www.sla-ready.eu

Title: High-level report on cloud SLA recommendations

Author(s): Silvana Muscella, Nicholas Ferguson & Stephanie Parker, Trust-IT

Contributor(s): Jesus Luna, Damir Savanovic & Marina Bregou, CSA

Date: 31 December, 2016

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

Executive Overview

Knowledge is key to helping Small and Medium Enterprises (SME) adopt cloud services and to trust cloud SLAs which can often be confusing, lack clarity and are difficult to follow due to legalese terms used. SLAs need to become trusted sources of information. The adoption of standard metrics and terms is the best way to achieve this.

A core activity within SLA-Ready is to increase trust and transparency in cloud SLAs by supporting both the definition of cloud SLA standards and also in supporting Cloud Service Providers (CSP) in assessing their own cloud SLAs in order to help create a culture of trust and transparency for CSPs.

The SLA-Ready Common Reference Model is an important step to achieving this. This document provides a set of recommendations regarding the standardisation of cloud SLAs.

Through online resources published in the SLA-Ready Hub and SLA Marketplace, and workshops targeting SMEs, SLA-Ready has contributed to driving a common understanding of SLAs for cloud services and increasing knowledge in this area for SMEs.

The recommendations in this document reflect SLA-Ready's activities in engaging a diverse range of experts including SMEs, SME associations, cloud procurers and standards experts. Recommendations are also provided for future research to address challenges relating to Data Protection, Security and Privacy.

Finally, this document provides an overview of actions in supporting the uptake and adoption of standards in cloud SLAs through contributions to ISO 19086 and other standardisation initiatives such as the EU catalogue of standards.

Table of Content

Table of Figures

Document information

Deliverable number	D3.4
Deliverable title	High-level report on cloud SLA recommendations
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	31 December 2016
Actual delivery date	31 December 2016
Author(s)	Silvana Muscella, Nicholas Ferguson & Stephanie Parker, Trust-IT
Contributor(s)	Jesus Luna, Damir Savanovic & Marina Bregou, CSA
Reviewer(s)	Arthur van der Wees, Arthur's Legal
Task(s) contributing to the deliverable	Task 3.1 Standardisation, Best Practices and Recommendations, Task 3.2 International cooperation, consensus building and coordination with the SLA-Ready Advisory Board
Target audience(s)	Cloud Service Providers, Policy Makers, Standardisation Bodies
Total number of pages	25 (report core), 63 (with annexes)

Disclaimer

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

List of Acronyms

AB	Advisory Board
CC	Cloud Customer
CD	Committee Draft (ISO/IEC)
CSA	Cloud Security Alliance
CSA STAR	Cloud Security Alliance's Security Trust and Assurance Registry
CSP	Cloud Service Provider
DIS	Draft International Standard (ISO/IEC)
EC	European Commission
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
EU27	27 EU Member States
FDIS	Final Draft International Standard (ISO/IEC)
FP7	The Seventh Framework Programme (2007-2013)
H2020	Horizon 2020
ICT	Information and communications technology
IS	International Standard (ISO/IEC)
ISO	International Organization for Standardisation
ISP	Internet service provider
JTC	Joint Technical Committee
MS	Member States
R&D	Research and Development
RTD	Research and Technological Development
SDO	Standards Development Organization
SLA	Service Level Agreements
SLO	Service Level Objectives
SME	Small and Medium-sized Enterprise
WD	Working Draft (ISO/IEC)
WG	Working Group
WP	Work Package

1 Introduction (Trust-IT)

Trusted and transparent cloud SLAs are an essential piece of the objectives of the Digital Single Market (DSM). Cloud computing is a key enabler for emerging technologies such as the Internet of Things and Data Science and is continuously driving the vast spectrum of both current and emerging applications, products, and services.

Mobile phones and tablets are now used more than desktops to access Internet as business and habits change. At SLA-Ready SME workshops we have seen how SMEs are adapting to this new reality. Cloud services are providing amazing opportunities for and giving the opportunity for businesses to be agile allowing them to adapt business plans to changing circumstances. We've seen real examples of SMEs[1] who are now able to provide services that were unthinkable before the advent of cloud computing.

Contracts and Service Level Agreements (SLAs) are key components in defining cloud services, but are the least understood cloud attributes. This is due to complex language and terms of service (technical and legal), lack of widely accepted standard frameworks, vocabularies, uncertainties as to what is regulated, who is responsible and which laws actually apply.

This document provides a set of recommendations for trusted and transparent Cloud SLAs for the DSM, with recommendations based on a multi-stakeholder dialogue to ensure all key issues are addressed. This includes expert views from SME associations, SMEs including customers and re-sellers, procurers of cloud services, and standardisation experts.

We then provide recommendations towards the DSM initiative on the Free Flow of Data. These recommendations challenges for data protection, security and privacy in relation to research challenges that can be addressed in the Horizon 2020 ICT Work Programme 2018 – 2020.

It is important to bear in mind that SLA-Ready was conceived before the Digital Single Market strategy was defined. Nevertheless, the project has anticipated many challenges related the free flow of data and the importance of standardisation in cloud SLAs that the DSM aims to address.

The document then looks at validation of the CRM and feedback regarding CSPs responses to the CSP self-assessment questionnaire and the SLA Repository.

Finally, actual contribution to cloud SLA standardisation directly is a key objective of SLA-Ready. Therefore, the final and key part of the document provides an update of SLA-Ready contributions to relevant cloud SLA standardisation and best practices initiatives, which were performed during Year 2 of the project. This serves to update previous deliverables on this topic (D3.1 & 3.2). By leveraging the analysis of the standardisation

[1] See case studies in D4.4 e.g. Parking Plus and Hypermedia.

landscape and the contributions made, we also identify existing gaps and future actions which go beyond the lifetime of the project.

2 *Recommendations for trusted and transparent Cloud SLAs – Expert views*

SLA-Ready has collected inputs from a diverse range of experts in order to provide an independent set of recommendations with regard to ensuring trusted and transparent cloud SLAs.

From an SME perspective, a current theme in SLA-Ready stakeholder engagement is the benefits of standardised and transparent SLAs for both sides of the equation:

- **Demand side**: SMEs should get together to negotiate SLAs that are more tailored to their needs as small businesses with the support of ICT clusters and national trade associations.
- **Supply side**: Having a transparent SLA is a unique selling point for a CSP, where SMEs represent a large segment of the market.

Other interactions have helped identify additional recommendations from stakeholders as diverse as SME cloud service providers, cloud service re-sellers, ICT clusters representing SME customers, standards experts, customers of large research institutes and service providers for educational institutions. The following recommendations clearly report the source and the target stakeholders.

Expert stakeholder category: Cloud SaaS provider and industry expert

Recommendation targets: Cloud service providers and customers

Recommendation focus: Fair contracts and liability

"When I think about the potential consequences of a SLA that has failed to deliver on its commitments and that results in a business failure then it gets no more serious. The CSP wants to know that in the severe test of its SLA in a court of law that it will stand up to the rigour of examination. The customer wants to the extent possible an SLA that is a fair balance of their interests and reliance upon the CSP to serve their business with a clear and unambiguous statement of the responsibilities of the CSP. The way to provide the support for a CSP and customer to be in a dialogue about an SLA is to have a trusted source of information available to both in the public domain."

Frank Bennett, iCloud Ltd & Cloud Industry Forum

Expert stakeholder category: ICT Clusters

Recommendation targets: SME customers and re-sellers

Recommendation focus: Advice on legal and security aspects

Workshops co-hosted with ICT Clusters have brought home the real need for informative

events where SMEs have access to freemium[2] advice on security and legal issues, especially the forthcoming GDPR, which SMEs find particularly complex.

"It's very important to have these types of events to disseminate the new directives and to exchange stories on how cloud is being used to deliver services to clients. I think 'legalese workshops' should be held regularly to help SMEs overcome the language barrier when signing cloud contracts"

Alex Rotaru, Altom Consulting & Board of Directors, ClujIT

Expert stakeholder category: SME cloud service provider

Recommendation targets: Cloud service providers, resellers

Recommendation focus: Transparency and comparability of Cloud SLAs

"*Cloud service providers should start by asking fundamental questions of what constitutes a trusted and transparent Cloud SLA, and then select the most appropriate CRM elements. This is the basis for constructing a proper agreement for the application or service.*

If your application or service depends on other cloud services, e.g. running on a cloud infrastructure provided by a third party, you need to check the SLAs they offer and be sure that the parameters of your SLA are not higher than the parameters of your cloud provider.

The Common Reference Model is also a reference point for providers using open source software wishing to implement best practices for transparent Cloud SLAs and facilitate comparability of services. In both cases, integration of appropriate CRM elements has real benefits for customers and cloud service and application providers. Transparency will support competition and general acceptance of cloud technology among EU businesses."

Katerina Materkia, 7Bulls

Expert stakeholder category: ICT Cluster

Recommendation targets: Policy makers

Recommendation focus: standardisation and regulation

"*Probably the best way to achieve transparency, and therefore trust, is to adopt a set of standards as mandatory reference for such SLAs. Although in the world of business it does not have a very good reputation, regulation seems the only reasonable (and achievable) approach. When security of potentially sensitive data or privacy of data are at stake I*

[2] A freemium service is provided free of charge but proprietary features, or in this case personalized consultancy on security and legal issues, are charged.

believe there is no other sensible response".

Andrei Kelemen, Executive Director, Cluj IT Cluster

Expert stakeholder category: Cloud SLA standardisation

Recommendation targets: Policy makers, standards bodies

Recommendation focus: standardisation

"An important property of a trustworthy SLA is the extent to which it can be monitored by the customer. A second important aspect is fairness, i.e. it must be balanced regarding obligations of the two partners. Today's SLAs as offered by the big providers as slanted towards the benefit of the provider.

From these two aspects a number of relevant properties for the implementation can be derived, e.g. Service Description Terms (SDTs) that are useful for the customer to express their requirements and useful for the provider, to express its capabilities.

These SDTs exist (having been developed in a number of European projects for example) and need to undergo a standardisation process in order to become generally usable. Other concerns that need attention include guarantees, penalties and rewards. Their embodiment between provider and customer is crucial for trusted and transparent cloud SLA. Monitoring needs to be addressed in an implementation, probably by strengthening the concept of a trusted third party (TTP).

I would consider the current standardisation activities as in some sense helpful (providing insights into the problem). But not at all close to a generally usable solution for cloud SLAs. Simply because none of the developments would allow a project to pick it and implement it in a way that interoperability on the level of, e.g. language, protocol or service description terms with other implementations would be more or less automatically achieved.

A lot of more effort and time is needed, e.g. to create standards with relevance for implementing interoperable services. From my experience doing this out of European projects (or other projects) is difficult due to the different time scales, but not impossible. Regarding ISO I have some expectation that the current ad hoc activity for discussing and defining the future targets of SC38 might be suitable to do more in direction of working on standards that support implementing interoperable services".

Wolfgang Ziegler, Fraunhofer SCAI

Expert stakeholder category: Cloud service customer - research

Recommendation targets: Cloud service providers

Recommendation focus: Cloud procurement

"The ISO/IEC 19086 standard for SLAs is explicitly mentioned in the HNSciCloud tender material. Such a standard already represents a level of agreement in the community and should be leveraged. For example, having a service which classifies cloud service provider SLAs for conformance to ISO/IEC 19086 would be very helpful because it would avoid procurers having to perform such an analysis themselves. It would also be helpful for the cloud service providers to see how they perform against a recognised international standard. I could imagine such a service with the results being made publicly available online after having being reviewed by the cloud service provider and some independent and legally competent party. The cloud service providers could do an initial self-assessment by using a revised/expanded version of the SLA Aid questionnaire."

Bob Jones, CERN

3 DSM Initiative on Free Flow of Data: Objectives and impact

The overriding objective of the Digital Single Market (DSM) is to create one of the largest digital marketplaces in the world by making Europe a global leader in ICT. The five building blocks for the DSM are cloud computing, Internet of Things, (big) data technologies, 5G communications and cyber security while ICT standards are considered to be the cornerstone of the DSM.

The strategy for the Digital Single Market recognises the importance of the data economy. Data technologies and services that can be used for the collection, processing or storage of data (e.g. cloud computing, big data, the Internet of Things), are essential factors of progress in the new era of digitalisation.

In the section on "Maximising the growth potential of the Digital Economy", the DSM strategy commits to a European '**Free flow of data**' initiative to tackle restrictions on the free movement of data within the EU and unjustified restrictions on the location of data for storage or processing purposes.

The European Free Flow of Data (EFFD) Initiative therefore seen as an important step at EU level to allow businesses, citizens, researchers and consumers to take full advantage of data technologies and services, such as better access to cloud services and better data analytics. A free flow of data will support connectivity between sectors and industries, lowering costs, stimulating research and innovation and unleashing the potential of new economic models.

Among other issues, the EFFD will address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data. This will encourage access to public data which in turn can help drive innovation.

Actors within the nascent European data market need predictability and legal certainty on these emerging issues, not just 'data ownership' and the other items listed but also

liability arising from the use of data, in order to enter the market and invest in new business models, which is especially vital for European SMEs. Clarity on such emerging issues is also important for all European businesses because they need predictability to assess their current expenditure on research and on product innovation.

Existing legal frameworks and current contractual practices may not be sufficient to provide actors in the data value chain with such predictability and legal certainty. Contractual practices may also create obstacles to the free and smooth flow of data or to data access as well as lock-in effects.

3.1 Recommendations on data ownership and the free flow of data

SLAs generally do not address data ownership itself, although as explained above they may address or should address certain important components and elements thereof. Data ownership is generally not addressed, as it is a particularly complex domain which is difficult to define. For example, CSPs and other vendors may have a totally different opinion or perception about data ownership than CSCs, whether being SMEs or not. Furthermore, the laws and regulations that have deemed to be governing ownership are either outdated or are difficult to interpret, use and enforce in the digital world. It becomes even more problematic where some CSPs are very large, powerful and have a traditional mindset that owning assets, including data, is a goal in itself.

Taking another perspective, ownership of digital data in general is basically not possible. Owning data is just very difficult, as one would like, or need to, share such data, have it processed and transferred. The concept of ownership, blurs the discussion – and sometimes debate – about who is entitled to do what with data, and stalls innovation and the potential of technology in general.

SLA Ready and its consortium partners endorse joining the dialogue about how to be able address this domain of use rights and digital rights management.

With regard to the free flow of data, it can be established that restrictions on the free movement of data within the EU and unjustified restrictions on the location of data for storage or processing purposes are generally not addressed in generic SLAs, which is understood as most restrictions are only applicable to certain industries, markets or use.

Recommendation: SLA-Ready recommends that these restrictions and related compliance matters need to be assessed and dealt with, and where appropriate should be arranged for in a more specific SLA. The latter is not common practice at this point, also not in the relevant higher/highly regulated markets where Free flow of data is quite relevant.

3.2 Recommendations to address Data Protection, Security and Privacy Challenges

The EC Cluster on Data Protection, Security and Privacy (**DPSP Cluster**[3]) has been tasked with identifying challenges for the Free Flow of Data and in defining a research roadmap to address these challenges.

Main working areas of the Free Flow of Data include free movement of data, location of data, ownership, interoperability, usability, access to (public) data, certification, contracts and switch of CSPs.

These topics have a strong relationship to the work carried out in SLA-Ready, in particular with the Common Reference Model. In this section we present SLA-Ready's recommendations on each challenge based on the developed CRM.

