CLOUD ACCOUNTABILITY PROJECT

D15.2 Report on A4Cloud contribution to standards (Final)

Deliverable Number	D15.2
Work Package	WP 15
Version	Final
Deliverable Lead Organisation	CSA
Dissemination Level	PU
Contractual Date of Delivery (release)	31/03/2016
Date of Delivery	31/03/2016

Editor

Jesus Luna (CSA)

Contributors

Vasilis Tountopoulos (ATC), Daniele Catteddu (CSA), Jean-Claude Royer (EMN), Michela D'Errico (HPE), Frederic Gittler (HPE)

Reviewers

Anderson Santana de Oliveira (SAP), Martin Gilje Jaatun (SINTEF)

Executive Summary

During the whole duration of A4Cloud, a core activity has been related to engaging with relevant standardization bodies and actively influencing the initiatives related to the project's areas of interest. We refer in particular to the areas of Service Level Agreements, Assessment and Certification, Risk Management and Privacy Impact Assessment.

Beyond Standardization Development Organizations (SDOs), A4Cloud also acknowledges the importance and impact of best practices and other relevant industrial initiatives on the topic of accountability, for example, Cloud Security Alliance's Privacy Level Agreement and Open Certification Framework. The present deliverable represents the final report on the activities performed by A4Cloud targeting both SDOs and industrial/best-practices groups. This deliverable reports (i) the revised standardization strategy followed by the consortium, and (ii) a summary of A4Cloud's contributions to standards/best-practices. For each reported contribution, this deliverable presents the feedback received from the SDO/industrial working group and planned future activities on that particular initiative.

Finally, this deliverable also proposes a plan to guarantee the sustainability of the project's contributions to standards after A4Cloud's completion. The main elements of the proposed policy are related to continuing following the progress of the identified SDO/best practices initiatives, enhancing the industrial partners' standardization interests with those identified by A4Cloud, and maintaining an active presence also in identified SDO/best practices organizations.

Table of Contents

List of Figures

List of Tables

List of acronyms

Abbreviation	Meaning
AB	Advisory Board
CC	Cloud Customer
CD	Committee Draft (ISO/IEC)
CRMF	Cloud Adapted Risk Management Framework
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
NIST	National Institute of Standards and Technology
R&D	Research and Development
RTD	Research and Technological Development
SDO	Standards Development Organization
SLA	Service Level Agreement
SLO	Service Level Objectives
SME	Small and Medium-sized Enterprise
SSO	Standards Setting Organization
WD	Working Draft (ISO/IEC)
WG	Working Group
WP	Work Package

1 Introduction

In A4Cloud, standardization activities have been of benefit to the project to maximize its impact and supporting the dissemination and uptake of technical results even beyond its expected timeframe. Furthermore, standardization within A4Cloud have contributed to the exploitation potential of project outputs, and provided the consortium with access to a large pool of external/international expertise and valuable feedback. Contribution to standards have helped A4Cloud to build a competitive advantage and created the ability to design and validate relevant outcomes (e.g., conceptual framework, architecture, and metrics) according to internationally agreed principles. In addition, participating in standardization processes have brought higher international recognition to the project, and have provided new opportunities for collaboration.

This deliverable represents the final report on A4Cloud standardization activities. It summarizes a refined version of the project's standardization strategy, the contributions provided to relevant initiatives (including standards and industrial best practices) along with the respective feedback received from such interactions, and also develops a strategic approach to support the project's contributions to standards/best practices after its finalization.

1.1 Scope of the document

In analogy to the previous version of this deliverable (cf., Deliverable D:A-5.1) the present report documents the activities performed by A4Cloud's standardization work package (WP A5) during the final 24 months of the project, namely:

1. The development of a refined strategy developed to actively engage with relevant SDO/SSO and timely contribute to identified initiatives. This is aligned to task T:A-5.1 "Define the standards gap".
2. The actual contributions to identified SDOs/SSOs (i.e., in alignment with Task T:A-5.2 "Define and orchestrate and support standards activities"). This activity also included documenting the received feedback and the planning for future contributions (if any).
3. The creation of a sustainability strategy to continue the engagement with identified SDO/SSO initiatives after the finalization of the project.

