www.sla-ready.eu

Title: Standardisation and International Cooperation - Initial Report

Author(s): Jesus Luna, Daniele Catteddu, CSA

Contributor(s): Neeraj Suri, TUDA; Nicholas Ferguson, Trust-IT

Date: 31 December, 2015

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

Executive Overview

The most enthusiastic adopters of Cloud services should be small firms, the lifeblood of the European economy. But lack of knowledge about Cloud services is the main reason why more firms are not using the Cloud as much as expected. Moreover, small firms are typically offered "take-it-or-leave it" contracts (standard templates) with very little bargaining power. Not surprisingly the top barriers for business uptake of Cloud services are the lack of clearly defined terms and conditions, transparent pricing and balance between the rights and responsibilities of users and providers.

SLA-Ready focuses on removing the barriers to Cloud service adoption by analysing current Cloud Service Provider (CSP) practices for Service Level Agreements (SLA) as a critical user-Cloud interface. This analysis is the first step towards defining a **Common Reference Model** (CRM) (D4.3 & 4.4), which will benefit industry by integrating a set of SLA components, such as common vocabularies, metrics and measurements for service level objectives, as well as **best practices** and **relevant standards** to fill identified gaps in the current SLA landscape.

SLA-Ready is therefore driving a common understanding of SLAs for Cloud services with greater standardisation and transparency so organisations can make an informed decision on what services to use, what to expect and what to trust.

SLA-Ready aims to fill **a significant market gap** by offering a digital marketplace on Cloud and SLAs for small firms, which is currently lacking in the landscape. The marketplace will provide small firms with much-needed practical guides and tools so they can carefully plan their journey based on an informed, stepping-stone approach, so the Cloud and applications grow with their business.

SLA-Ready not only fills a market gap, it is also contributing to European policy objectives. When Neelie Kroes, former Vice-President of the European Commission responsible for the Digital Agenda, announced the European Strategy for Cloud Computing in September 2012, she highlighted the fundamental importance of removing barriers to adoption in order to deliver a €160bn boost to the European economy:

> "*Cloud computing could offer a huge lift to the European economy. But only if users can understand and trust it. [...] We need to remove those barriers. If we do remove them, virtually every company, 98% of them, says they would increase or start investment in the Cloud*" [1].

Almost exactly three years later Andrus Ansip, Vice President for the Digital Single Market at the European Commission, highlighted low uptake of digital technologies as a priority action for the European Digital Single Market:

[1] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, A European strategy for Cloud computing, September 2012, http://europa.eu/rapid/press-release_SPEECH-12-652_en.htm?locale=en.

> "*In Europe, our business and industry have been quite slow to take advantage of advanced digital technologies - mobile, social media, Cloud, big data. Under two percent of EU companies make full use of such technologies. About 40% do not use any at all. Making more and better use of IT processes will bring many operational and commercial advantages. However, we cannot build a data-driven economy which functions properly – or which can reach its full potential - without first removing a series of barriers*"[2].

SLA-Ready plays a timely and critical usability role through its advocacy of reference SLA and best practice repositories. Ultimately, SLA-Ready will help build confidence and trust in the European Cloud market as the very foundation of business.

SLA Standardisation

One of the three major objectives of the European Cloud strategy regards standards and certification, with the aim of building trust and confidence in Cloud services by helping:

> "*users evaluate and compare services, and know which ones to trust. For example, we will put Cloud users more in control of their data, with standards based on the principles of interoperability, portability and reversibility*"[3].

A core activity within SLA-Ready is international co-operation and standardisation with the aim of building consensus on best/good practices through an-depth analysis of the current standards landscape and industry-led initiatives. Our goal is to empower Cloud service customers through the use of standardised Cloud SLAs as a critical step towards better understanding the level of security and data protection offered by the CSP, and for monitoring the provider's performance and security levels.

SLA-Ready therefore takes a pro-active approach to standardisation efforts by engaging with relevant standards groups and actively influencing their Cloud SLA initiatives. The most relevant standards groups are:

- ISO/IEC of the Joint Technical Committee – 1[4].
- European Telecommunications Standards Institute (ETSI) – Cloud Standards Coordination – Phase 2[5].
- National Institute of Standards and Technology (NIST)[6].

---

[2] Andrus Ansip, Vice President for the Digital Single Market, European Commission, September 2015, https://ec.europa.eu/commission/2014-2019/ansip/announcements/speech-vice-president-ansip-bruegel-annual-meeting-productivity-innovation-and-digitalisation-which_en. On the main actions for the Digital Single Market, see 'Digital Single Market Strategy: European Commission agrees areas for action', March 2015, http://europa.eu/rapid/press-release_IP-15-4653_en.htm.

[3] A European strategy for Cloud computing, op cit.

[4] Please refer to http://www.iso.org/iso/iso_technical_committee?commid=45020.

[5] Please refer to http://www.etsi.org/ and http://csc.etsi.org/phase2.html.

- TM Forum[7]

In addition, SLA-Ready also acknowledges the importance of best-practices and other industrial initiatives in this area, for example, the work of the Cloud Security Alliance, the EC's Cloud Select Industry Group on SLAs (C-SIG), the European Agency for Network and Information Security (ENISA) and the Cloud Standards Consumer Council (CSCC).

This document reports on the first year activities by SLA-Ready, targeting both standards groups and industrial/best-practices groups.

The report focuses on SLA-Ready's contributions to standardisation efforts and best-practices, with particular attention to aligning standards/best practices with the definition of the Common Reference Model (WP2). The overriding objective is to maximise the impact of SLA-Ready and its future sustainability.

The report also covers the main outcomes to date of international co-operation activities, in particular our liaison with related initiatives taking place within NIST and Brazil and the continuous interaction with the project's Advisory Board. Liaison to date includes face-to-face and virtual meetings, integrating feedback into our activities, especially the Common Reference Model.

Future work related to this deliverable will focus on:

- A Business Guide to Service Level Agreements: How to be a well-advised user of Cloud Services (Deliverable 3.3, December 2016).
- High-level report on Cloud SLA recommendations (Deliverable 3.4, December 2016).

Both outputs will focus on the perspectives of small- and medium-sized businesses (SMEs), the lessons learned from standardisation and best practices influenced or leveraged by SLA-Ready over its lifecycle. The outputs also integrate feedback received from the Advisory Board and the international initiatives with which SLA-Ready interacts.

[6] Please refer to http://www.nist.gov/, http://www.nist.gov/itl/antd/Cloud-102214.cfm.

[7] Please refer to https://www.tmforum.org

Table of Content

List of Acronyms 8
1 Introduction 9
1.1 Positioning this document within SLA-Ready 9
1.2 Structure of the document 10
2 Revisiting SLA-Ready's standardisation approach 12
3 Progress on standardisation activities 13
3.1 ISO/IEC 19086 14
3.1.1 Invitation to Category C liaison 15
3.1.2 ISO/IEC 19086 Part 1 – Overview and Concepts 15
3.1.3 ISO/IEC 19086 Part 2 – Metrics 17
3.1.4 ISO/IEC 19086 Part 3 – Core Requirements 18
3.1.5 ISO/IEC 19086 Part 4 – Security and Privacy 19
3.2 ETSI CSC Phase II 20
3.3 CSA CloudTrust and Cloud Trust Protocol Working Groups 21
3.4 C-SIG SLA 23
3.5 Other Initiatives Being Observed 24
4 Report on International cooperation and Advisory Board 26
4.1 NIST Initiatives 26
4.2 How Brazilian organisations are addressing SLAs 28
4.2.1 SERPRO 28
4.2.2 Konsultex 29
4.2.3 Anolis Tecnologia (IT) 29
4.3 SLA-Ready Advisory Board 30
4.3.1 Engagement and contribution to standards organizations. 31
4.3.2 Contributions to Deliverables. 31
5 Communicating the value of standards 37
6 Conclusions 38
Annex 1. Contributions to ISO/IEC 19086-Part 1 (current draft) 40
Annex 2. Expert feedback provided to ISO/IEC 19086-Part 2 (metrics ad-hoc group) 45
Annex 3. Contributions to ISO/IEC 19086-Part 4 (current draft) 47

Annex 4. Contributions to ETSI CSC Phase II 53

Table of Tables

Table 1. The role of D3.2 in SLA-Ready 10
Table 2. Implementation of SLA-Ready standardisation strategy 12
Table 3. Updated set of standards/best practices being followed by WP3 14
Table 4. Stage history for ISO/IEC 19086 Part 1 16
Table 5. Stage history for ISO/IEC 19086 Part 2 18
Table 6. Stage history for ISO/IEC 19086 Part 3 19
Table 7. Stage history for ISO/IEC 19086 Part 4 20
Table 8. Other initiatives being observed by SLA-Ready 24
Table 9. Advisory Board feedback and leverage by SLA-Ready 32

Table of Figures

Figure 1. Positioning D3.2 within SLA-Ready. 10
Figure 2. SLA-Ready: standardisation strategy (Deliverable 3.1). 12
Figure 3. Benefits of (SLA) automation across risk management frameworks. 27

Document information

Deliverable number	D3.2
Deliverable title	Standardisation and International Cooperation – Initial Report
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	December 2015
Actual delivery date	December 2015
Author(s)	Jesus Luna and Daniele Catteddu (Cloud Security Alliance)
Contributor(s)	Neeraj Suri (TU Darmstadt), Silvana Muscella and Nicholas Ferguson (Trust-IT)
Reviewer(s)	Arthur van der Wees (Arthur)
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	61

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 Standardization
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

Standardisation activities in SLA-Ready play a central role in maximising our impact in building consensus not only in Europe but also on the international scene wherever common goals are identified. By engaging with relevant international activities SLA-Ready guarantees:

- Alignment of the project's outcomes with standards and best practices, thus facilitating their industrial adoption.
- Enhanced validation of the Common Reference Model within the standardisation community. During the initial 12 months of the project duration, standardisation activities in SLA-Ready have followed a strategic approach that is positively reflected in the outcomes presented in this report.

The development and validation of SLA-Ready's Common Reference Model (CRM) is also enhanced through collaboration with relevant and well-identified stakeholders in the field of Cloud SLAs. We refer in part to the Advisory Board (AB) where a group of experts, including organisations like NIST and ISO/IEC, has been continuously contributing with SLA-Ready to develop the Common Reference Model requirements and start its validation process. Apart from the Advisory Board, the collaborations initiated by SLA-Ready include a community of potential Common Reference Model users engaged through the project's social network channels (mostly coming from small and medium-sized businesses – SMEs) and the partner's network of contacts e.g., CSA's SLA and Cloud Trust working groups. SLA-Ready's international collaboration activities performed during Year 1, in particular with US and Brazil, are also reported in this deliverable.

1.1 Positioning this document within SLA-Ready

This document interacts with both the definition of the Common Reference Model (WP2) and Communications, Impact and Exploitation (WP4) in SLA-Ready, as shown in Figure 1[8] and summarised in Table 1. Further details are presented in the rest of this report.

[8] This figure presents a refined version of the one reported in Deliverable 3.1.

Table 1. The role of D3.2 in SLA-Ready

SLA-Ready activities	Role of Deliverable 3.2	
	Leverage from standards and collaborations	**Contribution to standards and best practices**
WP2 – Common Reference Model	Alignment with ISO/IEC 19086-P1/P4, EC SLA Model report (SMART). Requirements and validation from AB.	Contribution of security components to ISO/IEC 19086-P4. Contribution to ETSI CSC Phase II.
WP3 – Best Practices & Recommendations	Initial validation of the Common Reference Model requirements and elements with Advisory Board. Initial engagement with NIST and CSA WG.	Preparing contribution to ISO/IEC 19086-P3 (core requirements).
WP4 – Digital Marketplace/Tutorials	Alignment of SLA Repository structure (Common Reference Model) to 19086-P1 and 19086-P4. Relevant standards summarised in the Marketplace.	SLA-Ready SLA Repository being planned as a contribution to CSA WGs.