3.2.1 Main CRM elements relevant to DPSP challenges

The majority of recommendations make reference to the following CRM elements which reflect the nature of the topic:

Table 1 CRM elements relevant to DPSP challenges

CRM2 Findable: The Cloud Service Customer shouldn't have to spend too much time finding the cloud SLA, and therefore be able to devote time to studying and understanding it.
CRM3 Choice of Law: The choice of law, that is, the law that is proposed to be applicable between the Cloud Service Provider (CSP) and Cloud Service Customer (CSC), can change quite a lot, and this can easily cause confusion about rights and obligations. In addition, cloud service customers often have little relevant knowledge about the mentioned jurisdiction and the consequences it brings by agreeing. Jurisdiction governing contractual relationships often do not correspond to where the CSC may reside or be active with its business. In addition, conflicts between mandatory law where the CSC resides or is active with its end-users, may occur, leading to more insecurity and lack of trust. Generally, a lot of 'one jurisdiction fits all' approaches are encountered, basically being the laws of the country or state of the CSP where it has its headquarters being applicable to any CSC, regardless of where it resides, is active and of which mandatory laws are applicable to the CSC.
CRM4 Roles and Responsibilities: A consistent and sound definition of SLA-related roles and responsibilities is required by the Cloud Service Customer to fully understand in which terms the Cloud Service Provider will commit to provision the cloud service.
CRM11 Machine readable format: Machine-readable SLAs are the basis for integrating realistic levels of automation into the cloud service's life cycle management process (e.g., negotiation and monitoring). This might be a requirement for a Cloud Service Customer that is willing to lower their cloud services' operational costs.

[3] https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

CRM20 Service Level Reporting: Reporting of achieved Service Levels is necessary for CSCs to assess if the provider is fulfilling agreed Service Level Objectives (SLO). In order to guarantee these high levels of assurance and transparency, it is necessary for the CSC to have access to the mechanisms (e.g., tools, specifications) and know-how to perform the monitoring/assessment of CSP's Service Levels.
CRM21 – Service Level Continuous Monitoring: Currently, most cloud mechanisms for service level reporting are "point-in-time" i.e., the Cloud Service Provider periodically performs service level measurement at certain intervals of time. However, these assessments miss Service Level fluctuations (including SLA violations) occurring in between two scheduled assessments. A "continuous monitoring" based approach is much more advantageous for the customer. This fully assesses service levels, covering a specified period of time e.g. the whole contract length. Cloud Service Customers should be well-informed about the provider's capabilities to perform the continuous monitoring of offered Service Level Objectives, along with the associated trade-offs (e.g., performance, and price).
CRM24 Specified SLO Metrics: Well-documented and standardised metric definitions in the SLA will allow customers to compare different cloud offers, or to assess achieved versus committed SLOs during the operation of the cloud service. In general, clearly defined Service Level Objectives (SLO) metrics improve Cloud Service Provider's trust and transparency.
CRM28 Data Management SLOs: Data management SLOs concern aspects such as IPR, CSC/CSP data, derived data, account data, portability, data deletion/location/examination, and law enforcement access to customer data. The data management SLOs presented in the SLA cope with important quantitative and qualitative indicators related with data lifecycle management. They can be considered as complementary to existing and applicable security and data protection certifications offered by the Cloud Service Provider. Customers should verify the fulfilment of their requirements based on the information presented on the SLA and (if applicable) the respective provider's certifications.
CRM29 Security SLOs: Security SLOs concern cryptography, physical/operational/communication security, incident management, compliance, and business continuity. Currently, security is a major concern for (prospective) cloud customers. The specification of security commitments in the Cloud Service Provider SLA (i.e., in the form of SLOs) is expected to become part of standardised SLA templates in the near future. However, it will be equally important for customers to understand how specified security SLOs will relate to their own security requirements (including regulatory compliance). It is important to note that documented good practices do not suggest any specific SLO value to the customer. The required SLO value should be the result of applying a structured risk assessment.
CRM30 Personal data protection SLOs: Personal data management includes issues such as consent and choice, limitation, accountability, personally identifiable information (PII) collection/use/retention/disclosure limitation, and privacy compliance. SLOs related to PII protection should be considered as a critical element for customers, who must ensure compliance with legal obligations that may derive from the use of cloud services. Customers should clearly understand the Cloud Service Provider's roles and responsibilities related to personal data protection both through applicable certifications, codes of conduct, and defined SLOs.

3.2.2 Data Protection, Security and Privacy Challenges and SLA-Ready recommendations

Full control of data flow: *Control of the whole flow including data in transit and data in use, but also data at rest, meaning controlled access and usage of data across country and cloud boundaries. Context based access control policies are part of this challenge.*

Recommendation: Cloud SLA's will play a primary role in relationship to the automation of the envisioned control mechanisms in machine readable SLAs [CRM11]. Also the clear specification of related data management SLOs [CRM28] and associated metrics [CRM24] will be essential to achieve this challenge.

Efficient searchable encryption*: Enabling the efficient search and edit of encrypted data stored and processed in the cloud.*

Recommendation: To meet this challenge the CSP should establish minimum commitments in the relevant SLOs such as Data Management [CRM28], in particular data examination, Law Enforcement Access. Security SLOs [CRM29] are also important, in particular cryptography. Finally, Personal Data Protection SLOs [CRM30] are important, especially related to Consent & Choice.

Privacy preserving cloud-based (identity) services: *Improved and novel cryptographic methods to securely protect, store and share (private) data, including encrypted identity data.*

Recommendation: The cloud SLA should consider the commitments and metrics [CRM24] associated to the envisioned identity services, possibly as part of [CRM29] (Access Control, Cryptography) and [CRM30] (Privacy Compliance).

The cloud SLA should consider the commitments and metrics included in the SLA. Specific SLO metrics associated to the envisioned identity services should be well-documented and include standardized metrics [CRM24] possibly as part of security SLOs [CRM29] such as Access Control and Cryptography and Personal Data Protection SLOs [CRM30] compliance to Privacy certifications.

Fully secure APIs: *In order to enable to securely communicate the identity and user attributes (authentication and authorization) among cloud services.*

Recommendation: The clear specification of SLOs related to security is critical in aspects related to access control, and certifications guaranteeing the security associated with the software development process. The inclusion of customised, but standardised, software security metrics might also become necessary [CRM24].

Data Protection legal framework transparency: *For both cloud consumers and cloud providers.*

Recommendation: Cloud SLAs are a key opportunity for CSP's to improve their transparency. Firstly, it needs to be clear which law is proposed to be applicable between the CSP and the CSC [CRM3]. A consistent and sound definition of SLA-related roles and responsibilities [CRM4] is also required by the CSC to fully understand in which terms the CSP will commit to provision the cloud service. Standards such as ISO/IEC 17788 and ISOIEC 17789 provide details on this.

Reporting of achieved Service Levels [CRM20], is necessary for CSCs to assess if the provider is fulfilling agreed Service Level Objectives (SLO). Mechanisms (e.g., tools, specifications) and know-how to perform the monitoring/assessment of CSP's Service Levels should be clear for CSCs. CSCs require similar levels of understanding regarding the continuous monitoring of SLOs

Cloud Service Customers should be well-informed about the provider's capabilities to perform the continuous monitoring of SLOs [CRM21]. A best practice would be for the CSP to provide a certified form of continuous monitoring-based Service Level reporting e.g. CSA Open Certification Framework – Level 3 (OCF – STAR Continuous).

Finally, SLOs related to personal data protection are key. Metrics definitions associated to these SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Definition and enactment of fine-grained security policies: *Integration and composition of security and privacy policies across different cloud services.*

Recommendation: The real-world implementation of mechanisms related to security policies' composability depends on machine-readable languages [CRM11], which are leveraged on top of standardized metrics sets [CRM24]. The content of the metrics to compose may relate to security SLOs [CRM29].

Security-aware SLA management support for security and privacy terms formalisation, negotiation, composition, monitoring, continuous assurance and automation: *All these elements are applied to multi-cloud or federated cloud-based applications and cloud-services themselves*.

Recommendation: The main elements related to automation related to machine-readable languages/metrics [CRM11] [CRM24], and clearly specified security SLOs [CRM29]. Envisioned management mechanisms may even depend on the CSP willingness to make publicly available its SLA information [CRM2].

Risk assessment frameworks for applications at scale: *Innovative frameworks to assess risk in multi-technology and distributed applications mixing cloud, IoT, Big Data, or mobile addressing security assurance, automated deployment, monitoring and decision making.,…*

Recommendation: Cloud SLAs should be seen as an outcome of envisioned risk assessment frameworks, although CRM elements like security SLOs [CRM29] may provide guidance on used frameworks. Security SLOs concern cryptography, physical/operational/communication security, incident management, compliance, and business continuity.

Secure dynamic composition of cloud services*: This includes dynamic benchmarking and brokering of Cloud services for multi-cloud scenarios as well as federation of clouds.*

Recommendation: As in the case of security policies, the secure composition of cloud services will strongly depend on machine-readable formats [CRM11], standardized metrics [CRM24], and commitment to security SLOs [CRM29].

Cloud Security Certification*: Based on cloud security standards and auditing schemes.*

Recommendation: Certification can aid the creation of trust in cloud services for CSCs. This requires the SLA to include lists of security and privacy certifications which are expected to become SLOs in categories like security [CRM29] and personal data protection[CRM30].

Security- and privacy-by-design in cloud services: *Advanced mechanisms and tools to support the security and privacy intelligence from the early stages of the design of the services.*

Recommendation: The Security- and Privacy-by-design principles should be supported by standardised metrics [CRM24] to support the continuous monitoring of designed vs. achieved levels.

Continuous control of security, privacy conditions and obligations, and adherence to them: *Including continuous monitoring, assurance, enforcement, and automated reaction in inter-clouds, multi-cloud, federated clouds.*

Recommendation: Besides the monitoring of implemented control frameworks, we can expect cloud SLAs to become the focus of upcoming continuous cloud monitoring/assurance mechanisms [CRM21]. The specification of metrics to monitor

[CRM24], formats [CRM11], and commitments [CRM29] will be essential for the implementation of those mechanisms.

Efficient secure and privacy-preserving multi-tenancy in Infrastructure, Platform and Software as a service models: *Including deduplication on encrypted multi-tenant data, or mechanisms for checking integrity and availability of multi-tenant data.*

Recommendation: Apart from the technical SLA commitments related to the cryptographic mechanisms being used [CRM29], this challenge may rely on some of the privacy-related SLOs [CRM30|.

Improve market readiness of security and privacy solutions from projects: *Providing an online marketplace that enables the digital single market to access innovative open source applications with guidance on sustainability and future project exploitation.*

Recommendation: Market readiness is strongly related to the actual objective of the developed CRM, which targets the uptake of cloud systems through comprehensive, although also easy-to-understand SLAs. The foreseen marketplace should implement the contributed CRM in order to facilitate industrial adoption.

4 Cloud Service Providers and SLA Self-assessment

SLA-Ready has raised awareness of the importance of specified definitions of the privacy and security metrics in the Security Level Agreements composed by the CSPs.

In the context of supporting and guiding CSPs in delivering trusted SLAs, SLA-Ready created and distributed a targeted questionnaire to study and gather information on the kind of SLAs the CSPs offer today and at the same time, to examine the completeness of the CRM the project has created for this purpose. The questionnaire was mainly answered by the CSPs whose main cloud service customers (CSC) were SMEs. This way we approach the issue from the SME's perspective as well, and determine what are the needs for SMEs moving to the cloud that existing SLAs do not assist.

From an SLA perspective, CSPs did not identify any crucial gaps that the CRM might have that could prevent it from contributing to the improvement of the way the SMEs deal with cloud services.

From a CSC perspective however, feedback highlighted the following considerations for inclusion in a cloud SLA:

- Indication whether the SLA can be negotiated with the CSP.
- Breach handling and notifications
- Greater visibility of supply chain management and data location

- More information on the identity knowledge of third parties' suppliers.
- Scope of the cloud service. In order to fulfill requirements effectively and efficient, small and medium enterprise need cloud services with a broad scope.
- Global reach of cloud service. In order to support global business activities, small and medium enterprise need cloud services with global reach (e.g. to run applications supporting regional markets).
- Deployment options of cloud services, e.g. multi and single tenant environments. In order to ensure sustainability, small and medium sized companies need cloud services which can address diverse use cases (e.g. with diverse security and privacy classifications).

A total of 25 CSPs completed the questionnaire. This included the 4 successful bidders of the Helix Nebula Science Cloud tender. 15 CSPs agreed to make their information publicly available and this has been published in the SLA Repository[4] within the marketplace.

The remaining providers did not provide their consent to publish results[5] for the following reasons:

- ***The SLAs cannot be publicly available as they are considered only for customers that sign contracts with the respected provider.***
  Often for small providers, their relationship with customers is very personalized and SLAs are created for each customer. The majority of the CSPs do not have their contracted SLAs available online even for their customers to have access.
- ***Lack of understanding of the correlation between publishing the self-assessment as part of the SLA Repository and the CSA STAR Registry and gaining business from it.***
  This reflects a general lack of maturity by CSPs in their approach to SLAs. This includes also awareness of the potential unique selling point that this can bring.
- ***A declared intention to first remediate the weaknesses and reassess the SLA.***
  This demonstrates an intention to act upon CRM recommendations.

Recommendation: Contributions and support to ISO/IEC 19086 are an essential element in creating a culture of trust and transparency in cloud SLAs.

SLA-Ready's work in ISO/IEC 19086 regarding the gaps it has related to the elements covered in the CRM, can help increase the level of comfort and knowledge of CSPs towards a more open and mature approach to SLAs. By being engaged in the activities for commenting the production of the CD version of ISO19086 standard, the project

[4] http://www.sla-ready.eu/sla-repository

[5] For 3 respondents, the questionnaire was answered for information purposes with respect to the HNSciCloud PCP with the understanding that the answers to the questionnaire shall help developing the terms and conditions for the future phases without being binding. SLA-Ready is providing feedback to HNSciCloud based on questionnaire responses.

contributes to the development of a complete set of guidelines for conducting more comprehensive service level agreements in the cloud services market.

The quality of work and results SLA-Ready offers as well as the spectrum its products apply to (ISO/IEC, CSPs, SMEs) can take SLA delivery to the next level of quality, trust and openness.

In the next section we go into more detail on how SLA-Ready has contributed to the SLA standardisation process.

5 Supporting the uptake and adoption of standards

This section summarises the project's contributions to relevant cloud SLA standardisation and best practices initiatives, which were performed during SLA-Ready's Year 2 period. For each reported initiative the following information is presented:

- Brief introduction of the standard/best practice being contributed.
- Summary of the submitted contribution and, where applicable, the actual form[6] with the provided comments.
- Existing gaps and expected follow-ups after the duration of the project.

5.1 ISO/IEC 19086 Part 2 – Metrics

In July 2016 this draft standard went into its CD version[7]. It proposes a technical model for specifying cloud SLA metrics, which can be then used for automation, CSP comparison, service monitoring, and so forth.

Year 2 Activities.

The major contribution of SLA-Ready to ISO/IEC WD 19086-2 referred to the inclusion of Service Quantitative Objectives (SQOs) into the conceptual model, in order to keep alignment with ISO/IEC 19086-1. Furthermore, SLA-Ready also provided a major contribution related to validating the proposed model with respect to the security and privacy metrics being documented in ISO/IEC 19086-4. The validation took place by specifying one privacy and one security metric with the proposed model, along with the respective machine-readable versions. The documented contribution can be seen in Annex 2 of this deliverable. All submitted comments were accepted and published as part of ISO/IEC CD 19086-2.

[6] Due to copyright restrictions, the original ISO/IEC commenting form could not be included in this deliverable. Therefore we have proceed to attach a modified version of it.

[7] For an overview related to the development of ISO/IEC standards, see http://www.iso.org/iso/home/standards_development.htm.

Existing Gaps and Future Activities.

Upcoming contributions to ISO/IEC 19086-2 will be focused on the following conspicuous gaps still detected on the latest version of the draft standard:

- Refinement of the proposed machine-readable SLA specification taking into account the final (FDIS) release of ISO/IEC 19086-1.
- Contribution to the companion technical report (metrics catalogue), in particular related to documenting security and privacy metrics with the proposed model.

