service interruptions or to support requests]
- End-to-end responsiveness/throughput

We noted that the CD1 draft of ISO/IEC 19084-1 has no measurable 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.

See also the separate spreadsheet 'Metric Priorities.xlsx'. This shows the ranked priorities of the different ISO metrics for providers, adopters, others, and overall, with the top priorities for each highlighted. The following may be noted:

- Availability metrics were high priority for both providers and adopters, with total downtime the highest priority availability metric.
- The top priority for adopters was cloud service throughput. However, this was no 24 for providers. Comments from providers elsewhere indicated their difficulty with this metric because of the fact that they rely on third parties for communications, and have little control over them. Geographic location is also an issue, e.g. Germany or China.
- Service reliability metrics were also high priority for both providers and adopters.
- Cloud service performance metrics were comparatively low priority for both providers and adopters.
- 'Others' ranked a number of metrics highly which were not ranked highly by providers or adopters.

6. Service level research

6.1 Conclusions and proposals for final deliverable

- 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 providers and adopters. Automated SLA renegotiation was lowest rated for providers 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 providers, adopters, and others.

6.2 Supporting questionnaire analysis

Columns 135-139 – Quantitative Assessment of Research Topics

	Provider	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				

Columns 140-141 – Qualitative Assessment of Metrics Model Approach (Full Questionnaire Only)

From perspective of providers:

- 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 perspective of adopters:

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

From 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)

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