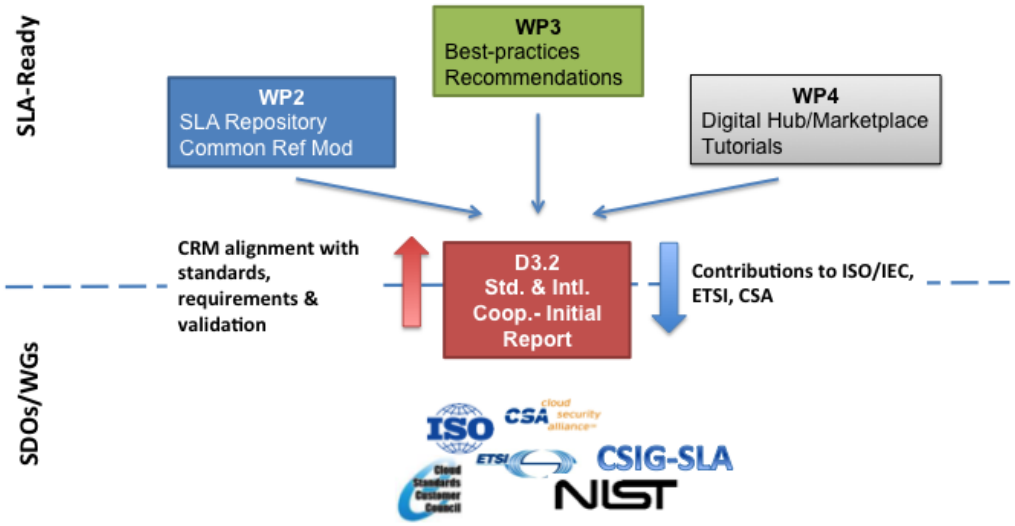


Figure 1. Positioning D3.2 within SLA-Ready.

1.2 Structure of the document

This document is structured as follows:

- Section 2 presents the enhanced strategy followed by SLA-Ready to identify and engage with relevant standardisation initiatives/best practices.
- Section 3 reports the standardisation-related activities that took place during the first year of SLA-Ready duration. For each reported activity this section analyses

the value from the SLA-Ready perspective along with future activities being planned.

- Section 4 presents the international collaborations started by SLA-Ready with relevant organisation and working groups as well as how Brazilian companies are dealing with SLAs. This section also discusses the feedback received from the Advisory Board and how it is managed by SLA-Ready.
- Section 5 elaborates on the value of SLA-related standards for SMEs.
- Section 6 discusses the conclusion and plans for the upcoming Deliverable 3.3 and Deliverable 3.4.

2 *Revisiting SLA-Ready's standardisation approach*

In the Engagement Plan for Standardisation and International Cooperation (Deliverable 3.1) we reported SLA-Ready's strategy to contribute and receive feedback from identified standards, best practices, and industrial initiatives. The rest of this section explains how we have further refined the strategy adopted, for example, by identifying partner roles and controls to guarantee the quality of contributions provided.

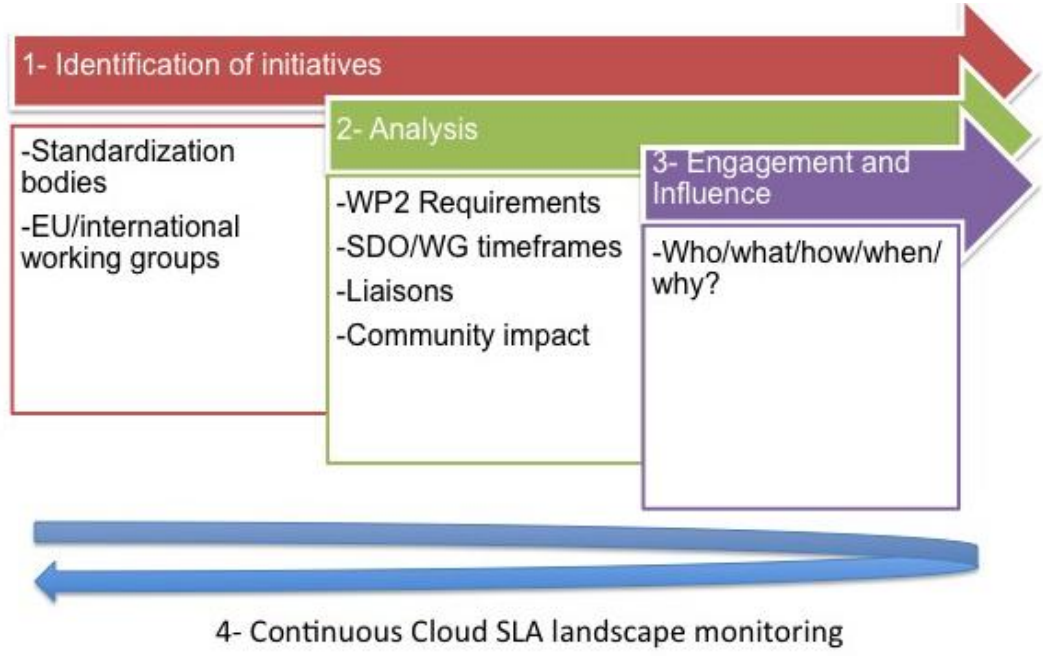


Figure 2. SLA-Ready: standardisation strategy (Deliverable 3.1).

The strategy documented in Deliverable 3.1 can be seen in Figure 2, where 4 well-differentiated stages have been implemented by WP3 (International Co-operation, Consensus and Standardisation) to efficiently identify, engage, influence and receive feedback from relevant standards groups and industrial organisations. From a more project-centric perspective, the strategy shown in Figure 2 was leveraged as explained in Table 2.

Table 2. Implementation of SLA-Ready standardisation strategy

Stage	Participating Partner/Role	Quality Controls
1 – Identification of initiatives	Arthur – related industrial initiatives CSA – Standards Development Organisations (SDO) and Standards Setting Organisation (SSO) landscape survey	✓ Focus on well-known SDOs/SSOs ✓ Prioritise initiatives being developed within the duration of SLA-Ready ✓ Emphasis on initiatives with major industrial participation and relevance
2 – Analysis	TUDA – gap analysis related to Common Reference Model (CRM)	✓ Focused analysis with the goal of maximising the impact of the

Stage	Participating Partner/Role	Quality Controls
	Arthur – gap analysis legal/data protection perspectives Trust-IT – gap analysis sociological perspective CSA – distribute relevant information within consortium	Common Reference Model ✓ Emphasis on SMEs (keywords e.g., end-user, core requirements) ✓ Keep consistency when related to multi-part standards
3 – Engagement and influence	TUDA/Arthur/CSA – development of contribution based on WP2 outcomes CSA – seek SDO/SSO consensus related to contribution, orchestrate output respecting format and timelines	✓ Relate to content provided in Deliverables 2.1 and 2.2 (CRM Requirements and elements) ✓ Present, discuss and refine prospective contribution based on feedback from representatives of other SDO/SSO members ✓ Follow-up status of contribution
4 – Continuous Cloud SLA landscape monitoring	Arthur/CSA – landscape update based on liaisons and memberships.	✓ Identify new SDO/SSO initiatives that may provide sustainability to SLA-Ready's outcomes ✓ Prioritise existing SDO/SSO engagements to keep project's focus. ✓ Avoid "opportunistic" (last minute, non-strategic) engagements.

The above referenced strategy and quality controls have provided, during the first 12 months of the project's duration, the results reported in the following section.

3 *Progress on standardisation activities*

Based on the proposed standardisation approach presented in Section 2, SLA-Ready selected an initial set of standards and best practices on which to focus its efforts (please refer to *Deliverable 3.1 - Engagement Plan for Standardisation and International Cooperation*) and which has been further refined and enhanced during the execution phase. The current standards/best practices being in the focus of WP3 are shown in Table 3 and Table 8, where it can be noticed that with respect to the information provided in Deliverable 3.1 the following updates have been applied:

- A first set of entries is not being followed anymore because after a more detailed analysis, and within the context of SLA-Ready, they were not considered relevant. Examples of such discarded initiatives are ATIS' Trusted Information Exchange, CSA Cloud Audit, and GICTF's Intercloud.

- A second set of initiatives is now being considered for future analysis, given the current activities taking place within SLA-Ready. In particular we refer to those targeting the technical specification of SLAs (e.g., WS-Agreement), related-protocol/interfaces specifications, and general-purpose ICT SLAs.
- A third set of entries has been added given their relevance to SLA-Ready e.g., CSA Cloud Trust.

Table 3. Updated set of standards/best practices being followed by WP3[9]

Organisation	Initiative acronym	Initiative	Relevance to SLA-Ready (Year 1)
CSA	CT	Cloud Trust	The security and privacy components from the CRM should be measurable. CSA CT is providing some of the metrics to recommend.
EC	C-SIG SLA	SLA Std. Guidelines	The CRM adopts the vocabulary proposed by these guidelines (WP2). In support to C-SIG SLA the security and privacy SLOs have been part of the contribution to 19086-Part 4 (WP3).
ISO/IEC	19086 Part 1 – 4	Cloud SLAs	SLA-Ready is aligning the CRM (WP2) to 19086-P1. Contributions are expected to 19086-P2/P3/P4 (WP3). Best practices are partially based in 19086 (WP4).
NIST[10]	CSM	Cloud Service Metrics model	SLA-Ready is expected to contribute to CSM (WP3) as a prior step to 19086-P2.

Based on the information from the previous table, the rest of this section focuses on presenting in further detail the standardisation activities performed by SLA-Ready during Year 1 along with the planned follow-ups.

3.1 ISO/IEC 19086

In mid-2014 ISO/IEC JTC 1/SC38/WG 3 started three new working items in the topic of Cloud SLAs namely overview and concepts, metrics, and core requirements. Afterwards, during Q1/2015 ISOI/IEC approved a new working item on security and privacy SLAs as part of the 19086 series of standards. Altogether, these four items are probably the most influential international standardization work on Cloud SLAs. They have the potential to provide higher levels of transparency and trust to the way Cloud Customers and CSPs will interact in the near future.

9 The listed standards and best practices will also be part oft he SLA-Ready Marketplace (WP4).

10 Contributions to NIST are reported in Section 4.

This section will look at how the project is actively engaged in the development cycle of the ISO/IEC 19086 standards, with the goal of maximizing the impact of SLA-Ready's outcomes, in particular the CRM.

3.1.1 Invitation to Category C liaison

In Year one SLA-Ready, was mentioned in the following SC38 recommendation: *"WG 3 recommends SC 38 to invite SLA-Ready to apply for a Category C liaison as SLALOM did."*

Consortium members already active in this group and members of the Advisory Board advised on whether the consortium should accept the invitation. Benefits of this included the visibility and kudos of being an official liaison and that this would most likely be positively. The prospective liaison may maximise the influence that SLA-Ready's CRM contributions can have in SC38, taking into account that further alignment and consensus can be reached also thanks to CSA's liaison.

However, importantly, the partners and the AB stressed that the impact of contributions are most important. Overhead in establishing the liaison would take valuable effort away from actually contributing positively.

In general the AB advised against the formal liaison for the following reasons:

- Consortium partners are already SC38 members and contributing to the standards process from within the established groups. It is already clear and to all and sundry that SLA-READY is already actively contributing to and influencing SC38 through its existing partner participations.
- Effort is saved from administrative overhead of creating the liaison and can be funneled into contributing and making a positive impact. In particular as quality of contribution is vital.
- SLA-Ready could also contribute to SC27. With no project partners present there a liaison may be required for this. Effort should be spent in establishing this which would be necessary for a contribution.

3.1.2 ISO/IEC 19086 Part 1 – Overview and Concepts

This draft standard, which is currently moving into DIS version[11], defines base terminology and concepts related to Cloud SLAs. This includes lifecycle and main Service Level Objectives categories (known as "Components" in ISO/IEC) and is not restricted only to a security perspective.

11 For an overivew related to the development of ISO/IEC standards, see http://www.iso.org/iso/home/standards_development.htm.

Year 1 Activities.