Given the finalisation of the SLA-Ready project, partner CSA is expecting to perform the related standardisation efforts in the H2020 CloudWATCH2 project[8], where CSA leads this specific topic.

5.2 ISO/IEC 19086 Part 3 – Core Requirements

Based on both ISO/IEC 19086 Part 1 and Part 2, this draft "core requirements" document (currently in DIS version) provides conformance criteria for Cloud SLAs based on three main pillars:

1. Manifest of applicable documents (e.g., master service agreements, etc.),
2. Covered services,
3. Cloud SLA definitions including areas and components defined in Part 1.

For each pillar, and following the structure from Part 1, this draft presents particular requirements for assessing conformance. For example, the ISO/IEC 19086 Part 3 defines that the "covered services" component referenced in Part 1 shall identify the Cloud service(s) that are covered by the Cloud SLA.

Year 2 Activities.

The consortium provided a contribution based on the CRM and its good practices, just as documented in Deliverable 2.4 and this deliverable respectively. Particular emphasis was put on highlighting the SME-perspective, contrary to the CSP-focus put in the reviewed version of the draft standard. For example, SLA-Ready highlighted the need to specify the uses of derived CSC data, audit targets, and circumstances for service termination (CSP-initiated). The provided contribution can be seen in Annex 2, and the corresponding disposition of comments has been accepted by the ISO secretariat. Balloting on the comments will be done after the finalisation of the SLA-Ready project.

Existing Gaps and Future Activities.

The conformance requirements presented in ISO/IEC 19086-3 focus on SLA areas not related to security or privacy. Despite ISO/IEC 19086-3 references ISO/IEC 19086-4 for any specific security/privacy requirements, the later basically discusses "implementation

[8] Please refer to http://www.cloudwatchhub.eu/

guidelines" and not conformance requirements. The coverage of security and privacy conformance requirements is a topic to be further elaborated after the finalisation of SLA-Ready, most likely in the context of H2020 CloudWATCH2.

At the time of writing this deliverable the current version of ISO/IEC 19086-3 was still missing some specific CRM elements, most of which were also not included in ISO/IEC 19086-1. We refer in particular to the General, Freshness and Readability elements. Through its dissemination actions (including the tutorials and workshops in WP4), SLA-Ready identified the importance of the referenced elements for SMEs willing to embrace cloud SLAs. After the finalisation of SLA-Ready, partners Trust-IT and CSA will continue contributing with those elements to ISO/IEC 19086-3 (e.g., through CloudWATCH2).

5.3 ISO/IEC 19086 Part 4 – Security and Privacy

Late 2014 CSA participated on a proposal for a new working item under ISO/IEC JTC 1/SC27 (IT security techniques) which became the current 19086-Part 4 draft. Given its strong relationship to ISO/IEC SC38, during Q2/2015 the SC27 committee created a liaison with SC38 to leverage their cloud expertise on the SLA topic.

Year 2 Activities.

The contribution of SLA-Ready to ISO/IEC WD 19086-4 referred to the Security and Protection of Personally Identifiable Information components. While SLA-Ready contributed to the inclusion of Service Quantitative Objectives (SQOs) into the conceptual model in ISO/IEC 19086-2, it also provided a major contribution related to validating the proposed model with respect to the security and privacy metrics being documented in ISO/IEC 19086-4. The validation took place by specifying one privacy and one security metric with the proposed model, along with the respective machine-readable versions. While the comments on the guidance on SLOs and SQOs as well as the comments on the security components and privacy commitments were not yet addressed, extensive changes were applied to clause 7 on Security Components and to clause 8 on Security and Protection of Personally Identifiable Information Components. The documented contribution can be seen in Annex 2 of this deliverable.

Existing Gaps and Future Activities.

The consortium provided a major contribution on Security Components and on Security and Protection of Personally Identifiable Information Components of SLOs. The provided contribution can be seen in Annex 2. While the security components and privacy commitments were not addressed in the CD current version of the ISO/IEC 19086-4, new CD version will be issued and CSA will continue contributing on security components and privacy commitments after the finalisation of SLA-Ready project.

5.4 EU Catalogue of Standards

During June 2016 the SLA-Ready consortium was invited to participate in the development of the "EU Catalogue of Standards" (project led by the Cloud Unit and

executed by Trilateral Research Ltd.). This initiative seeks to develop a set of use cases and associated standards to support public procurers in the uptake of new technologies, where cloud is one of the four domains being covered. Some of the problems targeted by the catalogue can be seen in Figure 1.

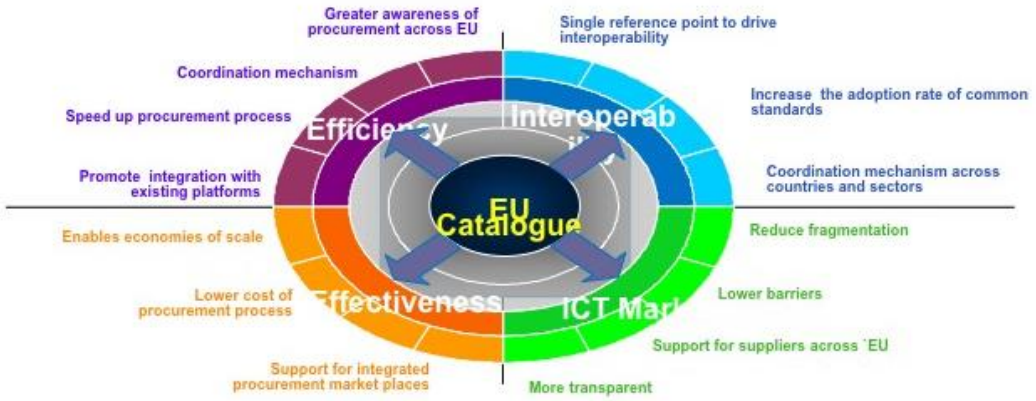

Figure 1. EU Catalogue of Standards.

When contacted by the EC, the SLA-Ready consortium was requested to support the contractor in putting together the content which will appear within the initial prototype of the catalogue. In essence, the contractor requested a project's contribution/feedback on the sub-topics related to SLAs, security, and privacy for inclusion within the Catalogue.

SLA-Ready's contributions to the catalogue focused on the following topics (within the SLA sub-domain):

- Guidelines for interoperability and implementation, based on the project's Common Reference Model.
- Major contribution to the four documented use cases, in particular related to the relevant guides to the application of referenced standards.
- List of relevant cloud SLA standards and best practices.

Full details of the contribution can be found in Annex 3.

5.5 CSA Security as a Service – Continuous Monitoring

Numerous security vendors are now leveraging cloud-based models to deliver security solutions. This shift has occurred for a variety of reasons including greater economies of scale and streamlined delivery mechanisms. Regardless of the motivations for offering such services, CSCs are now faced with evaluating security solutions which do not run on premises. Therefore, consumers need to understand the unique nature of cloud delivered security offerings so that they are in a position to evaluate the offerings and to understand if they will meet their needs. Given this background, the CSA founded a working group on the topic of Security-as-a-Service[9] (SecaaS). The purpose of this working

[9] Please refer to https://cloudsecurityalliance.org/group/security-as-a-service/

group is to identify consensus definitions of what SecaaS means, to categorize the different types of SecaaS and to provide guidance to organizations on reasonable implementation practices.

Within SecaaS, the topic of continuous monitoring was identified as a priority for the working group. Continuous Monitoring performs the function of continuous risk management presenting the current security posture of the organization. Using industry approved risk management frameworks, Continuous Monitoring collects inventory of deployed organizational assets (including but not limited to current patch/version status, vulnerabilities, threats, and traffic) and generates ongoing risk scores across the enterprise. The intent of Continuous Monitoring is to reduce the time and effort required to identify security risks, assist in defining mitigation strategies, and implement any necessary controls reducing the security risk window.

6 Conclusions

This document has provided an overview of recommendations and actions regarding the standardisation of cloud SLAs. This reflects SLA-Ready's activities in engaging with a diverse range of experts including Advisory Board members, recommendations relating to cloud SLAs based on future research challenges for Data Protection, Security and Privacy supporting future research, and recommendations and actions in supporting the uptake and adoption of standards in cloud SLAs through contributions to ISO 19086 and other standardisation initiatives such as the EU catalogue of standards.

Our experts provided insight on the importance of greater standardisation in cloud SLAs in order build trust and in turn increase adoption by SMEs. SLAs need to become trusted sources of information. The best way to achieve transparency, and therefore trust, is to adopt a set of standards as mandatory reference for such SLAs. The CRM is a reference point for providers using open source software wishing to implement best practices for transparent Cloud SLAs and facilitate comparability of services. Transparency will support competition and general acceptance of cloud technology among EU businesses.

SLA-Ready's SME workshops were designed to educate SMEs on areas of cloud SLAs, in particular legal topics including data protection. Indeed, SME associations recognize the need for regular 'Legalese workshops' to help SMEs overcome the language barrier when signing cloud contracts.

The need for a generally usable solution for cloud SLAs standards with relevance for implementing interoperable services was also recognized as well as the need for restrictions on the free movement of data and related compliance matters need to be addressed in a more specific way.

The importance of having a service which classifies cloud service provider SLAs for conformance to ISO/IEC 19086 was also recommended as a way to avoid cloud procurers having to perform such an analysis themselves.

Based on the CRM, this report has also provided recommendations relating to cloud SLAs for future research challenges in Data Protection, Privacy and Security, in support of the EC Cluster to which SLA-Ready contributes. Cloud SLA's will play a primary role in relationship to the automation of the envisioned control mechanisms in machine readable SLAs. Also the clear specification of related data management SLOs and associated metrics will be essential to achieve full control of data flow which is of high importance for the DSM initiative on the free flow of data. Specified SLOs, security SLOs and personal data protection SLOs were all of high relevance to address these challenges.

Feedback from CSPs on the CRM was also provided, highlighting that from a CSP perspective no major gaps in the CRM had been identified. Suggestions from a CSC perspective were also provided including clearer indications on whether the SLA can be negotiated with the CSP; breach handling and notifications; and greater visibility of supply chain management and data location.

In addition to these recommendations, this deliverable has also reported on the project's contributions to standards/best practices which have taken place during Year 2. It is worth to highlight our efforts to position SLA-Ready as key contributor to ISO/IEC 19086-2 and ISO/IEC 19086-3. Given the lifetime of relevant standardisation activities, the consortium has also taken some initial set of actions to continue its engagement with SDOs like ISO/IEC through the EU H2020 CloudWatch2 project. Those sustainability actions have been also documented in this deliverable.

Annex 1 - Document Log

DOCUMENT ITERATIONS		
V1.0	ToC and initial contributions	Nicholas Ferguson, Trust-IT & Jesus Luna, CSA
V2.0	Initial first draft including DPSP recommendations and Standards update	Nicholas Ferguson, Trust-IT & Jesus Luna, CSA
V3.0	New sections on Expert views and CSP self assessment questionnaire	Stephanie Parker, Trust-IT & Damir Savanovic, CSA
V4.0	Further general edits	Silvana Muscella, Nicholas Ferguson & Stephanie Parker, Trust-IT
V5.0	Internal review	Arthur van der Wees, Arthur's Legal
V6.0	Final Version	Nicholas Ferguson, Trust-IT

Annex 1 – Contributions to ISO/IEC 19086-2

This annex presents the project's contributions to ISO/IEC WD 19086-2, just as presented in Section 3.

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment	Comments	Proposed change	Observations of the secretariat
	45	4		Ed	The "Note to Entry" related to Measurement Result actually seems to be referring to the term Measure.	Seems that this Note to Entry should be deleted.	
	97	6.2		Te	Missing reference to 19086-4	This line should read "…with associated SLOs/SQOs is included in ISO/IEC 19086-1 and 19086-4.""	
	141 and 143	6.2.2		Te	Missing reference to SQOs	These lines should read as follows "…making process, the SLOs/SQOs are currently described using natural language and take different forms depending on the CSP. This not only adds ambiguity to the process, it adds additional time and complexity to the process as each SLO/SQO must be thoroughly reviewed and assed in each case."	
	278	6.4.2		Ed	The sentence seems to be broken	Please rephrase as: "Since a cloud metric describes not only the requirements for measuring a characteristic but it also describes the…"	
	311	6.4.2		Te	Missing reference to SQOs	Line should be changed to "…measurement results against the SLO/SQO commitments made in cloud service agreements".	
	319 - 323	6.4.2		Te	Missing reference to SQOs	Line should be changed to: "Since the measurement is based on the same metric that is used to describe the characteristic in the SLA (through the SLO/SQO) it is straightforward to compare the service level measurement result to the SLO/SQO commitment (shown in Figure 5). If the service level does not meet the SLO/SQO, then the commitment is not met and a remedy, as described in the service agreement, will likely be sought.	

	333 – 346	6.5		Te	Missing reference to SQOs	Please change to: “The use of metrics for cloud services can be broken down into three general types 1) describing a service characteristic for service selection 2) describing an SLO/SQO used in a SLA, and 3) comparing a measurement result to an SLO/SQO value to verify service performance. Metrics are essential, not just within each of these concepts, but to connect these three distinct parts of the cloud procurement and operation process. Among the things that a cloud service agreement (CSA) contains are the covered services, the rights and responsibilities of both the CSP and the CSC and other terms and conditions. It also contains information related to the measurement of cloud service properties (e.g., its performance level). The definition and usage of appropriate metrics with their underlying measures are essential components of the Service Level Agreement (SLA) and Service Level Objectives (SLO) and Service Quantitative Objectives (SQO), which are constituents of the CSA. At this point, the metrics are used to set the boundaries and margins of errors the provider of the service commits to and their limitations. For instance, metrics could be used at runtime for service monitoring and balancing, or remediation (e.g., financial). Standardized metrics and metric templates for CSAs makes it easier and quicker to develop SLAs and included SLOs/SQOs. Additionally, standardized metric templates make it easier to compare cloud services form different providers. ”	
	347	6.5		Ed	Missing reference at the beginning of this line	This may seem to be referring to a figure, please fix.	
	370	7.1		Te	Missing reference to 19086-4	Please use the following text: “A defined metric or formula in the context of 19086-2 should directly reference to which SLO/SQO of 19086-1 or 19086-4…”	
	372	7.1		Ed	Broken sentence	The following sentence should be revised: “Not all actors of metrics need or want to the same amount of information related to such metrics.” It should probable read as “Not all actors of metrics need or want to access the same amount of information related to such metrics.”	
	379	7.2		Ed	Broken sentence	Please fix the following sentence: “to identify the metric a provide a basic description. ”	

	392	7.2.1		Te	Missing SQO example	Please consider using the following example of a privacy-related SQO: Description: This SQO relates to a qualitative metric describing the type of consent obtained for collecting, using and sharing PII data. The type of consent can be ranked in levels according to its preference. Formulation and output: • Level 0 – No Consent: Consent is not obtained at or before collection of private data. • Level 1 – Implied Consent: The consent is inferred from the behavior of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered. • Level 2 – Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered. • Level 3 – Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data.	
	459	A.1.2		Te	Missing reference to 19086-4, also we detected a broken sentence	Please change the referred line to “To facilitate the discussion of metrics supporting 19086-1 and 19086-4 SLOs and SQOs a metric model shown in Figure 8 is…”	
	480	A.1.3		Ed	Broken sentence	Please change the referred phrase to: “The Metric class contains the basic information related to the metric. ”	
	482	A.1.3		Te	Missing notion of SQOs	Please change the referred phrase to: “The Expression contains the equations or textual description (e.g., expressed in natural language) need to quantitatively or qualitatively calculate a value for a measurement based upon the metric. ”	
	484	A.1.3		Ed	Broken sentence	Please fix the following sentence: “…UnderlyingMetrics that take are written in the same form as the Metric…”	
	488	A.1.3		Te	The role of the Extend element could be better understood with a simple example.	Please change the sentence to: “Additional elements can be added under the Extend element as needed (e.g., to add information related to the evidence that need to be provided to assess the confidence level of the measurement result). ”	
	492	A.1.4	Table	Te	The Expression field on the table needs to consider textual descriptions for SQOs	Please consider modifying to: “The expression of the calculation of the Metric and supporting information. An SLO metric shall have an expression while an SQO may or may not have an expression (e.g., specified in natural language).”	