1.2 Positioning of WP A5 and D:A-5.2 within the A4Cloud project

As presented in the previous version of this report, the standardization WP A5 plays two main roles within the A4Cloud project, as seen in Figure 1. On one hand, the blue arrow in the central part of Figure 1 represents that WP A5 is in charge of (i) identifying and prioritizing those standards that are leveraged by the rest of WPs, and (ii) orchestrating the contributions coming from A4Cloud to those relevant standardization initiatives. While the former activity requires WP A5 to be in constant contact with all the WP leaders in order to be aware of their standardization-specific requirements, the later actively uses WP A5 as a unique point of contact with the relevant SDOs (therefore optimizing and streamlining the actual orchestration of relevant contributions).

On the other hand, the red arrow in Figure 1 represents that WP A5 is constantly monitoring the standardization landscape in order to identify (i) new/incubator initiatives related to A4Cloud, and (ii) standards that might not have been originally considered by the WPs, but nevertheless are both relevant to the project and with an open commenting period. Once again, WP A5 is used by the rest of the WPs as a unique point of contact to be constantly updated about relevant standardization initiatives. The present report D:A-5.2 is build on top of its predecessor (D:A-5.1) by (i) enhancing the originally defined standardization strategy with a set of well-identified areas of interest where WP A5 efforts have been focused, (ii) following-up on some of the initiatives identified in D:A-5.1 (i.e., those which were still receiving inputs), and (iii) proposing an approach to support the project's sustainability through standardization.

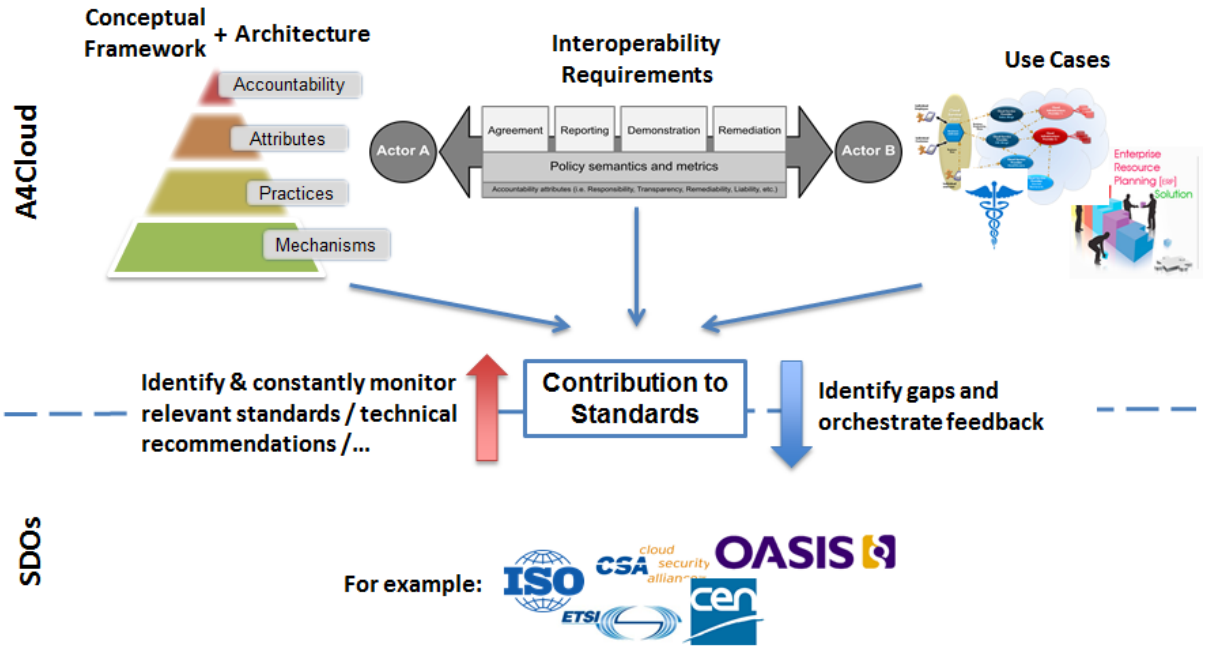

Figure 1. The role of standards in A4Cloud (D:A-5.1)

1.3 Outline of the document

The rest of this document is organized in the following manner:

- Section 2 discusses the revised standardization strategy, based on the one presented in Deliverable D:A-5.1
- Section 3 reports the actual performed contributions (from month 25 to month 42 of A4Cloud's duration), along with the received feedback and future plans for collaborations.
- Section 4 presents the developed sustainability strategy designed to support the project's contributions to identified SDOs/SSOs after its finalization.
- Finally, Section 5 summarizes the conclusions of this report.