Between January-2015 and December-2015 members of the SLA-Ready consortium participated in the two face-to-face ISO/IEC JTC 1/SC38 meetings organized in Austria (March) and Ireland (September). The outcomes from the meeting in Austria related to ISO/IEC 19086 Part 1 have been reported in the previous Deliverable 3.1.

Member of the SLA-Ready consortium (CSA) attended the corresponding meeting in Ireland in order to discuss the contributions provided through the CSA liaison (please refer to Annex 2). It is worth noting that provided contribution also integrated feedback from relevant EU FP7 projects, in particular A4Cloud[12] and SPECS[13].

Planned Year 2 Activities.

At the time of writing the present report the 19086 Part 1 draft was about to become a DIS version, meaning that basically only minor technical contributions can be expected before its final publication. During Year 2 SLA-Ready will be focused on keeping the alignment of its CRM with the 19086 Part 1 DIS, in particular with respect to the list of applicable SLOs/SQOs/components (i.e., performance, security and privacy). The same list of components will also become part of the analysis to be performed by WP4 (SLA Repository).

Table 4 shows the current timeline associated to ISO/IEC 19086 Part 1.

Table 4. Stage history for ISO/IEC 19086 Part 1

Version	Description	Limit date	Started	Status
1	New project approved		2014-09-22	CLOSED
1	Committee draft (CD) registered		2014-11-04	CLOSED
1	CD study/ballot initiated		2014-11-05	CLOSED
1	Close of voting/comment period		2015-02-07	CLOSED
1	CD referred back to Working Group		2015-07-01	CLOSED
2	CD study/ballot initiated		2015-07-01	CLOSED
2	Close of voting/comment		2015-09-01	CURRENT

12 Please refer to http://www.a4cloud.eu/.

13 Please refer to http://www.specs-project.eu/.

Version	Description	Limit date	Started	Status
	period			
	DIS registered	2016-09-22		WAIT
	International Standard published	2017-09-22		WAIT

3.1.3 ISO/IEC 19086 Part 2 – Metrics

This draft standard is currently still in WD version[14]. It proposes a technical model of reference for documenting Cloud SLA metrics (not only security-related). It is important to note that the current ISO/IEC 19086-Part 2 draft is passing through several changes in both structure and content, as expert feedback has highlighted that content is overly technical and complex.

Year 1 Activities.

In analogy to the reported ISO/IEC 19086 Part 1 meetings described above, SLA-Ready also attended the SC38 discussions related to ISO/IEC 19086 Part 2. Given the continuous changes related to this draft standard, SLA-Ready has focused on following the discussions related to the proposed templates for documenting Cloud SLA metrics. In particular SLA-Ready has been providing expert feedback related to applying one of the proposed templates (coming from NIST) to security metrics like the one shown in Annex 3. The former is just an example of how the currently documented template can be used, although SLA-Ready's goal is to get fully understanding of the actual process in order to make it "SME-friendly".

Planned Year 2 Activities.

Given the latest outcomes from the ISO/IEC SC38 meeting reported above and the minor progress related to this particular draft standard, SLA-Ready will continue to focus on validating the proposed 19086 Part 2 model with the security and privacy metrics elicited in the context of ISO/IEC 19086 Part 4. During Year 1 this activity was executed along with the EU FP7 projects A4Cloud and SPECS. As both projects are finishing before SLA-Ready (Q1/2016) then the sustainability of their contributions will be supported through WP3. SLA-Ready partners CSA and TUDA participate in SPECS or A4Cloud. At the time of writing,

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

the reported timeline for 19086 Part 2 was still very general, as can be seen in the following table:

Table 5. Stage history for ISO/IEC 19086 Part 2

Version	Description	Limit date	Started	Status
1	New project approved		2014-09-22	CURRENT
	New project registered in TC/SC work programme			WAIT
	DIS registered	2017-09-22		WAIT
	International Standard published	2018-09-22		WAIT

3.1.4 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 WD version, but aiming to becoming CD early 2016) 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 components defined in Part 1.

For each of these pillars, and following the structure from Part 1, this draft discusses a particular requirements for assessing its conformance to the standard. 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 1 Activities.

In M1-12 the ISO/IEC 19086 Part 3 draft stayed in a WD version with regular changes made by the editors mostly reflecting the changing nature of both Part 1 and Part 2. During this period SLA-Ready observed the development of the standard also by attending the SC38 meetings in Austria and Ireland during 2015.

Planned Year 2 Activities.

The core requirements being documented in the draft 19086 Part 3 are close related to the best practices that SLA-Ready is developing for the CRM. During the rest of its duration, the SLA-Ready consortium will actively contribute to 19086 Part 3 with a set of best practices that align the proposed compliance requirements with the actual SME

expectations (WP2 and WP4). Furthermore, in the current 19086 Part 3 there is a conspicuous lack of core requirements related to the security and privacy components being documented in ISO/IEC 19086 Part 4. SLA-Ready will also contribute to those requirements by engaging relevant communities through the partners' network of contacts e.g., deploying targeted surveys in the CSA website/channels. The timeline associated to 19086 Part 3 is shown below.

Table 6. Stage history for ISO/IEC 19086 Part 3

Version	Description	Limit date	Started	Status
1	New project approved		2014-09-22	CURRENT
	New project registered in TC/SC work programme			WAIT
	DIS registered	2017-09-22		WAIT
	International Standard published	2018-09-22		WAIT

3.1.5 ISO/IEC 19086 Part 4 – Security and Privacy

In October 2014 some Cloud stakeholders (including CSA) highlighted the need for an international standard focused on the definition of security and privacy Cloud SLA elements. Based on this argument, in 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 expertise on the topic.

Year 1 Activities.

From month 1 to 12 the SLA-Ready consortium engaged with ISO/IEC 19086 Part 4 in two different ways:

- Aligning the CRM's security and privacy components to those proposed by 19086 Part 4.
- Contributing FP7 CUMULUS security properties[15] developed by CSA to the 19086 Part 4 draft. It is worth highlighting that the CUMULUS project did not have a standardization-related task, therefore a collaboration with SLA-Ready was created. The overall CSA contribution to 19086 Part 4, including SLA-Ready's, is shown in Annex 2.

15 Please refer to http://www.cumulus-project.eu/.

Planned Year 2 Activities.

As mentioned previously, one of the major standardization activities planned for SLA-Ready during Year 2 relates to actively contributing to the core requirements contained in ISO/IEC 19086 Part 3. As part of the foreseen contributions, SLA-Ready plans to provide also security/privacy requirements aligned to 19086 Part 4. Furthermore, SLA-Ready will follow-up on the contributions that originated from EU FP7 SPECS and A4Cloud both of which are finishing Q1/2016.

Table 7. Stage history for ISO/IEC 19086 Part 4

Version	Description	Limit date	Started	Status
1	Proposal for new project registered		2014-12-11	CLOSED
1	New project ballot initiated		2014-12-12	CLOSED
1	Close of voting		2015-03-14	CLOSED
1	New project approved		2015-03-30	CURRENT
	DIS registered	2018-03-30		WAIT
	International Standard published	2019-03-30		WAIT

3.2 ETSI CSC Phase II

Started in February 2015, the ETSI CSC Phase II activity was designed to develop a follow-up set of reports to the ETSI Cloud Standards Coordination deliverable[16] from 2013. More in particular, ETSI CSC Phase II (finished in December 2015) produced four reports: Cloud Computing User Needs (WI1), Standards and Open Source (WI2), Interoperability and Security (WI3), and Standards Maturity Assessment (WI1). The topic of Cloud SLAs was mostly in the focus of the WI3 report.

Year 1 Activities.

SLA-Ready provided feedback on Cloud SLAs to the WI3 report during the public commenting period in September-2015. The following areas were covered:

1. Proposed a categorization of Cloud SLA standards, given that the reviewed version did not have such classification.

16 Please refer to http://csc.etsi.org/phase1/CSC_report.html.

2. Proposed further research/awareness on the topic of machine-readable SLAs, as considered by the SLA-Ready CRM.
3. Provided explicit references to the work being done by ISO/IEC JTC 1 SC 38/WG 3 on Cloud SLAs.
4. Highlighted the relevance of metrics/SLOs/SQOs for the creation of Cloud SLAs.

The feedback provided was discussed during the "Final Review Workshop" that took place in October 1-2 2015 in Brussels[17]. Furthermore CSA also represented SLA-Ready on a panel organized by ETSI in Brussels to present the final version of the CSC Phase II reports[18].

The final version of the ETSI CSC Phase II WI3 report managed and integrated all the received SLA-Ready comments[19].

Planned Year 2 Activities.

The ETSI CSC Phase II activity finalized in December 2015, however the resulting reports will become part of the CRM's recommended set of guidelines for understanding Cloud SLAs. During Year 2, the SLA-Ready consortium will further analyse the recommended set of actions (in particular from WI3) to fine-tune the CRM. In particular we refer to the following:

- The relevance and potential high-value use of the upcoming framework for Cloud SLA (ISO/IEC 19086 Part 1 to 4).
- Using the Cloud SLA to identify and populate core concepts with content relevant for the Cloud service for which the Cloud SLA is created, in order to substantially alleviate the burden of keeping track of all relevant areas that need to be included in the Cloud SLA.
- The availability of standardised metrics that can be populated with values set in the Cloud SLA as a mean to provide better visibility in terms of the level of quality of the Cloud services provided, thus establishing better trust and confidence in the Cloud Computing space.

3.3 CSA CloudTrust and Cloud Trust Protocol Working Groups

In the Description of Action document (DoA) the SLA-Ready consortium identified some CSA research working groups[20] related to Cloud SLAs namely the Privacy Level Agreement

17 Please refer to http://csc.etsi.org/phase2/phase2/ReviewWorkshop.html.

18 Please refer to http://csc.etsi.org/phase2/FinalPresentation.html.

19 The final version of the ETSI CSC II report (Interoperability and Security) is available at http://csc.etsi.org/resources/STF_486_WP3_Report-v2.0.0.pdf.

20 Please refer to https://cloudsecurityalliance.org/research/.

(PLA) WG, the SLA WG, the Cloud Trust Protocol (CTP) WG, and the Cloud Trust (CT) WG. During Year 1 the project mostly focused on the later given its strong relationship to ISO/IEC 19086 Part 2 and Part 4.

In order to support the industrial validation and standardization of Cloud security metrics, CSA created in April-2015 the Cloud Metrics working group (renamed to Cloud Trust[21] or CT in July-2015). The CT working group aims to build confidence in the market and to accelerate secure adoption of Cloud services by promoting collaboration between Cloud customers (in particular SMEs), CSPs, international standards organisations and global regulatory authorities, all of which are considered stakeholders in the CT Working Group. The CT working group's activities focus on the collection and validation of monitorable security and privacy metrics for Cloud SLAs, which includes the following tasks:

a) Developing a catalogue of security and privacy Cloud service metrics with standardized measurement methods, based on the latest research in the field, industry practices and Cloud customers' interests.
b) Motivating and documenting the validation of the metrics catalogue by stakeholder.
c) Documenting the best practices associated with the use of these metrics in the definition of SLAs, as well as their measurement and monitoring.

Year 1 Activities.

With the support of SLA-Ready, the CT working group aligned its activities in order to support ISO/IEC and NIST. In particular, SLA-Ready contributed to the CT's catalogue of security/privacy metrics (partially documented in WP2). Furthermore, SLA-Ready supported the CT WG by providing feedback related to the automated catalogue of Cloud SLA security and privacy metrics being developed by the EU FP7 SPECS project. This automated catalogue system was described in a previous section, where contributions to NIST were presented.

Planned Year 2 Activities.

During the rest of its duration SLA-Ready will continue collaborating with the CSA CT WG on the topics related to the security and privacy metrics catalogue. Furthermore, the best practices developed in the context of the CRM (WP2) will be also provided to CT as part of the efforts to develop the foreseen "CSA Cloud metrics guidance" late 2016.

[21] Please refer to https://cloudsecurityalliance.org/group/cloudtrust/.

3.4 C-SIG SLA

On October 29th, 2015 the EC organized a meeting[22] to discuss follow-up actions associated to the Cloud Selected Industry Groups (C-SIGs) including C-SIG SLA. One of the main topics discussed during this meeting was the synergy generated between the C-SIGs and the Digital Single Market communication (DSM). This section focuses on C-SIG SLA.