	493	A.1.4	Table	Te	The usage of ids within an Expression is not clear	Consider rephrasing as: "…the expression statement used to quantitatively or qualitatively compute the metric. Where necessary it can be written using the ids to represent UnderlyingMetrics, parameters, and rules."	
	510 – 512	B.1.1		Ed	Missing reference to SQO, broken section reference	Please change to: "The template described provides the format necessary for creating a metric that can be used for describing an SLO/SQO value. If a document-based format is used for a metric, these tables shall be used. The details of each attribute are described above in Annex A.1."	
	517	B.1.2		Te	Not all expressions should be equations	Please change to: "The **Expression table** contains the expression (e.g., equation or textual description) for quantitatively or qualitatively calculating the measurement described by the"	
	536 – 537	B.2		Te	SLO/SQO are evaluated with respect to Service Levels (cf., 19086-1)	Please change to: "The following table provides the information necessary to evaluate an SLO or SQO against a measured Service Level when both the SLO/SQO and the measurement result (quantitative or qualitative) are based on the same metric."	
	655	C		Te	Missing reference to SQOs and 19086-4	Please change to: "**(informative) SLOs/SQOs listed in 19086-1 and 19086-4**" And add the following: **The following SLOs/SQOs are listed in ISO/IEC 19086-4** Information security policy • Separation of roles and responsibilities • Accountability, classification, and inventory of assets • Mean time required to revoke user access • User registration and de-registration • Monitoring and logging • Authentication mechanisms • Third party authentication support • Strong authentication • Cryptographic controls policy • Key management • Data at rest • Data Center Monitoring • Secure disposal and re-use of equipment	

						• Percentage of timely vulnerability reports • Change management • Malware protection • Vulnerability management • Network segregation • Secure communications • Information security risk analysis • Secure development • Incident management procedures • Standards or Regulations • Audits • Attestations • Certificates • Principals Rights Capabilities • Provider processing of PII • Transparency • Temporary File Erasure Period • Use, retention and disclosure of data • PII Subcontractor List • Consent for collection, use or retention of data • General consent for data use • PII Data Breach Notification Period • PII Retention Period • PII Data Breach Notification Method • PII Disposal Policy • Geographical Location of PII	
	654	B.3		Te	An example of SQO is missing	Please add the SQO example included in Appendix 1 of this commenting form	

APPENDIX 1.

Type of PII Consent example SLO using tables

General

The following is an example of a qualitative privacy metric describing the type of consent obtained for collecting, using and sharing PII data (based on ISO/IEC WD 19086-4, NIST 800-53v4, and GAPP). The type of PII consent can be ranked in levels according to its preference.

Example Availability SQO

Guarantee

The cloud service customer (i.e., data subject) must provide unambiguous consent to the CSP for collecting or using his PII data. Such consent to be expressed by a statement or by a clear affirmative action. If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SQO text

The PII consent is defined by the CSP in a qualitative manner, so that data subjects can provide their consent based on any of the following levels:

- Level 0 – No Consent: Consent is not obtained at or before collection of PII data.
- Level 1 – Implied Consent: The consent is inferred from the behavior of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered.
- Level 2 – Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered
- Level 3 – Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data.

This gives enough information to build a metric for PII Consent. In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of PII Consent Example using tables

A cloud SQO consists of a description of the characteristic being committed to, the qualitative value for the SQO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (TypePIIConsent, TC_001)	
scale	ORDINAL
Unit	--
note	The type of consent obtained for collecting, using and sharing private data is ranked in levels.
Expression	TCE_001
Parameters	--
rules	--
underlyingMetrics	TL_001_L0, TL_001_L1, TL_001_L2, TL_001_L3

extend	--

Expression (TCE_001)	
expression	TC_001 is equal to the value of either TL_001_L0, TL_001_L1, TL_001_L2, or TL_001_L3, depending on the fulfilment of their respective rules (namely, TL_001_R0, TL_001_R1, TL_001_R2, and TL_001_R3)
expressionLanguage	ENGLISH
note	--

Metric (TypeOfConsent_Level0, TL_001_L0)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R0
underlyingMetrics	--
expression	0
expressionLanguage	ISO80000

Rule (TL_001_R0)	
rule	No Consent: Consent is not obtained at or before collection of private data
ruleLanguage	English

Metric (TypeOfConsent_Level1, TL_001_L1)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R1
underlyingMetrics	--
expression	1
expressionLanguage	ISO80000

Rule (TL_001_R1)	
rule	Implied Consent: The consent is inferred from the behaviour of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered
ruleLanguage	English

Metric (TypeOfConsent_Level2, TL_001_L2)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R2
underlyingMetrics	--
expression	2
expressionLanguage	ISO80000

Rule (TL_001_R2)	
Rule	Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered.
ruleLanguage	English

Metric (TypeOfConsent_Level3, TL_001_L3)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R3
underlyingMetrics	--
expression	3
expressionLanguage	ISO80000

Rule (TL_001_R3)	
Rule	Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data

ruleLanguage	English

SQO Metric PII Consent Example expressed in XML

The following code represents the PII Consent example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>
<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"
 xmlns:myns="http://custom"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd
  http://custom custom.xsd">

 <Metric id="TC_001" description="TypeOfConsent" scale="ORDINAL" note="The type of consent obtained for collecting, using and sharing private data is ranked in levels">
  <Expression  expression="TC_001 is equal to the value of either TL_001_L0, TL_001_L1, TL_001_L2, or TL_001_L3, depending on the fulfillment of their respective rules (namely, TL_001_R0, TL_001_R1, TL_001_R2, and TL_001_R3) " expressionLanguage="English"/>
  <UnderlyingMetricRef refid="TL_001_L0"/>
  <UnderlyingMetricRef refid="TL_001_L1"/>
  <UnderlyingMetricRef refid="TL_001_L2"/>
  <UnderlyingMetricRef refid="TL_001_L3"/>
 </Metric>
 <Metric id="TL_001_L0" description="TypeOfConsent_Level0" scale="ORDINAL">
  <Expression  expression="0" expressionLanguage="ISO80000"/>
  <Rule id="TL_001_R0" ruleLanguage="English" xml:lang="en"
   ruleDefinition="No Consent: Consent is not obtained at or before collection of private data"/>
 </Metric>
 <Metric id="TL_001_L1" description="TypeOfConsent_Level1" scale="ORDINAL">
  <Expression  expression="1" expressionLanguage="ISO80000"/>
  <Rule id="TL_001_R1" ruleLanguage="English" xml:lang="en"
   ruleDefinition="Implied Consent: The consent is infered from the behaviour of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered"/>
 </Metric>
 <Metric id="TL_001_L2" description="TypeOfConsent_Level2" scale="ORDINAL">
  <Expression  expression="2" expressionLanguage="ISO80000"/>
  <Rule id="TL_001_R2" ruleLanguage="English" xml:lang="en"
```

```
    ruleDefinition="Opt-out Consent: Data subjects can take measures for prevent the collection of private
data, but no opt-in mechanisms are offered."/>
 </Metric>
 <Metric id="TL_001_L3" description="TypeOfConsent_Level3" scale="ORDINAL">
  <Expression  expression="3" expressionLanguage="ISO80000"/>
  <Rule id="TL_001_R3" ruleLanguage="English" xml:lang="en"
    ruleDefinition="Opt-in Consent: Data subjects explicitly grant permission for collecting or using private
data"/>
 </Metric>
</Metrics>
```

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SQO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SQO Evaluation (id)	
slo_id	SQO_TC_001
metric_id	TC_001
slo_value	3
measurementResult_value	3
uncertainty	Third Party Audit-based
measurementTime	May 25th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Level of redundancy (LoR)

General

In the following, a metric describing the level of redundancy required for a given system component (e.g., a web server) is described. The level of redundancy is expressed as a numeric integer value and can be calculated in different ways.

Example of SLO

Guarantee

The CSP must ensure that, at any time during system operation, at least N replicas of the component are up and running, with N defined by the cloud service customer (CSC). If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SLO text

The level of redundancy is defined as an integer >= 1.

In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of LoR Example using tables

A cloud SLO consists of a description of the characteristic being committed to, the quantitative value for the SLO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (LevelOfRedundancy_p, LOR_001)	
scale	RATIO
Unit	--
note	The level of redundancy is an integer number and can be measured by counting the number of active replicas of the component (NOR)
Expression	LOR_001_Exp
Parameters	LOR_001_P001
rules	LOR_001_R001
underlyingMetrics	--
extend	--

Expression (LOR_001_Exp)	
expression	LOR_001 = NOR
expressionLanguage	ISO80000
note	NOR is obtained via the strategy defined by rule LOR_001_R001

Parameter (LOR_001_P001)	
parameterDefinition	ping interval
unit	seconds

Rule (LOR_001_R001)	
rule	The number of active component replicas (NOR) is checked by pinging them every LOR_001_P001 seconds
ruleLanguage	English

Metric (LevelOfRedundancy_hb, LOR_002)	
scale	RATIO
Unit	--
note	The level of redundancy is an integer number and can be measured by counting the number of active replicas of the component (NOR)
Expression	LOR_002_Exp
Parameters	LOR_002_P001
rules	LOR_002_R001
underlyingMetrics	--
extend	--

Expression (LOR_002_Exp)	
expression	LOR_002 = NOR
expressionLanguage	ISO80000
note	NOR is obtained via the strategy defined by rule LOR_002_R001

Parameter (LOR_002_P001)	
parameterDefinition	Heartbeat interval
unit	seconds

Rule (LOR_002_R001)	
rule	The number of active web server replicas (NOR) is checked by means of heartbeats generated by replicas every LOR_002_P001 seconds
ruleLanguage	English

SLO Metric LoR Example expressed in XML

The following code represents the LoR example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>
<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"
 xmlns:myns="http://custom"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd
   http://custom custom.xsd">
<Metric id="LOR_001" description="LevelOfRedundancy_p"
   scale="RATIO" unit="n/a">
        <Expression expression="LOR_001 = NOR" expressionLanguage="ISO80000"/>
        <Rule id="LOR_001_R001" ruleLanguage="English" xml:lang="en"
   ruleDefinition="The number of active component replicas (NOR) is checked by pinging them every
LOR_001_P001 seconds" />
        <Parameter id="LOR_001_P001" parameterDefinition="ping interval" unit="seconds"/>
 </Metric>
 <Metric id="LOR_002" description="LevelOfRedundancy_hb"
   scale="RATIO" unit="n/a">
        <Expression expression="LOR_002 = NOR" expressionLanguage="ISO80000"/>
        <Rule id="LOR_002_R001" ruleLanguage="English" xml:lang="en"
   ruleDefinition="The number of active web server replicas (NOR) is checked by means of heartbeats
generated by replicas every LOR_002_P001 seconds" />
        <Parameter id="LOR_002_P001" parameterDefinition="heartbeat interval" unit="seconds"/>
 </Metric>
</Metrics>
```

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SLO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SLO Evaluation (id)	
slo_id	SQO_LOR_001
metric_id	LOR_001
slo_value	3
measurementResult_value	3
uncertainty	Third Party Audit-based
measurementTime	May 27th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Scan frequency (SF)

General

In the following, a metric describing the frequency of execution of scanning activities (e.g., to detect vulnerabilities) is described. The scanning frequency is expressed as a numeric integer value representing the number of seconds elapsed between two subsequent scans.

Example SLO

Guarantee

The CSP must ensure that a scan is executed every N seconds, where N is defined by the cloud service customer (CSC). If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SQO text

The scanning frequency is defined by the CSP as an integer>=1.

In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of SF Example using tables

A cloud SLO consists of a description of the characteristic being committed to, the quantitative value for the SLO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (ScanFrequency, SF)	
scale	RATIO
Unit	--
note	--
Expression	SF_Exp
Parameters	SF_P001
rules	SF_R001
underlyingMetrics	SR_AGE
extend	--

Expression (SF_Exp)	
expression	SF = 1/SR_AGE
expressionLanguage	ISO80000
note	

Parameter (SF_P001)	
parameterDefinition	scan interval
unit	seconds

Rule (SF_R001)	
rule	The scan starts as soon as the software is deployed and is performed every SF_P001 seconds.
ruleLanguage	English

Metric (ScanningReportAge, SR_AGE)	
scale	RATIO
Unit	millisec
note	--
Expression	SR_AGE_Exp
Parameters	SR_AGE_P001
rules	--
underlyingMetrics	--
extend	--

Expression (SR_AGE_Exp)	
expression	SR_AGE = NOW - SR_AGE_P001
expressionLanguage	ISO80000
note	

Parameter (SR_AGE _P001)	
parameterDefinition	report generation timestamp
unit	millisec

Parameter (NOW)	
parameterDefinition	current time
unit	millisec

SLO Metric SF Example expressed in XML

The following code represents the PII Consent example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>
<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"
  xmlns:myns="http://custom"
```

```
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd
  http://custom custom.xsd">

<!-- scanning frequency: obtained by calculating the time elapsed since the generation of the last report -->
 <Metric id="SF" description="ScanFrequency" scale="RATIO" unit="n/a">