2 Revised standardization strategy

This section presents the refined version of A4Cloud's standardization strategy, initially proposed in D:A-5.1, and revised in order to focus and resources during the second half of the project's duration. A4Cloud's standardization approach can be seen in Figure 2, where three different stages where orchestrated in order to refine the project's focus. During the first stage, the project analysed a group of baseline standards (122 in total) in order to perform a preliminary identification of those related to A4Cloud's topics of interest (based on the Description of Work). A second stage was then implemented to approach the WP leaders in order to refine and classify the baseline standards into three groups of entries namely complaint, leveraged and lack of standards. Finally, a third stage was in charge of continuously survey the SDO/SSO landscape in order to identify initiatives where timely contributions could be done.

The resulting set of observed standards/best practices, despite being more manageable than the original 122 entries, went through a second round of refinement to further focus efforts based on three main criteria:

1. Their *relevance* to any of A4Cloud's Areas of Interest based on the DoW.
2. The *opportunity* to contribute to the identified initiatives, taking into account existing liaisons with SDOs/SSOs and the timeliness of potential contributions.
3. A final criterion (*impact*) to quality both the degree of maturity associated with a potential contribution from A4Cloud, and the actual importance (from the standardization perspective) of such contribution.

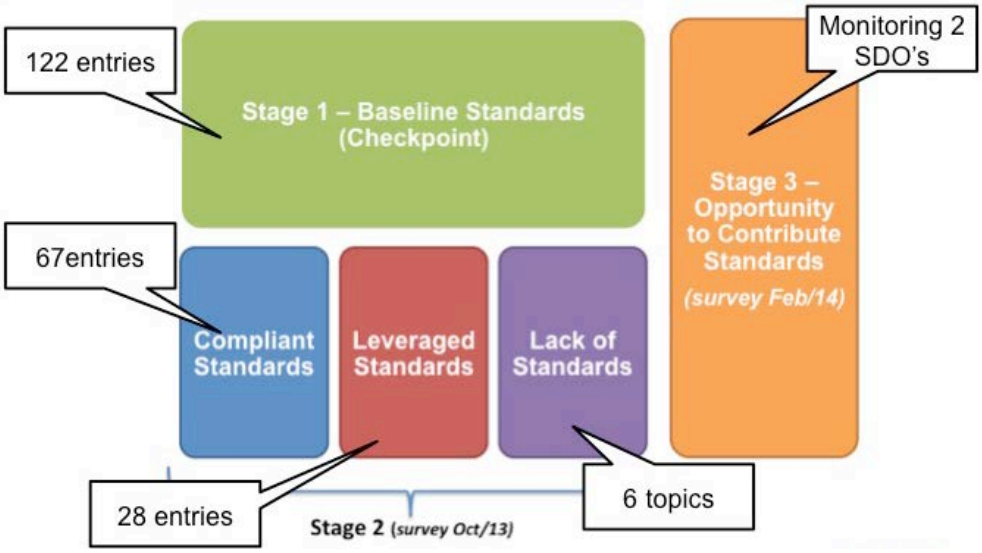

Figure 2. Standardization strategy at a glance.

The outcome of this revised strategy (i.e., Stage 3) was a subset of (7) identified standards/best practices, and two SDOs (ISO/IEC and NIST) being observed by WP A5 where A4Cloud contributions had the potential to impact on transparency and trust in the Cloud supply chain through SLA's, accountability assessment/certification, risk management, and privacy impact assessment. A summary of the identified A4Cloud areas of interest, potential contributions and the role of WP A5 can be observed in **Table 1**.

The following section summarizes the outcomes of the contributions to the identified set of SDO/SSO initiatives provided during the second half of the project duration.