Year 1 Activities.

Starting from the CRM requirements, SLA-Ready adopted the vocabulary proposed by the C-SIG SLA guidelines. Also, in support to C-SIG SLA the security and privacy SLOs have been part of the project's contribution to 19086-Part 4 (WP3), just as mentioned in Section 3.1.

Furthermore, SLA-Ready attended the C-SIGs meeting in order to find potential alignments with C-SIG SLA and engagement in future actions. The published C-SIG SLA guidelines are still considered as having a strong focus on business-to-business, and much less on the actual Cloud customers. Furthermore, there is also a conspicuous gap related to basic SLA guidance on minimum requirements to be taken into account by customers. Also, during this session was highlighted the need of creating a categorization/classification of CSP SLAs with the goal of supporting customers in their choice of providers and understanding of underlying SLAs. The topic of Cloud SLA standardization was also discussed, with some initial thoughts on focusing future C-SIG SLA efforts on ISO/IEC 19086 Part 3 (core requirements).

Planned Year 2 Activities.

Based on the preliminary conclusions drawn from the reported C-SIG SLA meeting, SLA-Ready will further analyse the relationships between its main outcomes and the future C-SIG SLA objectives. An early collection of potential Year 2 activities where synergies between SLA-Ready and C-SIG SLA can be developed is mentioned next:

1. End-user/SME engagement in order to further refine and validate the produced SLA Guidelines.
2. Lowering the barriers for SMEs to understand and make informed decisions involving Cloud SLAs.
3. Providing a "categorization" of Cloud SLAs, possibly based on the analysis of case studies (as planned by SLA-Ready's Deliverable 2.3).

22 Please refer to http://ec.europa.eu/digital-agenda/en/news/Cloud-select-industry-group-c-sig-plenary-meeting-0.

3.5 Other Initiatives Being Observed

Besides the contributions to standards/best practices previously reported SLA-Ready also monitors other set of initiatives relevant to the project, but which have not been yet contributed (or were not being maintained during Year 1). This section briefly summarizes the project's activities related to these other set of standards and best practices.

Year 1 Activities.

The entries listed in Table 8 are being leveraged by SLA-Ready, in particular WP2, to shape the work on Common Reference Model requirements and development (D3.3 & 3.4). Most of the initiatives mentioned in the rest of this section are not being maintained during the project's duration, nevertheless their relevance to SLA-Ready is being analysed by the project.

Table 8. Other initiatives being observed by SLA-Ready

Organisation	Initiative acronym	Initiative	Relevance to SLA-Ready (Year 1)
CSA	PLA	Privacy Level Agreement	The privacy components in the CRM (WP2) are being aligned with CSA PLA.
CSCC	CSCC SLA	Practical Guide to Cloud Service Level Agreements – v2	The 10 recommended CSCC SLA steps were considered as requirements for the CRM in WP2. Best practices from WP4 are partially based on CSCC SLA.
EC	SMART	Standards terms and performance criteria in service level agreements for Cloud computing services	The proposed Model SLA is being compared and analysed wrt. the CRM developed in WP2. In WP4 the best practices, which are partially based on SMART, will be extracted..
ENISA	Procure Secure	Procure Secure - A guide to monitoring of security service levels in Cloud contracts	SLA-Ready CRM's sector specific requirements (government) are being extracted from Procure Secure (WP2).
ETSI	TR 103 125	SLAs for Cloud services	Defines a simple Cloud SLA template that can be used as input to SLA-Ready's CRM.
ETSI	CSC Phase II	Security and Interoperability	SLA-Ready has contributed to CSC Phase II (WP3).
ISO/IEC	27004	Information security monitoring, measurement, analysis and evaluation	The recommended practices maybe applicable to SLAs, so these can be leveraged into the CRM's guidelines.
NIST	CSM	Cloud Service Metrics model	SLA-Ready is expected to contribute to CSM (WP3) as a prior step to 19086-P2.

Organisation	Initiative acronym	Initiative	Relevance to SLA-Ready (Year 1)
TMF	GB917	SLA Management Handbook	Non-Cloud specific. The SLA lifecycle in D2.2 is aligned with the GB917's "customer" lifecycle. It Is worth to notice that GB917 does not discuss any related regulatory or legal aspects, or common requirements based on identified lifecycles.
TMF	GB963	Cloud SLA Application Note	The CRM requirements (D2.2) took into account (and extended) the "Enterprise-grade External Compute IaaS" requirements developed in GB963. The CRM components (D2.3) also include the "Direct SLA Requirements" from GB963.

Our analysis also considered other relevant documents like TMF TR178 (Enabling end-to-end Cloud SLA Management) and TMF TR197 (Multi-Cloud service management pack – SLA Business Blueprint), although in both cases the core topic of multi-clouds was out of scope in SLA-Ready.

Planned Year 2 Activities.

The preliminary analysis of the initiatives mentioned in Table 9 shows the potential these standards/best practices may have for the development of the CRM being developed in WP2 and the Marketplace in WP4. During Year 2, SLA-Ready will further elaborate on these initiatives from two different perspectives:

- Opportunity to contribute: this is the case of CSA PLA and ISOIEC 27004, where expected SLA-Ready contributions on the topics of privacy components and SLA measurement/monitoring are expected. In particular, the relevance of SLAs is a conspicuous gap in ISO/IEC 27004, and the Common Reference Model's privacy components need further alignment with CSA PLA.
- Leverage into CRM and Marketplace: during Year 2 the project will put particular effort in gap analyzing the CRM with respect to well-known industrial initiatives like CSCC SLA and TMF's works (please refer to Table 9), in order to guarantee enough CRM coverage with these. Expected results will be documented in both Deliverable 2.3 and 2.4. Reports like SMART and Procure Secure will be also used as a basis to extract use cases for Deliverable 2.3. From a Marketplace perspective (WP4) these works will be referenced in the section devoted to standards and best practices, although leveraging them from a SME point of view.

4 Report on International cooperation and Advisory Board

This section reports the Year 1 activities related to international collaborations, and Advisory Board communication.

4.1 NIST Initiatives

NIST is devoting important efforts to the topic of Cloud SLAs both within the U.S. and internationally (e.g., ISO/IEC 19086). Besides NIST's participation in our Advisory Board with Dr. Eric Simmon, SLA-Ready also focused part of its Year 1 standardization efforts in developing other synergies with NIST as presented below.

Year 1 Activities.

One of the biggest challenges in the field of Cloud SLAs relates to the standard specification of metrics, which can allow some degree of comparability among CSPs. Before the efforts taken by ISO/IEC 19086-P2 (please refer to Section 3.1), NIST started developing a conceptual model for Cloud service metrics (CSM). The CSM model aims to be used as a standard for documenting Cloud metrics related to multiple aspects of a Cloud system (including performance and security). At the time of writing this report, the current version of the NIST CSM model specification was still on a public commenting period[23]. SLA-Ready is an active contributor to this specific NIST working group by (i) validating and providing feedback to the model through metrics documented in the CRM specification, and (ii) aligning the CRM's guidelines/best-practices based on the CSM model specification (to be documented as part of Deliverable 2.4). It is worth highlighting that NIST is the main editor of ISO/IEC 19086 Part 2, and the current draft standard leverages a "lightweight" version of the CSM model.

As part of the reported collaboration with NIST partner CSA presented an invited keynote during the "Cloud Computing Forum and Workshop VIII" event[24] on the topic of Cloud security SLAs. This event was useful to create awareness about SLA-Ready's objectives and tasks, in particular the CRM and the foreseen best practices.

Planned Year 2 Activities.

SLA-Ready is an active contributor to the NIST CSM model working group (also known as "RATAX") and future plans include continue supporting the specification of security and privacy metrics (please refer also to Section 3.3), and facilitating SME access to the CSM model through its leverage into SLA-Ready's CRM. With respect to the later, SLA-Ready plans to document best practices associated to the usage of the CSM model in particular

23 Please refer to http://www.nist.gov/itl/Cloud/upload/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf.

24 Please refer to http://www.nist.gov/itl/Cloud/Cloud_computing_wkshp_viii.cfm.

for comparability purposes. Another expected activity is to support EU FP7 SPECS[25] after it duration (April-2016), so research outcomes like the "Metric Catalogue" can be further refined and probably adopted by NIST RATAX. The current version of this catalogue[26] is being validated and tested by SLA-Ready partners CSA and TUDA.

Apart from continuing to collaborate with NIST RATAX, SLA-Ready has been also invited to participate in an upcoming NIST working group on the topic of Cloud security automation through SLAs and control frameworks. This upcoming working group already has the support of FedRAMP and may help to manage some AB comments related to machine-readable SLAs. In particular, this working group plans to develop a machine-readable specification for representing:

- Any security control (NIST 800-53, ISO/IEC 27001, or CSA CCM)
- Any technology/context (not only Cloud, but also for instance mobile and IoT)
- Any scope (functional capability or component for which it is implemented)
- Any implementation and assessment guidance (coming from providers when they submit their assessment report for example to CSA OCF - STAR)
- Any security SLA information.

A high-level view of the expected impact related to this new initiative can be seen in the following figure which shows how the benefits of automation/machine-readable formats are highlighted across a traditional risk management framework.

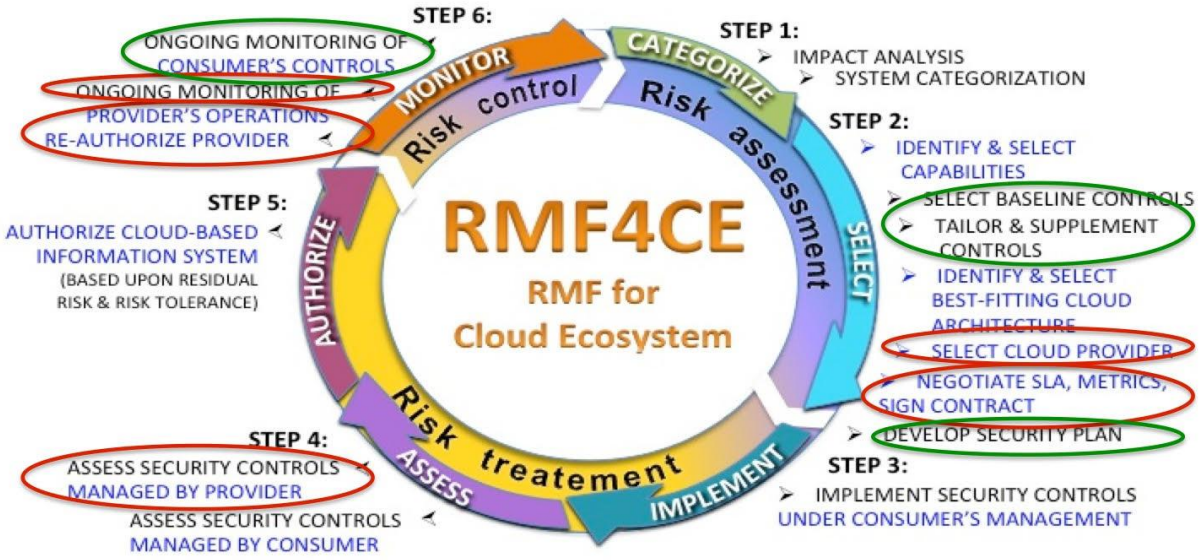


Figure 3. Benefits of (SLA) automation across risk management frameworks.

25 Please refer to http://www.specs-project.eu/.

26 Please refer to http://apps.specs-project.eu/specs-app-security_metric_catalogue/.

SLA-Ready's expected contribution to this new working group relates to elements of the CRM associated with the requirements captured in both Deliverable 2.1 – 2.2.