  <!-- this metric uses SR_AGE for its expression -->
  <UnderlyingMetricRef refid="SR_AGE"/>
  <Expression expression="SF=1/SR_AGE" expressionLanguage="ISO80000"/>
  <Rule id="SF_R001" ruleLanguage="English" xml:lang="en"
   ruleDefinition="The scan starts as soon as the software is deployed and is performed every SF_P001 seconds." />
  <Parameter id="SF_P001" parameterDefinition="scan interval" unit="seconds"/>
</Metric>
 <!-- scanning report age -->
<Metric id="SR_AGE" description="ScanningReportAge" scale="RATIO" unit="millisec">
  <Expression expression="SR_AGE = NOW - SR_AGE_P001" expressionLanguage="ISO80000"/>
  <Parameter id="SR_AGE_P001" parameterDefinition="report generation timestamp" unit="millisec"/>
  <Parameter id="NOW" parameterDefinition="current time" unit="millisec"/>
 </Metric>
</Metrics>
```

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SLO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SLO Evaluation (id)	
slo_id	SQO_SF
metric_id	SF
slo_value	30
measurementResult_value	30
uncertainty	Third Party Audit-based
measurementTime	May 27th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Annex 2 – Contributions to ISO/IEC 19086-3

Next is presented the consortium contribution to ISO/IEC DIS 19086-3.

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment	Comments	Proposed change	Observations of the secretariat
	21 – 24	5		Te	In the following phrase defining compliance related to 19086-2: "19086-2 includes a metrics model that may be used to express a specific metric. A conforming cloud SLA is encouraged to use metrics specified using the metric model in ISO/IEC 19086-2. A conforming cloud SLA should define what metrics are used, and a CSP should use metrics defined using the metric model in ISO/IEC 19086-2." The second sentence seems to imply that the use of 19086-2 is optional (even for complaint SLAs), whereas the next phrase seems to imply that it is mandatory ("..a CSP should use metrics….").	In order to avoid ambiguities, and allow compliant cloud SLAs to fully benefit from the features offered by ISO/IEC 19086-2 we recommend using the following paragraph: "19086-2 includes a metrics model that may be used to express a specific metric. A conforming cloud SLA should use metrics specified using the metric model in ISO/IEC 19086-2. A conforming cloud SLA should define what metrics are used, and a CSP should use metrics defined using the metric model in ISO/IEC 19086-2."	
	32	5		Te	There is no reference to the compliance criteria related to ISO/IEC 19086-4	We recommend adding the following paragraph: "19086-4 includes one or more SLOs or SQOs for security and privacy related components and content areas. A conforming cloud SLA is encouraged to use SLOs and SQOs from ISO/IEC 19086-4, when appropriate. Further conformance criteria for those components and content areas is defined in ISO/IEC 19086-4"	
	6 - 9	8		Te	In the phrase: "The role of cloud service level objectives,	In benefit of CSP transparency the following change is recommended:	

					cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA is covered in ISO/IEC 19086-1. There are no conformance requirements for role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA." the lack of conformance requirements related to remedies and exceptions in the SLA may be detrimental to the CSC, therefore forbidding the CSC to make informed decisions.	"The role of cloud service level objectives, cloud service qualitative objectives, metrics, remedies, and exceptions in the cloud SLA is covered in ISO/IEC 19086-1. There are no conformance requirements for role of cloud service level objectives, cloud service qualitative objectives, metrics in the cloud SLA. Remedies and exceptions should be clearly specified to the CSC in the SLA in order to be conformant to this standard."	
	14	10.2.1		Te	The phrase: "An accessibility component shall specify one or more SQOs for accessibility (see ISO/IEC 19086-1 for SQOs)" should also consider the existence of accessibility SLOs, despite these do not appear on ISO/IEC 19086-1. As mentioned on 19086-1: "Listed SLOs and their associated metrics and listed SQOs in each cloud SLA component in Clause 9 and Clause 10 are not meant to be prescriptive or be an exhaustive list for CSPs to use in their SLAs"	The following change is recommended: "An accessibility component shall specify one or more SLOs or SQOs for accessibility (see ISO/IEC 19086-1 for a non-exhaustive list of SQOs)"	
	17 - 22	10.2.1		Te	In the following two phrases: "An accessibility standards shall provide a statement listing any accessibility related standards the CSP supports in the covered services" and "An accessibility policies shall provide a statement listing policies and regulations for accessible ICT the CSP supports in the covered services"	To avoid confusions the conformance requirements should refer to the actual list of standards and policies/regulations. We recommend the following changes: "An accessibility standards shall list any accessibility related standards the CSP supports in the covered services" and "An accessibility policies shall list any policies and regulations for accessible ICT	

					the use of the term “statement” is not clear.	the CSP supports in the covered services”	
	29 - 30	10.3.1		Te	The following statement: “An availability SLO shall provide the amount or percentage of time in a given period that the cloud service is accessible and usable.” Does not specify the cloud actor that should be able to access and use the cloud service i.e., the cloud service customer.	The following change is recommended: “An availability SLO shall provide the amount or percentage of time in a given period that the cloud service is accessible and usable by the CSC.”	
	29 – 30	10.3.1		Te	The conformance criteria for the Availability SLO does not consider the existence of potential carve-outs (exceptions).	To be discussed.	
	12 – 14	10.5.1		Te	The following paragraph: “The cloud SLA shall include relevant information on what protection of PII requirements need to be met and what security controls are implemented to meet these protection of PII requirements. For details, refer to ISO/IEC 19086-4 for SLOs and SQOs relating to the protection of PII component” Introduces the following ambiguities: -At state of practice PII requirements are defined by the CSC along with the required level of protection. The current text seems to imply that the CSP defines the PII level of protection for the CSC requirements. -The controls implemented to meet the CSC requirements may relate to both security (e.g., ISO/IEC 27017) and privacy (ISO/IEC 27018), not only security as	The proposal is to define “core requirements” related to security and privacy in ISO/IEC 19086-4. In that case the proposed text to include in 19086-3 would be: “Core requirements related to the PII content area are defined in ISO/IEC 19086-4, which focuses on the definition of SLOs and SQOs with reference to the cases where the CSP acts as a data processor, on behalf of its CSC (data controller). CSPs that act as data controllers or joint controllers (notably by processing personal data for their own purposes, outside of an explicit mandate from the CSC) may still make reference to ISO/IEC 19086-4, but they and their customers need to ensure compliance with legal obligations that may derive from their controller role. Besides, ISO/IEC 19086-4 concentrates on data protection measures that are suitable for being translated into SLOs and SQOs, i.e. into objectives that must be achieved	

					mentioned on the paragraph. -ISO/IEC 19086-4 does not define any conformance requirements as 19086-3 does. In 19086-4 are defined "Implementation guidances", but not conformance requirements.	by the CSP. Other data protection measures and obligations can be better managed through other instruments, such as adherence to a code of conduct, certification against an approved standard and the relevant contract and/or service agreement and applicable law."	
	17 – 19	10.6.1		Te	As in the case of the PII content area, also the current description of the Information Security content area introduces ambiguities. The current text: "The cloud SLA shall include relevant information on the SLOs and SQOs that relate to Information Security for cloud services. For details, refer to ISO/IEC 19086-4 for SLOs and SQOs relating to the Information Security component" Introduces ambiguities like the following: -The notion of "relevant information" is not clear, because what is relevant for a CSC may not be for another CSC. Well adopted/standardized processes (e.g., risk management), usually help to define the relevant information to include. -As previously mentioned, ISO/IEC 19086-4 documents implementation guidances, not core requirements as 19086-3.	The proposal is to define "core requirements" related to security and privacy in ISO/IEC 19086-4. In that case the proposed text to include in 19086-3 would be: "Core requirements related to the Information Security content area are defined in ISO/IEC 19086-4, which focuses on the definition of SLOs and SQOs for security and privacy."	
	24 – 25	10.7.1		Ed	The following phrase: "For each of the termination of service SLOs or SQOs chosen, the SLO or SQO shall conform to the requirements listed below for the SLO or SQO." Needs proof reading.	Please rephrase as: "Each one of the chosen termination of service component's SLOs or SQOs shall conform to the corresponding requirements listed below."	
	33 - 34	10.7.1		Te	The following "Notification of Service Termination" statement: "A termination of service SQO shall document the process for notifying a CSC that their cloud service agreement is being terminated including the	Please rephrase as: "Termination of service shall document if the CSP is entitled to terminate the cloud service, the circumstances under which this is possible, and the process for notifying a	

					notification period." Does not take into account two important factor namely (i) if the CSP is entitled to terminate the service, and (ii) under which conditions the CSP can terminate the service.	CSC that their cloud service agreement is being terminated including the notification period."	
	2 – 4	10.7.4		Ed	In the following phrase: "A return of assets SQO shall document the responsibilities of the CSP and the CSC in relation to the ownership, use, return and disposal of data objects and the disposal of physical artifacts containing data objects as part of the service termination." the term "data objects" is being used for the first time without being previously introduced.	We recommend substituting the term "data object" for "cloud service customer data", as defined by ISO/IEC 17788 (cf., Clause 3.2.11). The new phrase should read: "A return of assets SQO shall document the responsibilities of the CSP and the CSC in relation to the ownership, use, return and disposal of cloud service customer data and the disposal of physical artifacts containing cloud service customer data as part of the service termination."	
	5 – 13	10.8.1		Te	The "Service Incident Notification" SLO/SQO needs to be further revised in order to make it compliant with the new European NIS Directive (https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive). Among other topics, the NIS directive requires companies in critical sectors – such as energy, transport, banking and health – as well as key Internet services to adopt risk management practices and report major incidents to the national authorities.	To be further discussed.	
	30 – 31	10.9.1		Te	The following description: "An audit schedule SQO shall document the schedule of audits the CSP undertakes using its own or third party resources."	Please rephrase as: "An audit schedule SQO shall document, for each target of audit, the schedule of audits the CSP undertakes using its own or	

					does not refer to the actual target of the audit.	third party resources."	
	34 – 35	10.10.1		Te	The phrase: "A changes to the cloud service features and functionality content area shall specify one or more SLOs or SQOs for changes to the cloud service features and functionality (see ISO/IEC 19086-1 for SLOs or SQOs)." Does not specify who is entitled to make changes on the cloud service, because those changes may imply (i) changing the SLA, and (ii) negative effects to the CSC.	Please change to: "The changes to the cloud service features and functionality content area shall specify the cloud actor entitled to perform the changes, the consequences and alternatives for the CSC derived from such changes, and one or more related SLOs or SQOs (see ISO/IEC 19086-1)."	
	2 - 3	10.11.3		Te	The phrase: "The customer data backup and restore component shall specify one or more SLOs or SQOs for customer data backup and restore (see ISO/IEC 19086-1 for SLOs or SQOs)." Does not specify the actual target CSC data of the backup.	Please change to: "The customer data backup and restore component shall specify the CSC data to be backed up, and one or more SLOs or SQOs for customer data backup and restore (see ISO/IEC 19086-1 for SLOs or SQOs)."	
	17	10.12.1		Te	The phrase: "IPR shall include a statement of any IPRs the CSP claims on the cloud service customer data." Is ambiguous, because it does not put any constrain on the CSC data (or even cloud service derived data) over which the CSP can claim any IPRs. Our main concern refers to PII, over which the CSP should never claim any IPRs.	To be discussed.	
	10 - 11	10.12.5		Te	The phrase: "Derived data shall define the types of derived data the CSP creates as a result of interaction with the cloud service by the CSC"	To be discussed. The statement should describe what derived data is created by the cloud service provider from cloud service customer data, the intended uses for the derived data and what rights the cloud	

					is ambiguous with respect to the actual ownership and intended uses of the data derived from CSC data.	service customer has to inspect the derived data. Please refer to European Commission's SLA Standardisation Guidelines (https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines)	

Annex 1. Proposed Security SLO/SQO.

7. Security Components

7.1. Security Policy Component

7.2. Organization of Information Security Component

7.3. Human Resources Security Component

7.3.3. Service level objectives

7.3.2.1. Percentage of authorized personnel that received training on the information system

This SLO describes the percentage of authorized personnel that has received relevant training on the Information System in order to ensure that is capable of configuring, installing, and operating the information system, and an effective use of the system's security features.

7.3.2.2. Cloud service provider personnel data access level

This SLO describes the confidentiality level of the resource with respect to the personnel operating the CSP.

7.3.2.3. Guidance

The human resources security component shall specify the percentage of authorized personnel that has received relevant training on the Information System. Also, this component shall provide an specification of the personnel data access level where the confidentiality level of the resource should be equal or less than that of the personnel operating the CSP.

7.4. Asset Management

7.5. Access Control Components

7.3.2. Service Level Objectives

7.5.2.1. User authentication and identity assurance level

This SLO measures the Level of Assurance (LoA) of the mechanism used to authenticate a user accessing a resource.

7.5.2.2. Guidance

The LoA shall we based on relevant standards like NIST SP 800-63 (Electronic Authentication Guidelines), ISO/IEC 29115 (Entity Authentication Assurance Framework) or the Kantara Initiative's Identity Assurance Framework (IAF).

7.3.3. Service Qualitative Objectives

7.1.3.9. Existence of User Access Storage Protection

This SQO describes the mechanisms used to protect cloud service user access credentials.

7.3.3.10. Guidance

The Existence of User Access Storage Protection shall provide an statement listing the mechanisms used to protect cloud service user access credentials.

7.6. Cryptography

7.3.3. Service level objectives

7.6.2.1. Cryptographic Brute Force Resistance

This service commitment expresses the strength of a cryptographic protection applied to a resource based on its key length. Instead of using key lengths alone, which are not always directly comparable from one algorithm to another, this normalizing scale allows comparison of the strengths of different types of cryptographic algorithms.

7.6.2.2. Key Exposure Level

Indication of the level of confidentiality afforded to cryptographic secrets, from a cloud client point of view.

7.6.2.3. Cryptographic hardware module protection level

This service commitment expresses the level of protection that is afforded to cryptographic operations in the cloud service through the use of cryptographic hardware modules.

7.6.2.4. Guidance

The Cryptographic Brute Force Resistance SLO shall be based on relevant standards or recommendations, for example using the ECRYPT II security level recommendations or the FIPS security levels for encryption.

The Key Exposure Level should specify any of the following values:

- Level 0 – Access to decrypted data or cryptographic secrets by the CSP is necessary to provide some functionalities of the service.
- Level 1 – Access to decrypted data or cryptographic secrets is available to specific personnel of the CSP, for administrative or debugging purposes only.
- Level 2 – Access to decrypted data or cryptographic secrets is available to specific personnel of the CSP, for administrative or debugging purposes only. It is governed by the principle of dual control and split knowledge.

- Level 3 – Access to decrypted data or cryptographic secrets is available to specific personnel of the CSP in exceptional circumstances only. It is governed by the principle of dual control and split knowledge, under the supervision of a hardware security module.
- Level 4 – Cryptographic secrets needed to decrypt the data are known to the cloud client only.

The Cryptographic hardware module protection level shall be specified in terms of the Cryptographic Brute Force Resistance SLO.

Note to entry 1: For the ECRYPT II recommendations please refer to Smart N. (ed.). "ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011)". Katholieke Universiteit Leuven (KUL). Deliverable SPA-17. June, 2011.

Note to entry 2: For the FIPS security levels please refer to "FIBS PUB 140-2: Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules". May, 2001.

7.7. Physical and Environmental Security Component

7.3.3. Service level objectives

7.7.2.1. Data deletion quality level

This service commitment measures the quality of data deletion.

7.7.2.2. Data isolation Testing Level

Indication of the level of testing that has been done by the cloud service provider to assess how well data isolation is implemented. The resources in the scope of the measurement need to be well defined (storage, CPU, network, memory, database, etc.), and a standard set of tools or procedures need to be defined to establish the tests that should be conducted to assess each level.

7.7.2.3. Guidance

The data deletion quality level shall range from 'weak' deletion where only the reference to the data is removed, to 'strong' deletion where data is overwritten / destroyed.

The data isolation testing levels shall specify any of the following:

- Level 0 – No data isolation testing has been performed.
- Level 1 – Read/write isolation has been tested.
- Level 2 – Secure deletion has been tested, in addition to read/write isolation.

- Level 3 – Absence of known side channel attacks has been tested, in addition to read/write and secure deletion.

7.8. Operations Security Component

7.9. Communications Security Component

7.10. Systems Acquisition, Development and Maintenance Component

7.11. Supplier Relationships Component

7.12. Information Security Incident Management Component

7.3.3. Service level objectives

7.12.2.1. Percentage of timely incident reports

This service commitment describes the defined incidents to the cloud service which are reported to the customer in a timely fashion.

7.12.2.2. Percentage of timely incident responses

This service commitment describes the defined incidents that are assessed and acknowledged by the cloud service provider in a timely fashion.

7.12.2.3. Incident notification level

Description of the level of the notification procedures after a privacy incident or breach.

7.3.4. Guidance

The Percentage of timely incident reports shall be represented as a percentage by the number of defined incidents reported within a predefined time limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month, week, year, etc).

The Percentage of timely incident responses shall be represented as a percentage by the number of defined incidents assessed and acknowledged by the cloud service provider within a predefined time limit after discovery, over the total number of defined incidents to the cloud service within a predefined period. (i.e. month, week, year, etc).

The incident notification level shall have any of the following possible levels:

- Level 0 – No notification of privacy incidents is done, or it is done inconsistently.
- Level 1 – General notification, usually as a public notice. Affected users may not be aware of the incident.
- Level 2 – Individual notification to each affected user.
- Level 3 – Automated and self-service procedures for data subject access are in place, including the case of denied access.

7.13. Business Continuity Management Component

7.3.3. Service level objectives

7.13.2.1. Number of Business Continuity Resilience (BCR) plans tested

Number of business continuity resilience and incident response plans that have been tested in a given interval of time.

7.13.2.2. Maximum tolerable period for disruption (MTPD)

Duration of the maximum tolerable period for disruption, expressed in a given time unit (e.g. minutes), as defined by the organizations' BCR plans.

7.13.2.3. Level of Redundancy

This service commitment describes the level of redundancy of the cloud service supply chain. Redundancy varies also on the type of cloud service provided (IaaS versus SaaS for example)).

7.13.2.4. Percentage of tested storage retrievability

This service commitment describes the percentage of data stored in the resource that has been verified to be retrievable during the measurement period.

7.13.2.5. Recovery point

This service commitment describes the recovery point objective (RPO) or recovery point actual (RPA) of the resource. The RPA represents the data freshness of a backup – i.e. the time elapsed since data was stored for the purpose of eventually restoring the system in a stable state, for example in a backup.

7.13.2.6. Recovery time

This service commitment describes the recovery time of the resource: this is the time that is needed after a failure to restore the system to a stable state.

7.13.2.7. Percentage of recovery success

This service commitment describes the percentage of successful backup restorations performed and verified to be correct (by a checksum, a format check, etc.).

7.3.4. Guidance

The MTPD shall be consistent with the CSP's business continuity resilience plans. The level of redundancy shall take into account the percentage of the components or service that have fail over mechanism. There are not compliance requirements on the rest of defined SLOs.

7.14. Compliance Component

Annex 2. Proposed PII SLO/SQO.

8. Security and Protection of Personally Identifiable Information Components

8.1. Consent and choice Component

8.1.2. Service Level Objectives

8.1.2.1. Type of Consent Level

The level associated to the type of consent obtained for collecting, using and sharing private data.

8.1.2.2. Guidance

The type of consent shall be ranked in levels according to the following scale:

- Level 0 – No Consent: Consent is not obtained at or before collection of private data.
- Level 1 – Implied Consent: The consent is infered from the behaviour of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered.
- Level 2 – Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered.
- Level 3 – Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data.

8.2. Purpose legitimacy and specification

8.2.2. Service qualitative objectives

8.2.2.1. Processing purposes

A list of processing purposes (if any) which are beyond those requested by the customer acting as a controller.

8.2.2.2. Guidance

The CSP shall provide a list related to the processing purposes beyond those requested by the customer acting as a controller. It is possible that there are not processing purposes which are beyond those requested by the customer acting as a controller, in which case it should be specified by the CSP. Furthermore the CSP shall specify if the cloud service customer can itself be a cloud service processor.

8.3. Collection limitation

7.3.3. Service level objectives

8.3.2.1. Percentage of Record of Data Collection, Creation and Update

Percentage of the extent to which a date is recorded when collecting, creating and updating private records.

8.3.2.2. Guidance

The CSP shall specify in “Percentage of Record of Data Collection, Creation and Update” a date of data collection, creation and update to the extend it is relevant for complying with data retention schedules.

8.4. Data minimization Component

8.5. Use, retention and disclosure limitation Component

7.3.3. Service level objectives

8.5.2.1. Maximum cloud service customer data retention period

The maximum period of time that cloud service customer data is retained before destruction by the cloud service provider and after acknowledgment of a request to delete the data or termination of the contract.

8.5.2.2. Guidance

The CSP shall define its “Maximum cloud service customer data retention period” in alignment with regulations and directives applicable to the cloud service customer.

8.6. Accuracy and quality Component

7.3.2. Service level objective

8.6.2.1. Percentage of PII Classified

Percentage of the extent to which PII is identified and classified according to its sensitivity and risk.

8.6.2.2. Guidance

PII identification and classification shall take into account relevant privacy impact assessment standards like ISO/IEC 29134.

8.7. Openness, transparency and notice Component

8.8. Individual participation and Access Component

8.8.2. Service qualitative objectives

8.8.2.1. Procedures for Data Subject Access Requests

Existence of procedures for guaranteeing data subjects’ access to their personal information.

8.8.2.2. Mean Time for Responding Data Subject Access Requests

Mean time for responding to data subject access requests.

8.8.2.3. Mean Time to Respond to Complaints

Average time that the organization takes for responding to complaints from stakeholders.

8.8.2.4. Guidance

The CSP shall specify the existence of procedures for data subject access requests based on the following scale:

- Level 0 - No procedures are established for permitting data subject access to their personal information.
- Level 1 - Procedures for data subject access exist but are not documented or consistent.
- Level 2 - Documented and consistent processes for data subject access are established. Employees responsible of such procedures are identified and trained on how to respond to requests. There also exist procedures for handling with denial of access.
- Level 3 - Automated and self-service procedures for data subject access are in place, including the case of denied access.

There are no compliance requirements associated to the other defined SLOs.

8.9. Accountability Component

8.9.2. Service level objectives

8.9.2.1. Periodicity of Privacy Impact Assessments

Periodicity of Privacy Impact Assessments for Information Systems.

8.9.2.2. Guidance

The CSP shall provide the frequency of privacy impact assessments being performed based on standards like ISO/IEC 29134.

8.10. Information security Component

8.11. Privacy compliance Component

8.11.2. Service qualitative objectives

8.11.2.1. Applicable data protection codes of conduct, standards, certifications

Lists the data protection codes of conduct, standards and certification mechanisms that the service complies with.

8.11.2.2. Data geolocation selection

Specifies whether cloud service customer can choose a given geographical location for the storage of the cloud service customer data.

8.11.2.3. Guidance

The CSP's list of applicable data protection codes of conduct, standards and certifications may include the EU Data Protection Code of Conduct for Cloud Service Providers, ISO/IEC 27018, international standards for the processing of personal data in the cloud, etc.

There are no compliance requirements associated to the other defined SQOs.

8.11.3. Service level objectives

8.11.3.1. Frequency of employees' certifications

Describes how often employees certify their acceptance of responsibilities for activities that involve handling of private data, for a given period of time.

8.11.3.2. Guidance

There are no compliance requirements associated to defined SLOs.

APPENDIX 1.

Type of PII Consent example SLO using tables

General

The following is an example of a qualitative privacy metric describing the type of consent obtained for collecting, using and sharing PII data (based on ISO/IEC WD 19086-4, NIST 800-53v4, and GAPP). The type of PII consent can be ranked in levels according to its preference.

Example Availability SQO

Guarantee

The cloud service customer (i.e., data subject) must provide unambiguous consent to the CSP for collecting or using his PII data. Such consent to be expressed by a statement or by a clear affirmative action. If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SQO text

The PII consent is defined by the CSP in a qualitative manner, so that data subjects can provide their consent based on any of the following levels:

- Level 0 – No Consent: Consent is not obtained at or before collection of PII data.
- Level 1 – Implied Consent: The consent is inferred from the behavior of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered.
- Level 2 – Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered.
- Level 3 – Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data.

This gives enough information to build a metric for PII Consent. In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of PII Consent Example using tables

A cloud SQO consists of a description of the characteristic being committed to, the qualitative value for the SQO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (TypePIIConsent, TC_001)	
scale	ORDINAL
Unit	--
note	The type of consent obtained for collecting, using and sharing private data is ranked in levels.
Expression	TCE_001
Parameters	--
rules	--
underlyingMetrics	TL_001_L0, TL_001_L1, TL_001_L2, TL_001_L3
extend	--

Expression (TCE_001)	
expression	TC_001 is equal to the value of either TL_001_L0, TL_001_L1, TL_001_L2, or TL_001_L3, depending on the fulfilment of their respective rules (namely, TL_001_R0, TL_001_R1, TL_001_R2, and TL_001_R3)
expressionLanguage	ENGLISH
note	--

Metric (TypeOfConsent_Level0, TL_001_L0)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R0
underlyingMetrics	--
expression	0
expressionLanguage	ISO80000

Rule (TL_001_R0)	
rule	No Consent: Consent is not obtained at or before collection of private data
ruleLanguage	English

Metric (TypeOfConsent_Level1, TL_001_L1)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R1
underlyingMetrics	--
expression	1
expressionLanguage	ISO80000

Rule (TL_001_R1)	
rule	Implied Consent: The consent is inferred from the behaviour of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered
ruleLanguage	English

Metric (TypeOfConsent_Level2, TL_001_L2)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R2
underlyingMetrics	--
expression	2
expressionLanguage	ISO80000

Rule (TL_001_R2)	
Rule	Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered.

ruleLanguage	English

Metric (TypeOfConsent_Level3, TL_001_L3)	
scale	ORDINAL
unit	--
note	--
parameters	--
rules	TL_001_R3
underlyingMetrics	--
expression	3
expressionLanguage	ISO80000

Rule (TL_001_R3)	
Rule	Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data
ruleLanguage	English

SQO Metric PII Consent Example expressed in XML

The following code represents the PII Consent example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>

<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"

 xmlns:myns="http://custom"

 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd

  http://custom custom.xsd">


 <Metric id="TC_001" description="TypeOfConsent" scale="ORDINAL" note="The type of consent obtained for collecting, using and sharing private data is ranked in levels">

  <Expression  expression="TC_001 is equal to the value of either TL_001_L0, TL_001_L1, TL_001_L2, or TL_001_L3, depending on the fulfillment of their respective rules (namely, TL_001_R0, TL_001_R1, TL_001_R2, and TL_001_R3) " expressionLanguage="English"/>

  <UnderlyingMetricRef refid="TL_001_L0"/>

  <UnderlyingMetricRef refid="TL_001_L1"/>

  <UnderlyingMetricRef refid="TL_001_L2"/>

  <UnderlyingMetricRef refid="TL_001_L3"/>
```

```
</Metric>
<Metric id="TL_001_L0" description="TypeOfConsent_Level0" scale="ORDINAL">
<Expression expression="0" expressionLanguage="ISO80000"/>
<Rule id="TL_001_R0" ruleLanguage="English" xml:lang="en"
ruleDefinition="No Consent: Consent is not obtained at or before collection of private data"/>
</Metric>
<Metric id="TL_001_L1" description="TypeOfConsent_Level1" scale="ORDINAL">
<Expression expression="1" expressionLanguage="ISO80000"/>
<Rule id="TL_001_R1" ruleLanguage="English" xml:lang="en"
ruleDefinition="Implied Consent: The consent is infered from the behaviour of the data subject, or even from failing to explicitly object. No opt-out or opt-in mechanisms are offered"/>
</Metric>
<Metric id="TL_001_L2" description="TypeOfConsent_Level2" scale="ORDINAL">
<Expression expression="2" expressionLanguage="ISO80000"/>
<Rule id="TL_001_R2" ruleLanguage="English" xml:lang="en"
ruleDefinition="Opt-out Consent: Data subjects can take measures for prevent the collection of private data, but no opt-in mechanisms are offered."/>
</Metric>
<Metric id="TL_001_L3" description="TypeOfConsent_Level3" scale="ORDINAL">
<Expression expression="3" expressionLanguage="ISO80000"/>
<Rule id="TL_001_R3" ruleLanguage="English" xml:lang="en"
ruleDefinition="Opt-in Consent: Data subjects explicitly grant permission for collecting or using private data"/>
</Metric>
</Metrics>
```