Table 1. Outcome of refined standardisation strategy

Area	A4Cloud contributions	Main A5 focus
Service Level Agreements	• Linking to evidence. • Accountability policy representation (A-PPL). • Terminology, cloud SLA management. • Accountability SLO's.	• CSA Privacy Level Agreements • ISO/IEC 19086 Part I "Cloud computing – Service Level Agreement (SLA) Framework and Terminology" • ISO/IEC 19086 Part IV "Cloud computing – Service Level Agreement (SLA) Security and Privacy"
Assessment and Certification	• Accountability Maturity Model. • Accountability metrics. • Continuous (risk) monitoring.	• CSA Open Certification Framework • ISO/IEC 19086 Part II "Cloud computing – Service Level Agreement (SLA) Metrics"
Risk Management	• Contributions to the risk model. • Risk management/assessment.	• NIST 800-173.
Privacy Impact assessment (PIA)	• PIA and the accountability dimension. • Synergies with DPIAT. • Enable external auditing.	• ISO/IEC 29134 "Privacy impact assessment – Methodology".

3 Report on contribution to standards

This section summarizes the contributions of the A4Cloud consortium to relevant standardization initiatives and industrial best practices, which followed the strategic areas of interest documented in Deliverable A:5.1. For each contribution, this section reports the following information:

- A summary of the provided contribution referencing (when available) the submitted commenting form.
- The value that A4Cloud obtained from the provided contribution e.g., related to the enhancement of the project's technical outcomes.
- A summary of the feedback received from the relevant SDO/SSO.
- If any, the plans to contribute after the finalization of the project.

3.1 ISO/IEC 19086 – Cloud Service Level Agreements

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 (ISO/IEC 19086-1), metrics (ISO/IEC 19086-2), and core requirements (ISO/IEC 19086-3). Afterwards, during Q1/2015 ISOI/IEC SC27 approved a new working item on security and privacy SLAs as part of the 19086 series of standards (ISO/IEC 19086-4). In the previous version of this deliverable (D:A-5.1) A4Cloud contributions to both ISO/IEC 19086 Parts 1 and 2 were reported. The rest of this section reports the follow-up activities mainly related to ISO/IEC 19086 Part 1 and Part 4.

A4Cloud Contribution
In August 2015 the A4Cloud consortium provided a contribution to ISO/IEC 19086 Part 1, which covered the following topics:

- Differentiation between measurable Service Level Objectives (SLO), and verifiable Service Quantitative Objectives (SQO).
- The following definition of "accountability":
    - 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."
- Discussion on the notion of "evidence" and its relationship to the identified Cloud SLA components (including proposed SLOs and SQOs). Since "evidence" tends to be an overused term within ISO/IEC standards, it was decided to use instead the term "documentation".
- Clarification related to the relationship between the Cloud Service Support component and the notion of accountability.
- Discussion on the relationship between the Governance and Data Management components, and accountability.

Similarly, A4Cloud also contributed to ISO/IEC 19086 Part 4 for the SC27 meeting that took place in October 2015. This contribution focused on proposing the use of accountability metrics (as elicited by WP A5) within both the Security and Privacy components described in Part 4. Table 2 summarizes the proposed mapping between A4Cloud's accountability metrics and ISO/IEC 19086 Part 4's components.

Table 2. Summary of A4Cloud's contribution to ISO/IEC 19086 Part 4

ISO/IEC 19086-4 Component	A4Cloud Accountability Metric
Organization of Information Security	Privacy Program Updates (Metric 3), Rank of Responsibility for Privacy (Metric 21), Certification of acceptance of responsibility (Metric 22), Frequency of certifications (Metric 23)
Asset Management	Certification of acceptance of responsibility (Metric 22), Frequency of certifications (Metric 23)
Access Control	Identity Assurance (Metric 25), Mean time to revoke users (Metric 26)
Cryptography	Level of confidentiality (Metric 11), Key Exposure Level (Metric 12)
Physical and Environmental Security	Data Isolation Testing Level (Metric 13), Log Unalterability (Metric 24)