4.2 How Brazilian organisations are addressing SLAs

The promotion of innovative technologies has been a major focus in recent years in Brazil as it has become the main ICT hub in South America. Further advances in information and communication technologies will significantly benefit the social and economic potential of the country. The Brazilian government has recently implemented fiscal policies favouring ICT investment and fast wireless broadband take up. Collaboration between Europe and Brazil in terms of research collaboration, knowledge and skills creation is growing. Major international research organisations have on-going research activities with Brazil and there are also collaborative efforts on common IT standards across different disciplines. Large national actors are contributing to defining joint strategies on data sharing in sectors such as agriculture and biodiversity, where Brazil provides unique sources of data. Through the Cloudscape Brazil[27] event held in Rio de Janeiro, Brazil, SLA-Ready has engaged with Brazilian cloud service providers, from very large organisations such as SERPRO; a medium to small enterprise, Konsultex; and a start-up company, Anolis IT; to see how they are dealing with cloud SLAs and in particular security standards and standard SLO measurements. Other organisations engaged with include the Brazilian Research Network (RNP)[28] and small and medium businesses such as RioSoft[29], Propus[30] and UStore.

4.2.1 SERPRO

SERPRO[31] is the largest South American Government ICT Company providing structural systems for the Brazillian Federal Government. It has three datacentres in Brasília, São Paulo and Rio de Janeiro.

As part of a clear cloud strategy and roadmap, SERPRO is planning the release of improvements in services such as billing, accounting, monitoring, etc. This is being accomplished by the adoption of OpenStack's component for telemetry, i.e., Ceilometer. This has been installed and configured in the SERPRO environment the full stack of projects offered through their site. SERPRO are gradually consolidating them in their production environments. Combined with Ceilometer, SERPRO has their own applications, mostly Python-Zope-Plone and PHP/Symfony portals. They have also developed some python middleware and APIs to work with the OpenStack APIs.

[27] http://www.eubrazilcloudconnect.eu/content/cloudscape-brazil-2015

[28] http://www.rnp.br/en

[29] http://www.riosoft.org.br/

[30] http://www.propus.com.br/

[31] http://www.serpro.gov.br/

For security issues, SERPRO are still establishing a technological layer compliant with ISO-IEC standards 17788[32], 17789[33] and 27000[34]. Presently SERPRO are integrating OpenStack Keystone with Open/LDAP services. The security certifications we are exploring for this project are ISSEP/CISSP for Cloud security personnel and CCSE for SERPRO's security staff.

4.2.2 Konsultex

Konsultex[35] is a systems integration and consulting organization based in Argentina and Brazil specialized in implementing business systems. The company has recently started to provide cloud services. Konsultex has implemented several private cloud solutions since 2010 based on the open source Xen hypervisor that give our customers competitive advantages.

SLA aspect of contracts is focused Konsultex's support for their customer's solutions. There are several ways in which Konsultex deal with contracts for consulting services and license sales. When it's with a private company a model based on the contract models that our partners use is applied such as Alfresco and Bonitasoft.

When a Government body is involved, Konsultex does not have a choice as the contract is normally take-it-or-leave-it. However, recently lawyers have been employed by the company to assess government contracts. .

Konsultex are now considering involving lawyers to take on the role of working on contracts. Until now, this has always been an expense that the company has tended to avoid.

4.2.3 Anolis Tecnologia (IT)

Anolis IT are a new startup in Brazil which aims to create a secure, resilient and available SDS service for academic researchers and, in the future, become a SDS reference company. Anolis IT has experience with heterogeneous environment spread across the country; we contribute to two open source cloud technology, Openstack and Owncloud

Anolis IT provide cloud services using the Brazilian Research Network (RNP) infrastructure. At the moment RNP defines its own SLA with their costumers including Anolis IT. This follows old agreements of R&D Experimental Services, which do not include any SLA. From 2016, this will change and we will be able to define our SLA with RNP.

[32] http://www.iso.org/iso/catalogue_detail?csnumber=60544

[33] http://www.iso.org/iso/catalogue_detail?csnumber=60545

[34] http://www.iso.org/iso/catalogue_detail?csnumber=63411

[35] http://www.konsultex.com.br/

Anolis IT does not have any standardised measurements of service level objectives nor security certifications and are very interested in following and adopting recommendations from SLA-Ready so they can offer a better service and follow international standards and good practices.

Monitoring services are currently with Zabbix[36] have a date of March 31, 2016. The perspective for a first version in billing and accounting services is July 31. A probable date (yet to be set) for a security architecture implementation would be the end of the year (December 31, 2016).

Planned Year 2 Activities.

Following the publication of the final set of user requirements in D2.2, the consortium will share these with the Brazilian organisations in order to get their feedback and validation. In addition, results from D2.3 which will feed into SME-targeted services rolled out through the SLA-Ready website will also be shared with them. Indeed, those we contacted at Cloudscape Brazil were interested in SLA-Ready recommendations:

"If you (SLA-Ready) have some pointers about contracts and SLAs I would really like to know about them." Miguel Koren o'Brien de Lacy, Konsultex

"We (Anolis IT) are very interested in following and adopting those recommendations so we can offer a better service and follow international standards and good practices." – Guillherme Maluf Balzana, Infrastructure Director, Anolis IT

4.3 SLA-Ready Advisory Board

During Year 1, the AB has closely interacted with members of the consortium to provide feedback on the different outcomes produced by SLA-Ready.

Since the start of the project the consortium have organized two phone conference call and one face-to-face meeting.

Conference calls:

- 8th July 2015
- 17th September 2015

Face to face meeting: 8 October 2015, ISO meeting, Dublin Ireland.

With a number of AB members attending the meeting, SLA-Ready held a face-to-face meeting during the event in order to maximize participation.

[36] http://www.zabbix.com/

4.3.1 Engagement and contribution to standards organizations.

The AB has given guidance on how the consortium can best contribute to standards bodies in particular ISO/IEC 19086. The experts considered parts 2, 3 and 4 as most relevant to the outputs of the project and also where impact can be greater.

As outlined in section 3.1, the AB also advised on whether the consortium should accept the invitation to liaison received from ISO. The AB advised against the formal liaison for the following stressing that the impact of contributions are most important. Overhead in establishing the liaison would take valuable effort away from actually contributing positively.

4.3.2 Contributions to Deliverables.

The AB have provided feedback on four deliverables:

- D2.1 and D2.2 Requirements emerging from the state-of-the-art analysis
- D3.1 and 3.2 Engagement plan for standardization and international cooperation

The most important input has been in validating the user requirements identified in section 4 of D2.1. This has been key for the completion of D2.2 and will feed into the completion of the iterations of the common reference model in D2.3 and D2.4. The contributions are outlined in the table below.

Table 9. Advisory Board feedback and leverage by SLA-Ready

Advisory Board Member	Received Feedback (WP3)	Leverage by SLA-Ready
Monique Morrow	Understanding the delta between machine readable SLAs and human readable SLAs.	Feedback was provided to WP2. A CRM requirement on "Machine readable formats" has been added. It is worth to mention that SLA-Ready does not aim to create any specification for machine-readable formats, although the project can create awareness related to the lack of such specifications.
	The notion of compliance is implied and will certainly come under the data sovereignty laws per country. Legal experts will want to engage early and certainly export compliance SMEs.	To be considered in Task 2.2
	Identification of Liability by which entities	To be considered in Task 2.2
	There is a fine line between "intelligent SLA" vs "static long contractual constructs that are often non readable [depending on the audience]	To be considered in Task 2.1 (Sociological analysis)
	Deprecating to what can be common across the various jurisdictions may be a start.	To be considered in Task 2.2
John Kennedy	What (human!) language(s) are the SLAs available in?	Feedback provided to WP2. As a consequence, a new CRM requirement has been added (cf., Deliverable 2.2).
	What format is the SLA available in: HTML? PDF? … Machine readable? If latter – what file formats/language/interface?	Feedback provided to WP2, and new related requirement added to CRM. From the marketplace perspective (WP4), because the project wants to keep easy to understand SLA information, the SLA Repository assess if a machine-readable version of the CSP SLA exists (cf., Deliverable 4.2). During Year 2 we will consider investigating more details related to the offered machine-readable Cloud SLA.
	Is the SLA based on any particular reference model/ontology/standard – if so which?	Feedback provided to WP2, and to be further analysed by Task 2.1 possibly by focusing on specific SLAs from the Repository.

Advisory Board Member	Received Feedback (WP3)	Leverage by SLA-Ready
	Are particular countries/markets being targeted by this CSP – maybe there are interesting differences between what different markets are looking for in an SLA?	Feedback provided to WP2 and requirement added to the CRM, although will be further analyzed by Task 2.2
	What contract/legal framework does the SLA operate under. What legal jurisdiction (if relevant)?	Feedback provided to WP2. This requirement was integrated into the CRM and will be further analysed by Task 2.2
	Req. 6 Contact Details: contact availability hours (and time-zones) might be worth capturing explicitly.	Feedback provided to WP2 and new requirement added to the CRM. WP4 has created the assessment criteria related to this new requirement, in order to build the SLA Repository.
Petter Deussen	Please add a list of acronyms. Also, a glossary might be a good idea.	Feedback provided to WP2, and these requirements will be added as part of the CRM (Deliverables 2.2 and 2.3)
	It might be a good idea to compare/complement your lifecycle with the one of the Cloud service provider, as this will give you a good idea on what can happen during the service lifecycle, and provide you with information on how to refine it. A good starting point would be ITIL, and it might be useful to look into ISO/IEC Cloud Computing Reference Architecture.	Feedback provided to WP2. Deliverable 2.2 aligns both the SLA's technical and legal life cycles. Also Deliverable 2.2 considers the Cloud service life-cycle and highlights conspicuous differences like the lack of SLA Termination within 19086-P1
	Table 1: I'm not sure that the distinction academic, industry, standards/recommendation makes sense. In Section 3.1.1 you have a lot or SLA elements that are of general interest, but classified as "academic" because of their source.	Feedback provided to WP2. To be amended in Deliverable 2.2, where these will be classified in "components" as proposed by 19086-P1/-P4.
	The SLA elements presented here are taken out of the context of the projects/standards they came from. Hence, it is not clear how specific/general they are. In addition, I'd expect some considerations on completeness/coverage:	Feedback provided to WP2. Deliverable 2.1 discusses about the completeness of the selected SLOs, which will be further put into context in Deliverable 2.2. The analysis in SLA-Ready cannot claim completeness, because new SLOs related to both state of the art/state of practice will continue appearing. Our belief is that in

Advisory Board Member	Received Feedback (WP3)	Leverage by SLA-Ready
	Are these a complete set of element? Some methodology on how to answer these questions would be very useful.	the short term (and after the release of the 19086-P1/-P4 standards) more alignment to the "components" will be provided by CSPs. We will further analyse and extend as required in Deliverable 2.3
	Since they are out of context, the following SLA elements require more explanation regarding levels, metrics, and measurements: • Tenant isolation level (I believe this one is very important) • Vulnerability exposure level • Percentage of authorized personal that received training … (how could a customer accept less than 100% here?) • Percentage of recovery success (should be ration between success and failure) • Configuration change reporting capability • Percentage of compliant applications (very unclear: compliant to what? And what does this percentage tell us?) • Authorized collection of PII (unauthorized collection of PII is illegal. Having a percentage less than 100% here means the CSP has committed a crime). • Privacy program budget (really?) • Privacy program updates These elements are not related to service levels.	Feedback provided to WP2. These comment will be further analysed in Deliverable 2.2 As mentioned before, the goal of SLA-Ready is not to create a comprehensive catalogue of metrics (which may be actually taken be organizations like ISO/IEC or CSA). SLA-Ready's CRM will integrate elements that are common to publicly available SLAs, possibly aligned with relevant standards, and including the best practices that facilitate their understanding to SMEs.
	Is the "new directive" (D2.1) mentioned here the upcoming data protection regulation? You might want to investigate the difference between a directive and a regulation. These terms must not be used interchangeable.	To be analysed by Task 2.2