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SQO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SQO Evaluation (id)	
slo_id	SQO_TC_001
metric_id	TC_001
slo_value	3
measurementResult_value	3
uncertainty	Third Party Audit-based

measurementTime	May 25th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Level of redundancy (LoR)

General

In the following, a metric describing the level of redundancy required for a given system component (e.g., a web server) is described. The level of redundancy is expressed as a numeric integer value and can be calculated in different ways.

Example of SLO

Guarantee

The CSP must ensure that, at any time during system operation, at least N replicas of the component are up and running, with N defined by the cloud service customer (CSC). If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SLO text

The level of redundancy is defined as an integer >= 1.

In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of LoR Example using tables

A cloud SLO consists of a description of the characteristic being committed to, the quantitative value for the SLO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (LevelOfRedundancy_p, LOR_001)	
scale	RATIO
Unit	--
note	The level of redundancy is an integer number and can be measured by counting the number of active replicas of the component (NOR)
Expression	LOR_001_Exp
Parameters	LOR_001_P001
rules	LOR_001_R001
underlyingMetrics	--
extend	--

Expression (LOR_001_Exp)	
expression	LOR_001 = NOR
expressionLanguage	ISO80000
note	NOR is obtained via the strategy defined by rule LOR_001_R001

Parameter (LOR_001_P001)	
parameterDefinition	ping interval
unit	seconds

Rule (LOR_001_R001)	
rule	The number of active component replicas (NOR) is checked by pinging them every LOR_001_P001 seconds
ruleLanguage	English

Metric (LevelOfRedundancy_hb, LOR_002)	
scale	RATIO
Unit	--
note	The level of redundancy is an integer number and can be measured by counting the number of active replicas of the component (NOR)
Expression	LOR_002_Exp
Parameters	LOR_002_P001
rules	LOR_002_R001
underlyingMetrics	--
extend	--

Expression (LOR_002_Exp)	
expression	LOR_002 = NOR
expressionLanguage	ISO80000
note	NOR is obtained via the strategy defined by rule LOR_002_R001

Parameter (LOR_002_P001)	
parameterDefinition	Heartbeat interval
unit	seconds

Rule (LOR_002_R001)	
rule	The number of active web server replicas (NOR) is checked by means of heartbeats generated by replicas every LOR_002_P001 seconds
ruleLanguage	English

SLO Metric LoR Example expressed in XML

The following code represents the LoR example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>
<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"
 xmlns:myns="http://custom"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd
  http://custom custom.xsd">
<Metric id="LOR_001" description="LevelOfRedundancy_p"
  scale="RATIO" unit="n/a">
        <Expression expression="LOR_001 = NOR" expressionLanguage="ISO80000"/>
        <Rule id="LOR_001_R001" ruleLanguage="English" xml:lang="en"
  ruleDefinition="The number of active component replicas (NOR) is checked by pinging them every LOR_001_P001 seconds" />
        <Parameter id="LOR_001_P001" parameterDefinition="ping interval" unit="seconds"/>
</Metric>
<Metric id="LOR_002" description="LevelOfRedundancy_hb"
  scale="RATIO" unit="n/a">
        <Expression expression="LOR_002 = NOR" expressionLanguage="ISO80000"/>
        <Rule id="LOR_002_R001" ruleLanguage="English" xml:lang="en"
  ruleDefinition="The number of active web server replicas (NOR) is checked by means of heartbeats generated by replicas every LOR_002_P001 seconds" />
        <Parameter id="LOR_002_P001" parameterDefinition="heartbeat interval" unit="seconds"/>
</Metric>
</Metrics>
```

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SLO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SLO Evaluation (id)	
slo_id	SQO_LOR_001
metric_id	LOR_001
slo_value	3
measurementResult_value	3
uncertainty	Third Party Audit-based
measurementTime	May 27th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Scan frequency (SF)

General

In the following, a metric describing the frequency of execution of scanning activities (e.g., to detect vulnerabilities) is described. The scanning frequency is expressed as a numeric integer value representing the number of seconds elapsed between two subsequent scans.

Example SLO

Guarantee

The CSP must ensure that a scan is executed every N seconds, where N is defined by the cloud service customer (CSC). If the CSP fails to meet this guarantee, then the CSC will be eligible to receive a credit to his account.

Analysis of SQO text

The scanning frequency is defined by the CSP as an integer>=1.

In the following sections the metric will be described using the metric template tables from Annex 2 and using XML based on the model.

Description of SF Example using tables

A cloud SLO consists of a description of the characteristic being committed to, the quantitative value for the SLO (the value the service provider has committed to), and a metric used to understand the meaning of that value. The metric is also used to make measurements of the characteristic.

Metric (ScanFrequency, SF)	
scale	RATIO
Unit	--

note	--
Expression	SF_Exp
Parameters	SF_P001
rules	SF_R001
underlyingMetrics	SR_AGE
extend	--

Expression (SF_Exp)	
expression	SF = 1/SR_AGE
expressionLanguage	ISO80000
note	

Parameter (SF_P001)	
parameterDefinition	scan interval
unit	seconds

Rule (SF_R001)	
rule	The scan starts as soon as the software is deployed and is performed every SF_P001 seconds.
ruleLanguage	English

Metric (ScanningReportAge, SR_AGE)	
scale	RATIO
Unit	millisec
note	--
Expression	SR_AGE_Exp
Parameters	SR_AGE_P001
rules	--
underlyingMetrics	--
extend	--

Expression (SR_AGE_Exp)	
expression	SR_AGE = NOW - SR_AGE_P001
expressionLanguage	ISO80000

note	

Parameter (SR_AGE _P001)	
parameterDefinition	report generation timestamp
unit	millisec

Parameter (NOW)	
parameterDefinition	current time
unit	millisec

SLO Metric SF Example expressed in XML

The following code represents the PII Consent example described using XML notation instead of tables to represent the metric.