ISO/IEC 19086-4 Component	A4Cloud Accountability Metric
Operations Security	Data Isolation Testing Level (Metric 13), Log Unalterability (Metric 24)
Information Security Incident Management	Number of privacy incidents (Metric 30), Coverage of incident notifications (Metric 31), Type of incident notification (Metric 32), Privacy incidents caused by third parties (Metric 33), Incidents with damages (Metric 37)
Business Continuity Management	Number of Business Continuity Resilience (BCR) plans tested (Metric 34), Maximum tolerable period for disruption (MTPD) (Metric 35)
Compliance	Number of privacy audits received (Metric 5), Successful Audits received (Metric 6)
Consent and choice	Type of Consent (Metric 14)
Purpose legitimacy and specification	Type of notice (Metric 15)
Collection limitation	Record of Data Collection, Creation, and Update (Metric 7)
Use, retention and disclosure limitation	Record of Data Collection, Creation, and Update (Metric 7), Data classification (Metric 8)
Accuracy and quality	Data classification (Metric 8)
Openness, transparency and notice	Authorized collection of PII (Metric 1), Type of notice (Metric 15), Readibility (Flesch Reading Ease Test) (Metric 20)
Individual participation and access	Procedures for Data Subject Access Requests (Metric 16), Number of Data Subject Access Requests (Metric 17), Responded data subject access requests (Metric 18), Mean time for responding Data Subject Access Requests (Metric 19), Mean time to respond to complaints (Metric 27), Number of complaints (Metric 28), Reviewed complaints (Metric 29)
Accountability	Privacy Program Budget (Metric 2), Privacy Program Updates (Metric 3), Periodicity of Privacy Impact Assessments for Information Systems (Metric 4), Number of privacy audits received (Metric 5), Successful Audits received (Metric 6)
Privacy compliance	Privacy Program Budget (Metric 2), Privacy Program Updates (Metric 3)

Value for A4Cloud

As presented in the previous version of this report (Deliverable D:A-5.1), the topic of Cloud SLAs is within the strategic scope of A4Cloud. Contributions to ISO/IEC 19086 Parts 1 and 2 have occurred during the initial 24 months of the project duration, and this set of standards has had the continued interest of the consortium.

More specifically, the contributions provided to both Part 1 and Part 4 have had the following value for the project's activities during the period being reported:

- The contributions to ISO/IEC 19086 Part 1 have focused on creating awareness in the relationship between the notion of accountability and SLAs. From a project perspective, this contribution had a direct impact on the outcomes produced by WP:D-4 (Contracts, SLAs and remediation) and in particular related to the topic of guidelines and tools for cloud contracts. The proposed concept of "accountability" has been also fed into the work being done by WP:D-2 (Reference architecture).
- A4Cloud's contribution to ISO/IEC Part 4 is expected[1] to provide further industrial/expert validation of the developed set of accountability metrics. Conclusions of a preliminary discussion

1 At the time of writing this report, the disposition of comments related to ISO/IEC 19086-Part 4 was not

with the CSA International Standardisation Council were used to refine the metrics contribution to the WP:D-2 deliverables.

Received feedback
At the time of writing this report, the consortium had only received the disposition of comments related to the contributions provided to ISO/IEC 19086 Part 1. The accepted set of comments relate to the relationship between the service support component and accountability (which was accepted with minor changes). The rest of the comments were rejected because either (i) they overlapped with the accepted feedback from other contributors, or (ii) were considered within the scope of ISO/IEC 19086 Part 4.

Plans after the finalisation of the project
As of December 2015, 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. Furthermore, the DIS commenting period for Part 1 will conclude after the completion of A4Cloud. Therefore, the consortium will focus on revising the latest draft (when available), and contributing only if major issues are detected. For informative purposes, **Table 3** shows the current timeline associated to ISO/IEC 19086 Part 1.

Table 3. Stage history for ISO/IEC 19086 Part 1

Description	Target date
DIS registered	2015-12-21
DIS ballot initiated	2016-01-04
Close of voting	2016-04-05 (after A4Cloud finalization)
International Standard published	Q4/2016

With respect to ISO/IEC 19086 Part 2 (Metrics) and Part 3 (Core Requirements), in both cases the commenting period before the CD release closes in April 2016 and the consortium will focus efforts in the following:

1. Validate the conceptual models being proposed to ISO/IEC 19086 Part 2 with the accountability metrics elicited by A4Cloud (please refer to WP:C-5 deliverables).
2. Where feasible, refine the ISO/IEC 19086 Part 2 conceptual model by adding accountability-related components e.g., evidence.
3. Pursue the alignment of the outcomes from WP:D-4 (in particular recommended SLA models) to core requirements from ISO/IEC 19086 Part 3.

Finally, A4Cloud is planning to continue contributing to ISO/IEC 19086 Part 4 in particular related to refining the inputs from Table 2 based on the disposition of comments[2]. Depending on the agreed new structure of the draft, A4Cloud may also provide major contributions to the data protection components and requirements of the Cloud SLA.