Advisory Board Member	Received Feedback (WP3)	Leverage by SLA-Ready
Wolfgan Ziegler	Certain aspects are not covered in the report: • Machine readability (already discussed during the last conference call) • Scalability and elasticity: Greatest market promises of Cloud computing but there seem to be no SLA element covering them.	Feedback provided to WP2, and both requirements integrated into the CRM (Deliverable 2.2) and documented as part of the SLA Repository (Deliverable 4.2).
	I have a general comment regarding the term SLA in the following table: You should distinguish between a template for an SLA and the SLA itself that comes into force when both parties agree upon. To my understanding in the following table the term SLA is used for both.	Task 2.2 will further discuss this particular topic, although in SLA-Ready our focus is on the actual SLAs offered by the CSPs and not on the templates.
	What will be publicly available is not the SLA but the template used to create the SLA (see my comment above). Once created both parties will have a link to the SLA. Which party stores the SLA might be domain dependent and usually should not matter.	To be further explained in Deliverable 2.2, although our focus is on the SLAs offered by the CSPs on their websites.
	Finding the SLA template(s) on the CSP's website seems essential for both the first step of selecting the most appropriate CSP and creating the SLA in the second step. "**Easily**" is a bit fuzzy though.	Feedback provided to WP4. Each CRM requirement is being associated with an "assessment criteria" that aims to minimize the subjectivity associated with terms like "Easily".
	Not quite clear what this information is used for by either of the parties. Is it assumed to be a measure for the complexity of the SLA? And, what does "Nr. Of pages " mean in case of electronic SLA templates?	Feedback provided to WP2. This element has been modified in order to be more concrete (refer to previous comment).
	Penalties and rewards should be part of the SLA (and included in the SLA template)	To be further analysed by Task 2.2

Advisory Board Member	Received Feedback (WP3)	Leverage by SLA-Ready
	This relates to monitoring (which is not addressed in the document) and which party is considered responsible for identifying a violation of the SLA. May be defined in the SLA itself.	Feedback provided to WP2. State of the art on monitoring is presented in Deliverable 2.2
	Penalties and rewards should be part of the SLA (and included in the SLA template)	To be further analysed by Task 2.2
	I don't understand the meaning of the "SLA Change Notifications" requirement.	Feedback provided to WP2, and this requirement will be further explained in Deliverables 2.2 and 2.3
	Unilateral change of the SLA should not be possible otherwise we would not need to create an SLA. This element seems superfluous.	Feedback provided to WP2 and WP4. This is a common state of practice. Some CSPs may have a different mechanism (to be further analyzed by Deliverables 2.3 and 4.2).
	I don't understand the meaning of SLA Transparency; does it refer to a common understanding of the attributes (which I think is essential)?	Feedback provided to WP2. The CRM requirement has been rephrased (it was referring to the specification of applicable SLO metrics). The common understanding of attributes will be reported in Deliverable 2.2

5 Communicating the value of standards

SLA-Ready is driving a common understanding of Service Level Agreements with greater standardisation and transparency so firms can make an informed decision on what services to use, what to expect and what to trust. The use of standardised Cloud SLAs can be critical step towards better understanding the level of security and data protection offered by the Cloud Service Providers (CSP), and for monitoring the CSP's performance and security levels.

As outlined in D4.1 (Communication & outreach strategy) and D4.2 (SLA-Ready hub & social marketplace), outreach activities and the SLA-Ready marketplace will include content designed specifically to make SLAs more understandable in the private sector and will support decision making during the entire SLA lifecycle. Standards are promoted on the marketplace with information and access to SLA-related initiatives; tutorials focussing on practical advice on which standards to use; and success stories highlighting the benefit of its usage. Next are shown examples of messaging promoting the use of standards as outlined in D4.1

The value of metrics for CSPs

The importance for metrics that can be used in Cloud computing cannot be understated. Developing metrics that are reliable, repeatable and measureable are timely considering the continued growth in Cloud computing and market forces. Ultimately, these metrics will result in Cloud computing being bought & sold in a confident and trustworthy manner that will add to additional growth. Reliable & trusted Cloud metrics give a Cloud provider additional marketing and business tools which allow them to set themselves apart from the competition.

From Robert Bohn's, NIST, Cloudscape VII Insights paper[37]

Wanted: An international standard for Cloud privacy

Enterprise customers around the world want an international standard for Cloud privacy. Now there is one, and Cloud providers are starting to recognize its value to their customers. It's known as ISO/IEC 27018, and it was developed by the International Organization for Standardization (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the Cloud.

37 Please refer to http://www.sla-ready.eu/news/towards-common-metrics-slas

6 Conclusions

This deliverable has presented the Year 1 progress on standardisation, international collaboration and feedback from the Advisory Board. From a standardisation perspective, SLA-Ready has followed an orchestration strategy (described in Deliverable 3.1) to monitor, contribute and also receive feedback from relevant initiatives (including, but not limited to ISO/IEC 19086). In order to guarantee both timeliness and quality of the provided contributions, SLA-Ready has improved its approach to standardisation approach. This report also summarised the achieved standardisation results (i.e., contributions and analysis of relevant initiatives), which can be summarised and prioritised as follows:

1. Contributions to ISO/IEC 19086, in particular to Part 1 and Part 4 in order to align with both life cycle and Common Reference Model (WP2).
2. Feedback to ETSI CSC Phase II related to the report on Interoperability and Security. SLA-Ready inputs highlighted the importance of standards like the ISO/IEC 19086 family, and the need for machine-readable SLAs.
3. Contributions to CSA working groups, in particular CloudTrust, with inputs related to the SLA components identified in WP2.

From an international collaboration perspective, this report described the synergies established by SLA-Ready with Cloud SLA-related initiatives taking place outside Europe. Chief among these, is the past and on-going collaboration with NIST in the US, collaboration with Brazilian organisations, as well as collaboration with SLA-Ready's Advisory Board.

Particular emphasis during the rest of SLA-Ready will be put on ISO/IEC 19086-Part 3, which will document the "core requirements" for Cloud SLAs based on ISO/IEC 19086-Part 1. SLA-Ready will seek to align those requirements in order to make them useful for European SMEs.

Results from activities in WP3 are feeding into WP2 and WP4 in order to refine and validate outcomes like the Common Reference Model, and provide information on standardisation which can be used for the SLA-Ready website and digital marketplace respectively.

Two follow-ups of this report will focus on 1) **Business Guide to SLAs – How to be a well-advised user of Cloud services** (D3.3) and 2) **High-level Report on Cloud SLA Recommendations** (D3.4). Both reports are expected to present the progress on standardisation activities (D3.2) from a SME-friendly perspective. For example, the Business Report will illustrate the practical guides especially for small firms created for the service-oriented marketplace, with a user-friendly guide to SLA-Ready's standardisation and collaboration activities, and insights into what they mean to Cloud

service customers. Also, the high-level report will provide a more policy oriented intervention from the AB experts from different communities with the aim of delivering an objective report to the EC, including recommendations for a research roadmap.

Annex 1. Contributions to ISO/IEC 19086-Part 1 (current draft)

This annex presents the contributions presented by members of the SLA-Ready consortium during the ISO/IEC JTC 1/SC38 meeting that took place in Ireland (October-2015).

CSA 01		3		Ge	The notes associated with terminology are not in compliance with ISO directives.	Use "Note x to entry:" instead of "NOTE" or other forms.	
					Currently the definition of SLO mixes the measurable and the verifiable. Splitting these into two separate definitions clarifies what can actually be measured with metrics and what is verified through documentation. Suggested definitions are given for both.	SLO definition A commitment from the Cloud Service Provider made to a specific, quantitative characteristic of a Cloud service, where the value follows the interval or ratio scale (ISO 3534-2)	
					Suggested definition for Service Quality Objective	SQO definition A commitment from the Cloud Service Provider made to a specific, qualitative characteristic of a Cloud service, where the value follows the nominal or ordinal scale (ISO 3534-2)	
CSA 03	n/a	3		Te	In order to be consistent with the test under “8.3 Service Levels”, it is necessary to add a new definition called “service level”.	Please add the following definition as a new item under 3 “service level measurement result for specific service level objective of the Cloud service"	
CSA 05	53	3.5	NOTE 2	Ed	In the current text: “NOTE 2 - A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific objective. ” it is not clear the use of the term “objective”.	In NOTE 2, if the term “objective” refers to the actual entity being assessed, then it should be changed to “component”: “Note 2 to entry: A metric is to be applied in practice within a given context that requires specific properties to be measured, at a given time(s) for a specific component.” If by the contrary, the term “objective” is used as a synonym for “goal,” then no change is needed.	
CSA 06	n/a	3	n/a	Te	In order to be consistent with CSA’s proposed changes to this document, it is necessary to add the concept of “Accountability”.	Please add the following definition: “Accountability	

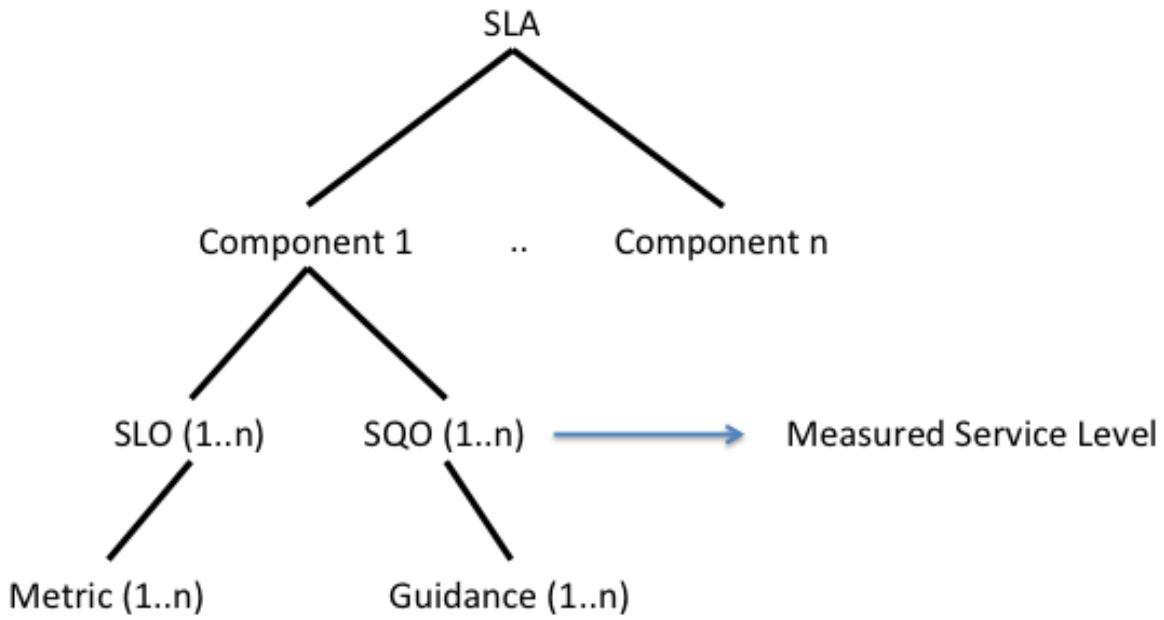
						state of accepting allocated responsibilities, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly. Note 1 to entry: Responsibilities may be derived from law, social norms, agreements, organizational values and ethical obligations."	
CSA 09	210	7.1		Te	The currently described Cloud SLA management life cycle is missing the negotiation stage.	Please change the following text: "Cloud SLA management covers the issues related to Cloud SLA design, evaluation and acceptance, implementation and execution and changes to the Cloud SLA. Cloud service customers should ensure that Cloud SLAs and other governing documents align with their business cases and overall strategy." To: *"Cloud SLA management covers the issues related to Cloud SLA design, evaluation and acceptance (including negotiation), implementation and execution and changes to the Cloud SLA. Cloud service customers should ensure that Cloud SLAs and other governing documents align with their business cases and overall strategy."*	
CSA 10	251	7.3	2	Te	Within the explanation of "Evaluation and Acceptance" the notion of Cloud SLA negotiation is missing.	Please add the following text just after finishing the current line 251: *"In Cloud computing business, there is interest in dynamically negotiated (electronic) SLAs. In particular negotiation of the terms for the Cloud service (if the Cloud service provider permits variable terms for the service), or selection among market offerings based on offered SLAs. Only if the Cloud service provider permits variable terms for the service, then the customer might need to specify additional requirements (including security and privacy) for the provider to implement."*	
CSA 13	n/a	8.1		Te	The notion of "evidence" is quite related to most of the elements comprising a Cloud SLAs. The	Please add the following text about "evidence" just the last paragraph in Clause 8.1:	