```
<?xml version="1.0" encoding="UTF-8"?>
<Metrics xmlns="http://www.iso.org/schemas/19086/metrics/v1.0.0"
 xmlns:myns="http://custom"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.iso.org/schemas/19086/metrics/v1.0.0 Metrics.xsd
  http://custom custom.xsd">

<!-- scanning frequency: obtained by calculating the time elapsed since the generation of the last report -->
 <Metric id="SF" description="ScanFrequency" scale="RATIO" unit="n/a">

  <!-- this metric uses SR_AGE for its expression -->
  <UnderlyingMetricRef refid="SR_AGE"/>
  <Expression expression="SF=1/SR_AGE" expressionLanguage="ISO80000"/>
  <Rule id="SF_R001" ruleLanguage="English" xml:lang="en"
   ruleDefinition="The scan starts as soon as the software is deployed and is performed every SF_P001 seconds." />
  <Parameter id="SF_P001" parameterDefinition="scan interval" unit="seconds"/>
</Metric>
 <!-- scanning report age -->
<Metric id="SR_AGE" description="ScanningReportAge" scale="RATIO" unit="millisec">
  <Expression expression="SR_AGE = NOW - SR_AGE_P001" expressionLanguage="ISO80000"/>
  <Parameter id="SR_AGE_P001" parameterDefinition="report generation timestamp" unit="millisec"/>
  <Parameter id="NOW" parameterDefinition="current time" unit="millisec"/>
 </Metric>
```

</Metrics>

Service monitoring

Once a service agreement has been reached between the CSC and the CSP containing the SLO referenced in Section 0, it is possible to evaluate the fulfilment of the agreed qualitative level e.g., by assessing the CSP's privacy policy and practices

SLO Evaluation (id)	
slo_id	SQO_SF
metric_id	SF
slo_value	30
measurementResult_value	30
uncertainty	Third Party Audit-based
measurementTime	May 27th, 2016 9:00pm edt
comparison_result (true/false)	TRUE

In the above example, the SLO commitment was met during this billing period.

Annex 3 – Contributions to EU Catalogue of Standards

See section 5.4 for an overview.

PLAN FOR VALIDATING CONTENT OF THE CATALOGUE

Schedule for validating content

- ***June – August:*** Draft content by contractor
- ***23 September:*** Presentation to Member States
- ***Oct-Nov:*** Validation by MS (written procedure)
- ***December:*** Publication on web of draft content + survey to experts
- ***January 2017:*** Expert Workshop

Possible participants for the expert workshop

- **EC:** DG CONNECT.C1 & E2 / DG DIGIT.C1
- **MS:** Restricted MSP
- **Standard experts:** ETSI / Commission High Level Expert Group European Open Science Cloud (E03353) / Cloud Select Industry Group / ECMA /
- **Europe organisations:** EuroCloud / Open Forum Europe
- **Industry bodies:** Cloud Security Alliance / EuroISPA /
- **Interoperability bodies:** Digital Interoperability Forum / European Committee for Interoperable Systems
- **Vendors and technology providers:** Digital Europe
- Other: OpenStack Foundation / Open Grid Forum / Cloud Watch 2 /

Dissemination

- *Targeted emails to communities (save the date/ draft content published/invitation/workshop report/..)*
- *Survey on the draft content (before the workshop)*
- *News/Update of the Web*
- *EC networks (MSP, CPB=central procurement body, ..)*

POSSIBLE CONTENT (for discussion)

Possible content

1. Introduction

1.a Policy

1.b Procurement needs (Use cases)

1.c Costs & Benefits

1.d Situation in MS

2. Standards

2.a Introduction

2.b Use Cases

2.c Standards by use case

3. Guidelines

3.a Vendor lock-in

3.b Interoperability & Implementation

3.c Costs

3.d Procurement

4. Horizontal Matters

4.a Strategic Procurement (Green, Social, Innovative)

4.b Security & Privacy

1. Introduction

1.a Policy

Maximising the growth potential of the European Digital Economy requires investment in ICT infrastructures and technologies such as Cloud Computing to boost industrial competiveness as well as provide better public services. In simply terms, Cloud computing is the storing, processing and use of data stored on remotely located computers accessed over the internet. Users can draw upon almost unlimited computing power and access their data from any internet connection, while reducing capital investment needs.

Cloud Computing is increasingly the chosen platform for the provision of new ICT infrastructure, services, software and applications. By using the cloud, small firms can reach out to large markets, while governments can make their services more attractive and efficient while reining in spending.

However, to maximise uptake within the developing Cloud environment, businesses require a level of surety over the services that will be provided by their Cloud Service Provider. This confidence can only be achieved by clear and transparent Cloud-Service/Service-Level Agreements governing the relationship between the Cloud Service Customer and their Cloud Service Providers.

- **LINK to COM(2012)529 *Unleashing the Potential of Cloud Computing in Europe***
- **LINK to COM(2015)192 *A Digital Single Market Strategy for Europe***
- **LINK to main website of EC**

1. Introduction

1.b Procurement needs (1 of 2)

The Cloud market represents a relatively new, yet rapidly developing, market sector that combines IT functionality (e.g. computing, storage and data management) with wide-area networking, delivered as a set of services. Although this market is still at an early stage in terms of both adoption and standardisation, due to its rapid expansion there are many services already available for procurement by governments covering: Software as a Service (Saas); Platform as a Service (Paas); and Infrastructure as a Service (IaaS).

Within this market, the instrument used to governing the relationship between the end user (the Cloud Service Customer) and the service provider (the Cloud Service Provider) is the contract entered into between these two parties, referred to as Cloud Service Level Agreement (CSLA). Given the global nature of Cloud offerings, CSLAs usually span many jurisdictions which often have their own applicable legal requirements, in particular with respect to the protection of the personal data hosted in a Cloud service. These agreements differ according to the each Cloud Service Provider, such that while they may contain similar functionality features, the individual terms and conditions applying to each provider's services may be both complex and expressed in a manner unique to the Service Provider.

1. Introduction

1.b Procurement needs (2 of 2)

This puts the onus on potential customers to carefully analyse what is being offered, however, it also makes the task of comparing and selecting the best service option difficult. Since the adoption of cloud services has potentially significant implications for operational and governance-related risk, lack of clarity on the details of the available service offers represents a barrier, particularly for applications with a long-term business importance to a user (as opposed to specific projects of limited scope and duration).

Care needs to be taken when drafting and/or agreeing to CSLA. Any ambiguity of language within the agreements can result in future (legal) disputes between both parties.

There is a need to define the role of the CSLA in the business relationships between the various Cloud service stakeholders. Specifically, it is important to understand how both the Cloud Service Customer and the Cloud Service Provider can use their SLA to provide the context for their individual decisions and operations moving forward.

1. Introduction

1.c Costs & Benefits

Cost savings from cloud adoption: Research has indicated that 27% of businesses identify cost savings from adopting cloud. Of these: 59% saw savings of between 5% and 19% of total IT costs; 26% saw savings of 30% or more; and 15% saw savings of 4% or less or could not quantify the savings.

This study presents some predicted net costs and benefits associated with Cloud Computing across Europe, as well as the impact of barriers to cloud take-up, such as restrictive and/or ambiguous Cloud Service Level Agreements

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742

For more general information see:

http://www.cloudwatchhub.eu/taxonomy/term/92

1. Introduction

1.d Situation in Member States

Eurostat has produced country-specific statistics on the use of cloud computing by enterprises across Europe.

http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Further_Eurostat_information

The following study provides information on uptake based on a number of country case-studies.

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742

2. Standards

2.a Introduction

Regulatory context:

Guide to application of standards:

Overall List of existing standards (CEN and ETSI):

http://www.etsi.org/deliver/etsi_sr%5C003300_003399%5C003391%5C02.01.01_60%5Csr_003391v020101p.pdf

http://www.sla-ready.eu/

2. Standards

Standards / guidance specific for UC

2.b Use Cases

Important points for procurers applying to all European Catalogue use cases:

- *The use cases provided here represent generic use cases. You may need to modify these to meet the specific procurement needs of your organisation.*
- *All standards listed with the individual use cases can be substituted with any reasonable equivalents alternatives unless this action is prevented by any applicable EU or national legislation.*
- *Simply listing these standards within your tender documents will not ensure the interoperability of any acquired solution/service, nor will the interoperability of your solution and your existing systems be guaranteed. You will still need to conduct your own internal technical assessment before publishing your tender – the European Catalogue is not a substitute for this process.*

2. Standards

2.b Use cases

Use Case 1: *The Cloud Service Customer needs to procure software as a service (SaaS) for use by its employees to replace software currently installed on computers.*

Use Case 2: *The Cloud Service Customer needs to (be able to) create a hybrid innovation platform whereby they share specific resources with their Cloud Service Provider.*

Use Case 3: *The Cloud Service Customer needs to (be able to) monitor the delivery of services by their Cloud Service Provider to ensure they are delivering these services at the agreed levels.*

Use Case 4: *The Cloud Service Customer needs to (be able to) ensure they can retrieve all data that is handled by their Cloud Service Provider when the service is terminated, regardless of why this service is terminated.*

2.c Standards by use case

Use Case 1: *The Cloud Service Customer needs to procure software as a service (SaaS) for use by its employees to replace software currently installed on computers.*

ISO/IEC 27005 (Risk Management)

ISO/IEC 19086 Part 1 (Overview and Concepts), ISO/IEC 19086 Part 3 (Core Requirements) and ISO/IEC 19086 Part 4 (Security and Privacy) – all in draft at the moment of writing this report

TMF GB963 (Cloud SLA Application Note)

Relevant guides to the application of these standards:

EU H2020 PICSE project "Case studies and best practices" http://picse.eu/case-studies

EU H2020 SLA-Ready project CSLA Common Reference Model: http://www.sla-ready.eu/


European Commission
2. Standards
Standards / guidance specific for UC
2.c Standards by use case
Use Case 2: The Cloud Service Customer needs to (be able to) create a hybrid innovation platform whereby they share specific resources with their Cloud Service Provider.
ISO/IEC 27005 (Risk Management)
ISO/IEC 29134 (Privacy Impact Assessment)
ISO/IEC 19086 Part 1 (Overview and Concepts), ISO/IEC 19086 Part 2 (Metric Model), ISO/IEC 19086 Part 3 (Core Requirements) and ISO/IEC 19086 Part 4 (Security and Privacy) – all in draft at the moment of writing this report
ETSI TR 103 125 "SLAs for Cloud services "
Relevant guides to the application of these standards:
EU H2020 SLA-Ready project CSLA Common Reference Model: http://www.sla-ready.eu/
C-SIG SLA "Cloud SLA Standardisation Guidelines"
EC SMART "Standards terms and performance criteria in service level agreements for Cloud computing services"


European Commission
2. Standards
Standards / guidance specific for UC
2.c Standards by use case
Use Case 3: The Cloud Service Customer needs to (be able to) monitor the delivery of services by their Cloud Service Provider to ensure they are delivering these services at the agreed levels.
ISO/IEC 27004 (Information security monitoring, measurement, analysis and evaluation)
ISO/IEC 19086 Part 1 (Overview and Concepts), ISO/IEC 19086 Part 2 (Metric Model), ISO/IEC 19086 Part 3 (Core Requirements) and ISO/IEC 19086 Part 4 (Security and Privacy) – all in draft at the moment of writing this report
ETSI TR 103 125 "SLAs for Cloud services "
Relevant guides to the application of these standards:
EU H2020 SLA-Ready project CSLA Common Reference Model: http://www.sla-ready.eu/
C-SIG SLA "Cloud SLA Standardisation Guidelines"
ENISA "Procure Secure: A guide to monitoring of security service levels in cloud contracts"
CSA Cloud Trust Protocol https://cloudsecurityalliance.org/group/cloudtrust-protocol/

2. Standards

Standards / guidance specific for UC

2.c Standards by use case

Use Case 4: *The Cloud Service Customer needs to (be able to) ensure they can retrieve all data that is handled by their Cloud Service Provider when the service is terminated, regardless of why this service is terminated.*

ISO/IEC 19086 Part 3 (Core Requirements) and ISO/IEC 19086 Part 4 (Security and Privacy) – both in draft at the moment of writing this report

CSA Privacy Level Agreement v2

Relevant guides to the application of these standards:

EU H2020 SLA-Ready project CSLA Common Reference Model: http://www.sla-ready.eu/
CSCC Practical Guide to Cloud Service Level Agreements – v2"
C-SIG SLA "Cloud SLA Standardisation Guidelines "

3. Guidelines

3.a Vendor lock-in

Within ICT, vendor lock-in is a recognised issue whereby public authorities, who have entered into contracts with providers of ICT product or service for a certain period of time, cannot easily change their provider once the contract ends as essential information is not available to any new suppliers.

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2327

Within Cloud Computing, vendor lock-in is intrinsically linked to the Service Level Agreements (the contracts) between the Cloud Service Customer and the Cloud Service Provider. If the customer is unable to negotiate the terms of their Service Level Agreement, and/or if these terms are not transparent and clearly defined then the customer may be prevented from accessing the full range of suppliers.

Similarly, a customer may be prevented from leaving a Cloud Service Prover (even if that Provider is providing a poor service) due to the drafting of their Service Level Agreement.

3. Guidelines

3.b Interoperability & Implementation

http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/

http://csc.etsi.org/resources/WP1-Report/Special_Report_033381-v2.1.1.pdf

http://www.sla-ready.eu/common-reference-model

http://cloudscout.cloudwatchhub.eu/#/app/home?lang=en&code=en

3. Guidelines

3.c Costs

No specific costs information appropriate here.

3. Guidelines

3.d Procurement

Procurement guidelines for Service Level Agreements have been produced by a number of organisations/initiatives, setting out Service Level Objectives.

PICSE (Procurement Innovation for Cloud Services in Europe) www.picse.eu/

- http://picse.eu/sites/default/files/Annex1_Guidetocloudprocurement_webversion.pdf

Cloud Select Industry Group – Subgroup on Service Level Agreement

- *Cloud Service Level Agreement Standardisation Guidelines*: *http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6138*

ENISA

- *Procure Secure - A guide to monitoring of security service levels in cloud contracts: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport*

4. Horizontal Matters

4.a Strategic Procurement

Regulatory context

To promote green, social and innovative procurement

Examples in MS

The EC has published a study: "Analysis of cloud best practices and pilots for the public sector". The study provides a detailed analysis of cloud initiatives at the national level and deployments in the public sector in ten Member States.

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3521
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3522

Annex 4 – Contribution to CSA SecaaS Continuous Monitoring

The contribution provided is summarised in the following paragraphs.

CMaaS for Consumers

[Guidance for building the business case and contractual elements for procuring a CM as a Service.]