Given the fact that contributions/follow-ups to ISO/IEC 19086 are expected after the finalization of the project, the consortium developed a policy to guarantee the sustainability of A4Cloud's standardization-related activities. More details will be presented in Section 4.

3.2 NIST CRMF

The Cloud Adapted Risk Management Framework (CRMF, NIST 800-173) has subtitle "*Guide for Applying the Risk Management Framework to Cloud-based Federal Information System".* Thus it is related to the activities of A4Cloud mainly with the risk and trust modeling work-package.

yet available.

2 At the time of writing this document, the disposition of comments related to ISO/IEC 19086 Part 4 has not been published yet.

A4Cloud Contribution
The interactions with NIST about CRMF leads to several points to discuss. One remark is that this document is focusing on security controls but A4Cloud can say more about privacy controls. It seems that a new future discussion and contribution could be possible on the dedicated document NIST 800-174 for cloud privacy controls (adaptation of NIST 800-53).

The main task was to provide some comments and suggestions resulting from the C6 work-package on risk management. The current draft (January 2015) is a draft for a guide on adapting the risk management framework (SP 800-37) to the to cloud based federated systems.

A first suggestion was to use the Cloud Adoption Risk Assessment Model (CARAM) [1] for helping cloud consumers to perform security risk and assessment, since no specific method was suggested. CARAM is an expert system dedicated to the analysis of which controls from a given security standard (e.g. FedRamp or CSA CCM) are implemented by a cloud provider, and to assess risk according to the cloud consumer assets (i.e., its profile).

A second point is related to trust boundaries which are not aligned with the risk management process. Thus the document should clarify how these boundaries arise from a use case and how they are used in the risk management framework.

The main bulk was to amend the step 4 and step 6 of the risk life cycle, the global process performed by CRMF.

Step 4: This step a cloud consumer can assess and research cloud solutions.

Step 6: This step is dedicated to monitoring the security controls of the cloud vendors.

Our collaboration with NIST could be a first step in the submission of comments for the Cloud Risk Management proposal at ISO (ISO/IEC JTC 1/SC 27).

Value for A4Cloud
Of course the first value for A4Cloud is to disseminate its results mainly the principles behind the CARAM model. It is also a good opportunity to collaborate and exchange with the NIST organisation on privacy concerns in the cloud.

Received feedback
At the time of writing this report, the consortium had not received the consolidated version of the draft, but we know that the comments were accepted.

Plans after the finalisation of the project
The contributions to CARAM will continue to live within SAP, which expects to improve metrics for the continuous risk monitoring. More generally SAP wants to make more reliable the continuous risk management and to interact with dedicated standards like the upcoming NIST CRMF.

3.3 ISO/IEC 29134

In late 2014, ISO/IEC started the process to revise the working draft (WD) version of the ISO/IEC standard 29134 on “Information Technology - Security techniques - Privacy impact assessment - Guidelines” and come up with the Committee Draft (CD). This standard is relevant to the A4Cloud work on the data protection impact assessment and the practices that should be followed in order for cloud providers and customers to be compliant with the data protection regulations.

A4Cloud Contribution
In the lifetime of this process, A4Cloud contributed to the development of both the 1st and the 2nd CD versions of the standard by providing comments to the working versions shared with A4Cloud through CSA and HPE. The timeline that was followed involved two major milestones for the provision of comments in the relevant versions of the CD version of the standard:

- On August 28th, 2015 for providing comments to the 1st CD version of the standard
- On February 24th, 2016 providing comments to the 2nd CD version of the standard

The main focus for contributions was on the period for commenting on the 1st CD version. During this period, which started in late 2014, A4Cloud filled in the requested commenting template by providing 9 comments. The majority of the comments was of a technical type, meaning that we submitted our technical view and proposal for modifications aiming to strengthen the standard contents and align them with industry innovations.