					current document does not elaborate about "evidence". Since evidence is an overused term with multiple meanings we are suggesting using the term documentation.	*"The CSP should also specify what forms of documentation can be provided in order to demonstrate that SLOs are being met or not. Systems and mechanisms should be put in place so that documentation can be presented not only when violations to the agreement occur, but also at any time upon request during regular service operation. Provision of documentation characterizes an accountability-based approach. Forms the documentation can take include audit reports, logs, attestations, certifications and, more in general, any technical proof that can be used to verify that the service is operating properly."*	
CSA 15	n/a	8.3.1		Te	The relationship between SLOs/SQOs and the documentation is not clarified in the current text. Service Level Objectives and SQOs contribute to Cloud accountability, and can be used as documentation for transparency, audit and redress, and remedies.	Please add the following text just after the last paragraph in suggested Clause 8.5 Service Quantitative Objectives: *"Service level objectives and service quantitative objectives also provide an element of accountability. They give transparency to the Cloud customer of what to expect as a service level and they give clarity to the Cloud service provider as to the service level it should deliver. For this reason, SLOs and SQOs can be used in various ways to provide documentation of the service performance. They can be used to audit and verity the measured service level; and they can be used to indicate that the Cloud service is achieving the required level of performance or not. They can provide documentation that remedy or redress is required."*	
CSA 16	n/a	10.8		Te	The relationship between the Cloud Service Support component and accountability is not clear in the current text.	Please add the following text just after the last paragraph in Clause 10.8.2: *"The Cloud service provider can provide that it will respond to a service failure within a certain time frame and by following a certain process for keeping the customer informed in a timely way of breaches. It can also provide that it will keep the customer informed of measures to repair or remedy the breach. Remedy can mean all efforts to alleviate any harm caused by a breach, for example, retrieval of lost data. "*	

CSA 19	801	10.9.2		Te	The Relevance clause of the Governance component is not clarifying its relationship to accountability.	Please add the following text at the begining of Clause 10.9.2: *"As Cloud providers are moving towards an accountable governance of the service provision, SLA could also be used to ensure proper implementation of accountability approach. Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly. An accountable approach requires including statements about the type of mechanisms used to provide evidence that governance is being managed as stated."*	
CSA 20	953	10.11.1		Te	The General clause of the Data Management component is not clarifying its relationship to accountability.	Please append the following text: *"In the context of accountability for the handling of personal or confidential data in the Cloud, accountability for an organization consists of accepting responsibility for data with which it is entrusted in a Cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties)."* To the paragraph: *"Multiple issues relate to Cloud service customer data including confidentiality, portability, deletion, retention, regulation, law enforcement access and geographic location. "*	
	145	5		ed	Reword last part of sentence to "a specific Cloud SLA" to make it more readable.	Reword fromj *"with specific Cloud SLAs* *To* *A specific Cloud SLA*	
	361	9.2.1		ed	Replace "might" with "may" for clarity	Replace "might" with "may".	

Appendix A.

In order to clarify the relationship among Component, SL, SLO, SQOs, Metrics and Assessment Guidance we recommend adding the following figure to Clause 9.1



Annex 2. Expert feedback provided to ISO/IEC 19086-Part 2 (metrics ad-hoc group)

This annex presents an example of a security metric documented by SLA-Ready with one of the templates being proposed for standardization in ISO/IEC 19086-Part 2. This material is part of the discussions taking place within the corresponding ad-hoc group, where CSA participates.

[AMD_CryptoStrength]
Abstract Metric Definition

Abstract Metric

name: Cryptographic strength of a Cloud resource
referenceId: AMD_CryptoStrength
unit: Security Levels (1 ... 8)
scale: Ordinal - Qualitative
expression: The cryptographic strength (security level) is computed based on the security bits associated to the Cloud resource. For this purpose is used the ECRYPT II mapping[38] shown in following table:

Security Level	Security bits (symmetric equivalent)
1	32
2	64
3	72
4	80
5	96
6	112
7	128
8	256

For computing the "Security bits" associated to the Cloud resource under evaluation, please refer to the underlying abstract metric definition below.

definition: expresses the strength of a cryptographic protection applied to a resource based on its key

[38] ECRYPT II recommended key sizes (symmetric equivalent), please refer to Table 7.4 in http://www.ecrypt.eu.org/documents/D.SPA.20.pdf

length, using the ECRYPT II security level recommendations for encryption. 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.

note: This metric is related to C-SIG SLA standardization guidelines' CR-1 (Cryptographic brute force resistance) SLO.

Abstract Metric Rule Definitions

name: Assessment method.
referenceId: AMR_Assessment_CryptoStrength
definition: This rule defines how to assess/measure the strength of the cryptographic mechanism. Each assessment method can be associated with a different level of assurance.
note: A Concrete Metric MUST specify the assessment method.

Abstract Metric Parameter Definitions

name: Security Bits (Symmetric Equivalent)
referenceId: AMP_SecurityBits
definition: This parameter refers to the "security bits" associated to the cryptographic mechanism under evaluation.
Note: Please refer to the parameters definition provided by AMD_SymmetricEquivalent

underlyingAbstractMetrics

name: Symmetric Equivalent
referenceId: AMD_SymmetricEquivalent

Annex 3. Contributions to ISO/IEC 19086-Part 4 (current draft)

This annex shows the overall CSA contribution to ISO/IEC 19086 Part 4, including SLA-Ready's work on security properties as a joint collaboration with EU FP7 CUMULUS.

ID	Original text	Proposed text
CSA01	Relevant security commitments are missing	Please add the security commitments referenced below.

6. Security Components

6.1. Security Policy

6.2. Organisation of Information Security

6.2.1. Service Commitments

6.2.1.1. Privacy Program Updates

The frequency of updates of the privacy program, policies and procedures by a competent role (e.g. Data Protection Officer (DPO)), for a given period of time.

6.2.1.2. Rank of Responsibility for Privacy

Numerical description of the level within the organization hierarchy, where the person responsible for privacy is located.

6.3. Human Resources Security

6.3.1. Service Commitments

6.3.1.1. Certification of acceptance of responsibility

Percentage of employees who have certified their acceptance of responsibilities for activities that involve handling of private data.

6.3.1.2. Frequency of certifications

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

6.4. Asset Management

6.4.1. Service Commitments

6.5. Access Control

6.5.1. Service Commitments

6.5.1.1. User authentication and identity assurance level

This service commitment measures the Level of Assurance (LoA) of the mechanism used to authenticate a user accessing a resource. The LoA can be 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).

6.5.1.2. User Access Storage Protection

This service commitment describes the mechanisms used to protect Cloud service user access credentials.

6.6. Cryptography

6.6.1. Service Commitments

6.6.1.1. Cryptographic Brute Force Resistance

This service commitment expresses the strength of a cryptographic protection applied to a resource based on its key length, for example using the ECRYPT II security level recommendations or the FIPS security levels for encryption. 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.

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.

6.6.1.2. Key Exposure Level

Indication of the level of confidentiality afforded to cryptographic secrets, from a Cloud client point of view. The possible levels are:

* 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.

6.6.1.3. Cryptographic hardware module protection level

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

6.7. Physical and Environmental Security

6.7.1. Service Commitments

6.8. Operations Security

6.8.1. Service Commitments

6.8.1.1. 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. The possible levels are:

* 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.

6.8.1.2. Log Unalterability

Indication of the level of protection of the log management systems against tampering. The possible levels are:

* Level 0 – No integrity mechanisms are in place.

* Level 1 – Log integrity is protected only by access control measures.

* Level 2 – Cryptographic mechanisms are in place for guaranteeing log unalterability or WORM (Write Once Read Many) devices are used.

6.8.1.3. Percentage of timely vulnerability corrections

Description of the number of vulnerability corrections performed by the Cloud service provider and is represented as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the Cloud service which are reported within a predefined period (i.e. month, week, year, etc.).

6.8.1.4. Percentage of timely Cloud service change notifications

Described the number of change notifications made within a specified period of time over the total number of change notifications, expressed as a percentage.

6.8.1.5. Reports of vulnerability corrections

Describes the mechanism by which the Cloud service provider informs the customer of vulnerability corrections applied to the provider's systems, including the frequency of the reports.

6.8.1.6. Logging and monitoring

Specify the period of time during which logs are available for analysis (e.g. the period of time that log files are available for use by the Cloud service customer).

6.8.1.7. Cloud service change reporting notifications

Describes the type of change (such as SLA change or functional change), mechanism and period for the Cloud service provider to notify Cloud service customers of planned changes to the Cloud service.

6.9. Communications Security

6.10. Systems Acquisition, Development and Maintenance

6.11. Supplier Relationships

6.12. Information Security Incident Management

6.12.1. Service Commitments

6.12.1.1. 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. This is 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.).

6.12.1.2. 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. This is 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).

6.12.1.3. Percentage of timely incident resolutions

This service commitment describes the percentage of defined incidents against the Cloud service that are resolved within a predefined time limit after discovery

6.12.1.4. Number of privacy incidents

Number of privacy incidents and breaches that have occurred in a given period of time.

6.12.1.5. Coverage of incident notifications

Percentage of privacy incidents and breaches for which affected stakeholders were notified, for a given period of time.

6.12.1.6. Type of incident notification

Description of the quality of the notification procedures after a privacy incident or breach. The possible levels are:

* 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.

6.12.1.7. Privacy incidents caused by third parties

Number of privacy incidents caused by a third party to whom personal information was transferred (i.e. Data Processors), for a given period of time.

6.12.1.8. Incidents with damages

Number of incidents that end up with compensatory or punitive damages, for a given period of time.

6.13. Business Continuity Management

6.13.1. Service Commitments

6.13.1.1. 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.

6.13.1.2. 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.

6.13.1.3. Level of Redundancy

This service commitment describes the level of redundancy of the Cloud service supply chain, possibly taking into account the percentage of the components or service that have fail over mechanism. Redundancy varies also on the type of Cloud service provided (IaaS versus SaaS for example)).

6.13.1.4. Service Reliability

This service commitment describes the ability of the Cloud service to perform its function correctly and without failure over some specified period.

6.14. Compliance

6.14.1. Service Commitments

6.14.1.1. Certificates

This service commitment refers to a list of certifications held by the Cloud service provider for a Cloud service, including the certifying body, the expiration date of each certification and the renewal period.

6.14.1.2. Number of privacy audits received

Number of independent audits, reviews and/or assessments performed to the privacy program, policies and procedures in place for complying with applicable contractual and regulatory obligations, for a given period of time.

6.14.1.3. Successful audits received

Percentage of successful independent audits, reviews and/or assessments performed to the policies and procedures in place for complying with applicable contractual and regulatory obligations, for a given period of time.

Annex 4. Contributions to ETSI CSC Phase II

This annex presents the full feedback provided by CSA to ETSI CSC Phase II (Security and Interoperability), including SLA-Ready's on Cloud SLAs.