Information for Decision Makers (C-Suite)

Technical ramifications

Operational Ramifications

Legal Ramifications and Privacy issues

SLAs

Decision makers, in their role of prospective cloud service customers (CSC), crucially require mechanisms (and also tools) that can enable them to understand and assess the level of security of the selected CSP, and especially the new challenges in risk assessment/management (e.g., continuous assessment, and risk composition in hybrid cloud) that the cloud entails. In this context, and as also highlighted by the European

Commission's Cloud Computing strategy (ec.europa.eu/digital-agenda/node/10565), the use of contracts and Service Level Agreements (SLAs) become key components driving cloud services. SLAs should facilitate cloud customers in understanding (i) the claims behind the cloud service, and (ii) relate such claims to their own requirements. These reports suggest the use of cloud SLAs to develop better assessments and perform informed customer decisions, and ultimately improve trust and transparency between Cloud stakeholders.

From the SecaaS Continuous Monitoring perspective, SLAs should be considered as an essential ingredient to continuously assess the cloud service's life cycle (i.e., procurement, operation, and termination). However, understanding the SLA terms and conditions (including committed security Service Level Objectives or SLOs) in order to deploy the adequate SecaaS monitoring features mainly requires (i) knowledge and mapping of the organization's security requirements into the Cloud SLA, and (ii) clear understanding of the SLA's

elements/components. In both cases, standards and best practices for SLAs/metrics play an important role (please refer to Section 5).

Furthermore, adequate risk IT management techniques and business guides for SLAs should be considered as a primary need for decision-makers. Risk profiling in the context of Cloud SLAs will be further discussed in Section 3.1.2, whereas a comprehensive suite of cloud SLA good practices for the private sector can be found in the SLA-Ready project10.

Information for Managers

Policies and procedures

What could/should be monitored i. Government

Personnel skills

Making it actionable

What to monitor? From Risk Profiling to cloud security SLAs

Organizations willing to exploit the benefits of SecaaS Continuous Monitoring need to leverage their contractual agreements to hold the CSPs (and Cloud brokers, when applicable) accountable for the implementation of the security controls to be monitored. But what are the elements of a successful Cloud risk profiling strategy in order to enable the usage of SecaaS Continuous Monitoring for Cloud SLAs?

A well-orchestrated process for organizations (in particular SMEs) willing to manage cloud risks by leveraging risk profiles into cloud SLAs can be partially based on the more general Cloud Adapted Risk Management Framework (CRMF) being proposed by NIST11, is a

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

[11] Please refer to "Cloud-adapted Risk Management Framework", Draft NIST SP 800-173, 2014.

cyclically executed process composed of a set of coordinated activities for overseeing and controlling risks. This set of activities consists of the following tasks:

- Risk Profiling/Assessment,
- Risk Treatment, and
- Risk Control.

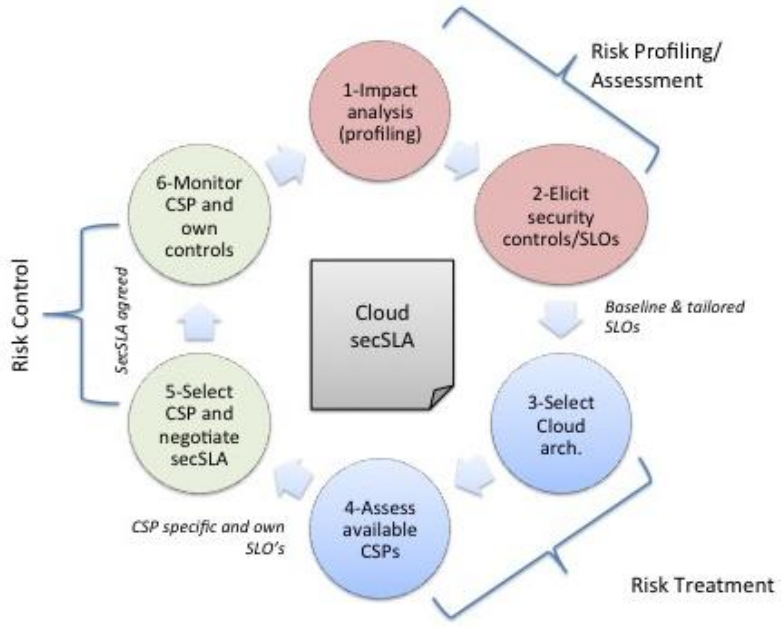

Figure 1. Cloud secSLA development within a risk management framework.

These tasks collectively target SecaaS the continuous monitoring of strategic and tactical security through SLAs. A cloud customer-centric approach for implementing the activities mentioned above is shown in the previous figure and presented next:

- Risk Profiling/Assessment Activities: these activities aim to (i) create the risk profile for the organization, and (ii) select the baseline and tailored supplemental cloud security controls/cloud enterprise architecture components.
- Risk Treatment Activities: once the security controls have been elicited, the following steps take place:
  - Step 3 – Select the Cloud ecosystem architecture (e.g., based on CSA EA12) that best suits the assessment results for the system.
  - Step 4 – Assess the CSP options. Identify the security controls needed for the system the CSP has implemented. Negotiate the implementation of any

[12] Please refer to https://cloudsecurityalliance.org/group/enterprise-architecture/

additional security controls that are identified. Identify any remaining security controls that fall under the organizations's responsibility for their implementation.

- Risk Control Activities: this final stage aims to deploy and continuously monitor the cloud SLA through the SecaaS. The following steps take place:
  - Step 5 – Select and authorize a CSP to host the organization's information system. Draft a (security) SLA that lists the negotiated contractual terms and conditions.
  - Step 6 – Monitor the agreed CSP (security) SLA to ensure that all service levels objectives (SLOs) are being met, and the risk profile is kept under acceptable thresholds (i.e. the cloud-based system maintains the necessary security posture). Monitor the security controls that fall under the organization's responsibility.

Once a cloud SLA is built and agreed with the CSP, the organization now has a mechanism to monitor the fulfillment of the requested security SLOs. This is the essence of the risk control stage in the proposed approach. Despite its apparent feasibility, to the best of our knowledge, there is a paucity of efforts exploring this area. One reason limiting the development of such SLA-based SecaaS monitoring solutions arises from the lack of cloud-specific standards associated with SLA's, SLO's, and metrics/measurements. This topic will be further discussed in Section 5. For more information about the proposed approach interested readers can refer to this article13.

CMaaS for Providers

[Guidance for building the business case and contractual elements for offering a CM as a Service.]

Information for Decision Makers (C-Suite)

Technical ramifications

Operational Ramifications

Legal Ramifications and Privacy issues

SLAs

At the time of writing this report, the latest draft of the ISO/IEC 19086-1 standard (please refer to Section 5) considered the inclusion of a "Service Monitoring Component" in compliant SLAs. The service monitoring component proposed by 19086-1 lists the parameters, for the covered cloud services, that are monitored by the CSP and the data

[13] Please refer to J. Luna, N. Suri, M. Iorga, A. Karmel, "Leveraging the Potential of Cloud Security Service Level Agreements through Standards". In IEEE Cloud Computing Magazine, 2015

provided to the cloud customer. Monitored parameters were expected to be associated to committed SLOs, and specified in terms of standardized metrics (also compliant to ISO/IEC 19086-2). It should be noticed that ISO/IEC 19086-2 does not recommend/mandate any specific set of SLOs/metrics to monitor, but it considers that complaint SLAs should at least specify (i) the monitoring parameters, and (ii) the monitoring mechanisms. Furthermore, 19086-1 opens the possibility to allow customers to monitor their agreed cloud SLAs through the tools provided by the CSP (possibly SecaaS). It is worth to notice that the ISO/IEC 19086 standards open the possibility of monitoring both quantitative and qualitative SLOs. Further information related to these standards can be found in Section 5.

Useful CSP guidelines related to cloud customer expectations in the context of SLA monitoring can be found on the SLA-Ready project14.

Annex 5 – SLA Repository: CSP Questionnaire

Next we include the questionnaire used to contact CSPs in order to request their contribution to fill in the SLA Repository.

Do you need to sign a Cloud SLA & you want to find everything you need, in the one place to make sure what you sign has the right: vocabularies, SLO metrics/measurements, and compliance with standards/best practices? Well this **May 2016**, the European project SLA-Ready[15] has developed precisely all of these features in its **Common Reference Model *(aka CRM)***. This CRM hopes to make European SMEs' life easier in sifting through time-consuming legal contracts for the uptake of cloud computing.

In order to validate the developed CRM[16] from your perspective, we kindly ask you to answer the following set of questions.

1. Information about the participant's profile:
   a) Which one of the following roles best describes your Cloud computing activity? *(Please tick just one answer)*
      [ ] Cloud Service Provider or CSP (e.g. CxO, R&D, etc).

      [ ] Cloud Service Partner (e.g. security auditor, Cloud broker, developer)

   b) Which industrial sector is your main cloud service customer?
      [ ] Small and Medium-sized Enterprise (SME, private sector)

      [ ] Non-SME (private sector)

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

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

[16] CRM follows a 3-level hierarchical structure: the top level contains eight (8) *groups*, organize thirty (30) *elements* that include the main notions that can be mapped to the different aspects of cloud SLAs. Following the ISO/IEC terminology, the lowest level comprises the *components* that are part of the service level objectives (SLO) related elements of the CRM.

[ ] Public sector

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

[ ] Education

[ ] Financial Services

[ ] Government

[ ] Information Technology (IT) & Telecommunications

[ ] Other (please specify): _____

d) How well the following high-level use cases[17] describe the interests of your cloud service customers? *(Please rank from 1 (better) to 5 (worst))*

[ ] Application on a Cloud. An Enterprise develops an App on a Cloud Service for their end users.

[ ] Cloud bursting. Describes the scenario where workloads are migrated on-demand to a public CSP as needed by the cloud customer.

[ ] Processing sensitive data. An enterprise wants to use an online cloud application (SaaS) to process sensitive data, including Personally Identifiable Information (PII).

[ ] Data integrity. A customer moves a three-tier application from an on-premises data centre to an IaaS CSP that will run the application off-premises.

[ ] High availability. Through the use of one of more CSPs an organization provides high availability in the event of a disaster or a large-scale failure.

e) In which aspects of the Cloud service life cycle are your cloud service customers interested? *(Please rank from 1 (high interest) to 3 (low interest))*

[ ] They are interested on how to acquire Cloud services (e.g., choosing a CSP).

[ ] They are interested on the actual operational stage of the Cloud service (e.g., monitoring)

[ ] They are interested on the termination process of the Cloud service (e.g., understanding data retention clauses)

2. Based on your offered Service Level Agreement, please perform its self-assessment based on the criteria presented on the *attached* spreadsheet.

3. From your point of view, is the CRM missing critical groups/elements/components that could contribute to improve the way SMEs deal with cloud services?

4. Do you agree to make publicly available in the SLA-Ready website the provided self-assessment?
   ☐ Yes, I agree
   ☐ No, I don't agree. Please specify a reason:

5. Would you be willing to participate in a follow-up discussion on this subject? If yes, please provide your name and a contact email address:

[17] Categorization based on ETSI's "Cloud Standards Coordination – Final Report". Available online: http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf

Annex 6 – SLA Repository: CSP Self-Assessment

This annex presents the questionnaire used to allow CSPs self-assessing their SLAs based on the developed CRM. An online version is also available[18].

Group	Name of CRM element	Explanation/Assessment Question	CSP Self-assessment	Comments
General	SLA URL	Is there a publicly (online) available version of your cloud SLA?	0 = No , 1= Yes (please provide URL)	
	Findable	How can customers find the SLA on your website?	0 = n/a , 1 = External search engine, 2 = Internal search engine , 3 = Homepage link	
	Choice of law	Is the SLA specific to a particular jurisdiction or geographical area?	0 = n/a or No, 1 = Yes	
	Roles and responsibilities	Does your SLA contain a clear definition of roles and responsibilities?	0 = n/a or No, 1 = Yes	
	Cloud SLA definitions	Does your SLA contain relevant definitions used in the text?	0 = n/a or No, 1 = Yes	
Freshness	Revision date	Does your SLA specify the date of its last revision?	0 = n/a or No, 1 = Yes	
	Update Frequency	Does your SLA specify the frequency of performed updates based on a reported "Last Update" value?	0 = n/a or No, 1 = Yes	
	Previous versions and revisions	Are the public available the previous versions of the SLA?	0 = n/a or No, 1 = Yes	
	SLA duration	Does your SLA contain a clear specification of its validity period?	0 = n/a or No, 1 = Yes	
Readability	SLA language	Is your SLA specified in more than one language?	0 = n/a or No, 1 = Yes	
	Machine-readable format	Is your SLA available in machine-readable format?	0 = n/a or No, 1 = Yes	
	Nr. of pages	What is the number of pages on your SLA? Only applies to SLAs in PDF/document format.	0 = n/a or No, 1 = Please specify the number of SLA pages	
Support	Contact details	Does your SLA contain a reference to the helpdesk number or other details to contact support?	0 = n/a or No, 1 = Yes	
	Contact availability	Does your SLA contain information about contact availability, specifying days of the week and working hours?	0 = n/a or No, 1 = Yes	
Credits	Service Credit	Does your SLA has a clear specification of the service credits provided to the CSC?	0 = n/a or No, 1 = Yes	

[18] http://www.sla-ready.eu/sla-common-reference-model-questionnaire-csps

	Service credits assignment	Does your SLA specify the conditions whether a service credit shall be provided or not to the customer?	0 = n/a or No, 1 = Yes	
	Maximum service credits (Euro amount) provided by the CSP	Does your SLA describe how much does the can CSP credit (Euros) to the customer?	0 = n/a or No, 1 = Yes	
Changes	SLA change notifications	Does your SLA specify of how the CSP notifies customers about SLA changes?	0 = n/a or No, 1 = Yes	
	Unilateral change	Does your SLA describe if the CSP is entitled to unilaterally change it?	0 = n/a or No, 1 = Yes	
Reporting	Service Levels reporting	Does your SLA describe if reports about achieved Service Levels are provided to the customer?	0 = n/a or No, 1 = Yes	
	Service Levels continuous reporting	Does your SLA explain if/how the service level reports are continuously updated?	0 = n/a or No, 1 = Yes	
	Feasibility of specials & customisations	Does your SLA clearly define any "specials"/exceptions and other possible customisations?	0 = n/a or No, 1 = Yes	
	General Carveouts	Does your SLA clearly define CSP assumptions, exclusions, scope of force majeure, and other carve outs to the negotiated cloud services, SLOs and SLA?	0 = n/a or No, 1 = Yes	
SLOs & Metrics	Specified SLO metrics	Does your SLA clearly and unambiguously specifies metrics related to the SLOs defined in the SLA?	0 = n/a or No, 1 = Yes	
	General SLOs	Does your SLA specify SLOs related to aspects like service monitoring, accessibility, availability, termination of service, applicable certifications, and governance?	0 = n/a or No, 1 = Yes	
	Cloud Service Performance SLOs	Does your SLA specify SLOs related to aspects like response time, capacity, and elasticity?	0 = n/a or No, 1 = Yes	
	Service Reliability SLOs	Does your SLA specify SLOs related to aspects like service resilience, disaster recovery, and customer's data backup/restore?	0 = n/a or No, 1 = Yes	
	Data Management SLOs	Does your SLA specify SLOs related to aspects like IPR, CSC/CSP data, derived data, account data, portability, data deletion/location/examination, and law enforcement access to CSC data?	0 = n/a or No, 1 = Yes	
	Security SLOs	Does your SLA specify SLOs related to aspects like cryptography, physical/operational/communication security, incident management, compliance, and business continuity?	0 = n/a or No, 1 = Yes	
	Personal Data Protection SLOs	Does your SLA specify SLOs related to aspects like consent and choice, limitation, accountability, PII collection/use/retention/disclosure limitation, and privacy compliance?	0 = n/a or No, 1 = Yes	