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
Cloud Security Alliance	1	99	Technical	The following text: "…increase the level of trust in Cloud Computing" does not consider that also the level of transparency can increase thanks to both interoperability and security assurance.	Please change the following text: "…increase the level of trust in Cloud Computing" to: "…increase the level of trust and transparency in Cloud Computing"
Cloud Security Alliance	5.2.4	572-578	Editorial	The entire paragraph is not clear. Please clarify and rephrase.	The entire paragraph is not clear. Please clarify and rephrase.
Cloud Security Alliance	5.2.4	623	Technical	The statement: "The well-‐known IT certifications such as ISO 27001, SSAE16 are not that helpful, as they do not cover the Cloud specific requirements in all aspects.." is not correct and it contradicts with the result of your survey.	Please amend the statement taking into account the results of the your survey
Cloud Security Alliance	5.2.5	ALL	Technical	The scenario 5 doesn't mention at all the concept of "containers".	Please update the scenario including the concept of containers
Cloud Security Alliance	5.2.7	837-853	Technical	The conclusion and remarks of this scenario do not provide any guidance on standard. It just highlights a eventual risk that might surface IF/WHEN the new GDPR will enter into force. Since the scenario is about the rather well know issue of privacy compliance in the Cloud.	We suggest to focus on existing national laws and directive and provide guidance about those e.g. by referring to what exist both in terms of rules and in term of solutions (EC C-SIG Code of Conduct, CSA Privacy Level Agreement v2.)
Cloud Security Alliance	5.2.7	810	Editorial	The "High-Level Requirements" in this scenario are not presented as in previous scenarios i.e., organized by core concepts.	Please present these requirements organized in core concepts.
Cloud Security Alliance	5.2.7	811	Technical	The reference to the "new data protection directive" is misleading. What are you referring to? The new PROPOSED draft of the General Data Protection Regulation (GDPR)? If that correct and you are referring to the GDPR then please note that is not finalised yet and you cannot refer to imaginary requirements.	There's no proposed change. Please clarify and fix the mistake.
Cloud Security Alliance	5.2.7	845	Editorial	The text "Some of the major players in Cloud Computing (…) have already warned that the new EU Data Protection regulation will "kill Cloud Computing" within Europe." is unreferenced, vague (i.e. "some major players") and unverifiable claims. The EU position that follows in the next sentence would also benefit from a reference.s	Provide a citation/reference.

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
Cloud Security Alliance	5.2.8	865	Editorial	The "High-Level Requirements" in this scenario are not presented as in previous scenarios i.e., organized by core concepts.	Please present these requirements organized in core concepts.
Cloud Security Alliance	6	615	Technical	You refer to Cloud Customer as owner of the data. What do you mean? The owner of the personal data is normally the "data subject" which is normally the end-user of a Cloud customer.	Please correct the reference to the data owner.
Cloud Security Alliance	6.1.3	974-1083	Technical	The terminology used doesn't seem to be consistent with widespread information security literature. Concepts like confidentiality and trust are mixed together as well as privacy and integrity as well as privacy and security. Moreover several import information security domains are not considered at all, e.g. incident management, business continuity / disaster recovery, mobile security.	We suggest the editor to rework this chapter and use appropriate references to existing literature to avoid possible misunderstandings.
Cloud Security Alliance	6.1.3	990-991	Technical	The sentence says: "An Initiative that addresses transparency and accountability is the program from Cloud Security Alliance (CSA), "Security, Trust & Assurance Registry (STAR), where CSPs can register and have their offerings ranked." The CSA STAR is the name of the transparency and certification program of CSA, is not a place where Cloud offerings are ranked.	Please rephrase as follows: "The Cloud Security Alliance (CSA) maintains the Security, Trust & Assurance Registry (STAR) which is a public repository where CSPs can voluntarily publish the result of their assessment based on CSA CCM/ and ISO27001-2013 or AICPA SOC2. CSPs can submit both the results of their Self Assessment and third party based assessment (i.e. CSA STAR Certification and CSA STAR Attestation) in the registry"
Cloud Security Alliance	6.1.3	1036	Technical	Presenting "Privacy" as an area under "Security" may be misleading.	Please move "Privacy" (lines 1036 – 1046) to a new subsection 6.1.x
Cloud Security Alliance	6.1.3 and all the	1036	Technical	This section and the document in general use "information privacy" and "data protection" as	Review definitions of privacy and security, and refer to standard definitions of these terms where appropriate

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
	doc			equivalent terms. This is generally incorrect, especially in Europe. Data privacy relates to the confidentiality of data, or the ability/inability to link information to individuals. Data protection deals with much more than protecting the confidentiality of data, it also encompasses, among other things: - The rights of individuals to access their data / rectify / modify it. - The principle of purpose limitation. - The principle of retention limitation. - Data minimization and anonymization. - International data transfer rules. - Data security (confidentiality, integrity and availability). - Etc. All these elements require specific attention in the Cloud.	(see Directive 95/46/EC for a description of data protection). See also other comments related to privacy and security.
Cloud Security Alliance	6.1.3 and all the doc	1075	Technical	The document frequently bundles together the notion of privacy and data integrity (this is also the case in the survey). This is an odd choice that is likely to confuse readers and experts in the field. In information security, integrity describes the "means to protect the accuracy and completeness of information and the methods that are used to process and manage it" (ISO 27000). Integrity is a distinct notion from privacy altogether. Integrity, confidentiality and availability are usually described as the 3 pillars supporting information security. The frequent association of "integrity" and "privacy" throughout the documents seems unjustified (e.g. why exclude "confidentiality"?)	Review terminology to make it aligned with common use in information security and data protection.
Cloud Security Alliance	7	1178-1232	Technical	It is unclear why the standards have been categorised as described in this chapter. Someone would have expected to find standards categories according for instance to the core concept: Interoperability, portability, security, SLA, instead, Interoperability and portability are listed under Security and Cloud SLA falls into the other standard category. We suggest using a more appropriate way to classify standards.	We suggest using a more appropriate way to classify standards. Since this would need a major rework it has to be the main editor to do it.
Cloud Security Alliance	7	1178	Technical	Very few relevant standards between the relevant	There are major changes to be made in this chapter: 1)

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
				ones are mentioned. Several standards used in the Cloud security space and also included in the previous ETSI effort are left out of this this list. There are major changes to be made in this chapter: 1) provide a justification of on which ground you have selectively chosen some standards vs others and 2) include those Cloud security standards that cannot be left out: e.g. NIST, CSA and BSI standards	provide a justification of on which ground you have selectively chosen some standards vs others and 2) include those Cloud security standards that cannot be left out: e.g. NIST, CSA and BSI standards. Since this is major change in the context of this document it should be the editorial team / main authors to rework the chapter.
Cloud Security Alliance	7.1	ALL	Technical	Several information security standards missing	Please add at least relevant Standards from NIST and German BSI.
Cloud Security Alliance	7.2	1192-1196	Technical	It is unclear why you are adopting such a granular distinction between Authentication and Authorization standards, especially since you are mentioning only 1 standard / category	Please merge Authentication and Authorization under the label: Identify and Access Management
Cloud Security Alliance	7.2	1192-1196	Technical	Missing standards	Please add other relevant standards, e.g. • ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts • ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements, ISO/IEC WD 24760-3 A Framework for Identity Management—Part 2: Practice • ISO/IEC 29115 Entity Authentication Assurance • ISO/IEC WD 29146 A framework for access management • ISO/IEC WD 29003 Identity Proofing and Verification • etc.
Cloud Security Alliance	7.2	1191	General	Categorising “Privacy” under “Security” may be misleading.	Please add a new subsection “7.x Privacy” containing all items starting on line 1208.
Cloud Security Alliance	7.2	1191	Editorial /Technical	Do you refer to Cloud Specific Standards or Topic Specific topic or both? It would be worth specifying.	Please clarify
Cloud Security Alliance	7.2	1205	Technical	Missing several standards from CSA and NIST	Please add CSA CCM, CSA CAIQ, CSA CTP, CSA Cloud Audit, CSA Enterprise Architecture, and NIST standards / special publications (http://csrc.nist.gov/publications/PubsSPs.html)
Cloud Security Alliance	7.2	1207	Technical	On the list of references standards is missing the published CSA “Privacy Level Agreement – version 2” (https://cloudsecurityalliance.org/download/privacy-level-agreement-version-2/)	Please add the following to the list (after line 1213): “CSA PLA (Privacy Level Agreement)”
Cloud Security Alliance	7.2	1207	Technical	Missing standards	Please add CSA Privacy Level Agreement v2

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
Cloud Security Alliance	7.3	1216-1220	Technical	Very relevant security and Cloud certification standards are missing. For instance: FedRAMP (especially important for the Public Sector audience), AICPA SOC 1-2-3	Please add FedRAMP AICPA SOC 1-2-3
Cloud Security Alliance	7.3	1218	Editorial	The following entry has an error: "CSA OSF Level 2"	Please correct to: "CSA STAR Certification Level 2"
Cloud Security Alliance	7.3	1218	Technical	This section only lists one of the applicable certification schemes related to CSA STAR.	Please add the full list of CSA STAR certifications: "CSA STAR Self Assessment - Level 1 CSA STAR Certification - Level 2 CSA STAR Attestation - Level 2"
Cloud Security Alliance	7.3	1218	Technical	The reference to CSA certification standards is completely wrong. The Open Certification Framework (OCF) Working Group (not OSF) is the technical WG that oversees the CSA certification effort (a parallel would OCF WG vs ISO SC27). The CSA STAR is the name of the overall certification program. The names of the CSA certification standards are: • CSA STAR Certification (ISO27001+CCM) • CSA STAR Attestation (SOC2+CCM) • CSA C-STAR (Chinese equivalent of ISO27001+CCM) • CSA Self Assessment We would recommend you consult the ENISA or CSA web sites: https://resilience.enisa.europa.eu/Cloud-computing-certification https://cloudsecurityalliance.org/star/	Please replace CSA OSF level 2 with: • CSA STAR Certification (ISO27001+CCM) • CSA STAR Attestation (SOC2+CCM) • CSA C-STAR (Chinese equivalent of ISO27001+CCM) • CSA Self Assessment
Cloud Security Alliance	7.4	1222-1232	Technical	Several reference to standards are not accurate: COBIT? Which version ITIL ditto, ISO 19086, which part? 1-2-3-4	Please add appropriate references to standards
Cloud Security Alliance	8	1234-1283	Technical	There is no analysis result in this document to support the conclusion and recommendations.	Please substantiate the statements in the conclusion with facts/ results of the analysis
Cloud Security Alliance	8	1243	Technical	The current text seems to imply that identified interoperability and security gaps will be covered with an "enough" number of standards and certifications. This may be misleading, taking into account that the CSC may be unaware of which standards and certification are really needed to fulfil his security and privacy requirements.	Please add the following text at line 1249: "Despite the undisputed advantages of Cloud computing, customers (in particular small and medium enterprises – SMEs) are still in need of "meaningful" understanding of the security and privacy changes that the Cloud entails, in order to assess if this new computing paradigm is "good enough" for their security requirements. Cloud-specific risk management

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
					frameworks are conspicuously missing at the state of the art, and are needed to empower CSC with information related to the levels of security and privacy that are required in their own contexts."
Cloud Security Alliance	8	1243	Technical	Despite being identified in the first ETSI CSC report, there is no mention to the existing gap in standards related to machine-readable specifications, for example in the area of CSLA.	Please add the following text at the end of the "Outstanding gaps" subsection: "Standardised machine-readable specifications are required to improve both interoperability and security in Cloud computing, in particular related to the adoption of realistic levels of automation in areas like CSLA management."
Cloud Security Alliance	8	1266	Technical	The following text: "The same need can be applied to certifications; well-structured and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the CSCs confidence in the Cloud. " Misses the fact that the (security) assurance provided by certification schemes strongly depends on the periodicity of the assessment, where continuous (security) certification for the Cloud is a topic that appears on novel schemes like CSA STAR Level 3 Continuous.	Please change the following text: "The same need can be applied to certifications; well-structured and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the CSCs confidence in the Cloud. " To: "The same need can be applied to certifications; well-structured, continuous and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the CSCs confidence in the Cloud. "
Cloud Security Alliance	8	1272	Editorial	The following text: "The relevance and potential high-value use of the upcoming framework for Cloud SLA must also be mentioned as part…" Does not clarify to which "upcoming framework for Cloud SLA" it refers.	Specify the referenced framework (supposedly ISO/IEC 19086?).
Cloud Security Alliance	8	1275	Technical	The following text: "Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report." Does not highlight the relevance of Cloud SLA metrics, in particular for security and privacy (as highlighted in ISO/IEC 19086-P4).	Please change the text: "Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report." To: "Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture

Organisation	Section	Line Number	Comment Type General, Technical Editorial	Comments	Proposed change
					along with the definition of security/privacy metrics, will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report.”
Cloud Security Alliance	ANNEX A	1299	Technical	Several references are missing from the Bibliography	Please add missing references