In detail, the technical comments raised in the contents of the 1st CD version of the ISO 29134 standard (dated June 25th, 2015) span across the different areas covered by the standard, as analysed in the following lines:

- In the preparation of the privacy impact assessment (PIA) analysis, we consulted the ISO board members to enlarge the cases of who is conducting a PIA and cover the case that a PIA is mandated by the regulators to both controllers and processors, subject to special cases of jurisdictions.
- In the scale of a PIA, we suggested the critical factors for scaling the conduction of the PIA in a certain context, as the readers of the standard did not have any guidance on how they can assess this scale. In this area, an important clarification that we introduced has to do with the case of small and medium-sized enterprises and how such organisations that do not employ a Privacy Officer should be guided to decide on the scale of the PIA to be conducted.
- An important parameter in the guidelines for the conduction of the PIA is the human resources factor. Although the standard identified the stakeholders for taking this responsibility, we encouraged the assignment of one role that should be accountable to signing off the final report and for implementing the identified measures.
- When presenting the assets for the PIA analysis, ISO 29134 introduces a set of questions, but it was not clear whether this is an exhaustive list or not. Due to the particularities that can impact on privacy being left behind with respect to this set of questions, we suggested that the standard should clarify that this list is non-exhaustive.
- We raised our doubts on the figure explaining the work flow of the PII life cycle, as the roles for PII processing were considered insufficient. The figure itself was not self-explanatory and it could be difficult to understand by the readers without proper and extensive discussion on the points reflected in it.
- When assessing the privacy risks, the implementation guidance was deemed insufficient from the A4Cloud perspective, because some cases, like when the data controller contracts cloud services, had been left out and the provided threats were not specific for cloud services. Our opinion on this was that certain cloud risks and risk assessment methodologies for cloud systems should be documented in the standard as references.
- We suggested distinguishing between control identification and selection in the processes for performing a PIA.

Apart from these comments on the 1st CD version, we also submitted our perspective for the 2st CD version prepared on November 23rd, 2015. The main comment in this version had to do with the definition of “Privacy Impact’, which is very broad and vague and we were not aware whether this is thoroughly clarified in ISO/IEC 29100:2011. The reason for a strong definition of privacy impact is crucial, because an unclear definition may allow the users of the standard to apply a narrow understanding of privacy impact. Our proposal to the ISO/IEC JTC 1/SC 27 board was to include a definition addressing, among others, that the processing of personally identifiable information (PII) would cause harm to individuals’ right to privacy, or prevent them to exercise their legal rights in terms of personal data protection: information about who is processing what data, for which purpose, right to modify, reclaim, delete data, among others (depending on the individual’s country). As a result, we proposed a definition that engages concepts found in other reference material (such as other standards) and introduces the privacy impact as the “*effect on the privacy of a PII principal*”. Further to the core definition, we proposed a side note to this, explaining that the privacy impact might result from the processing of assets in conformance or in violation of privacy safeguarding requirements.

Value for A4Cloud

By being engaged in the activities for commenting the production of the CD version for the ISO 29134 standard, A4Cloud aimed to contribute to the development of a complete set of guidelines for conducting a privacy impact assessment in the cloud services market. This is strongly related to the concept of accountability that the project promotes as the prerequisite for the effective stewardship of personal data in the cloud. Especially, this standard adds value to the development of tools for accountability, like

DPIAT, which provides support to cloud customers and providers on how to assess the risks and their impact to the protection of the cloud subjects' personal data and their privacy.

The contribution to this standard has been compiled based on the A4Cloud work on risks and the risk assessment methodology for cloud environments. The alignment of this work with the standardized activities for performing a PIA process will give credits to A4Cloud research and innovation efforts, while it will offer a good connection between a PIA analysis and accountability.

Received feedback
The comments that we submitted to the 1st CD version of the ISO 29134 standard have been evaluated by the responsible ISO/IEC JTC 1/SC 27 board and they have been accepted either fully or with modifications. Based on these comments and the comments received from other initiatives as well, SC27 provided a revised 2nd CD version of the ISO 29134 standard. As the commenting period lasted till the 24th of February, 2016, there was not enough time to receive their feedback on the comments we submitted for this 2nd CD.

Plans after the finalisation of the project
As mentioned above, the feedback related to A4Cloud's contributions to ISO/IEC 29134 is expected to be received after the finalization of the project. However, future contributions through CSA International Standardisation Council (ISC[3]) will be still feasible because this draft standard is not yet on its final version (FDIS on ISO/IEC terminology). Future contributions may further refine the terminology defined in the current draft.

3.4 CSA Privacy Level Agreement

Privacy Level Agreement is intended to be used by CSPs to disclose the practices they adopt to be compliant with EU personal data protection mandatory legal requirements. A PLA should be used by potential customers to evaluate the level of data protection offered by a CSP. CSA PLA seeks to promote a powerful industry standard through the adoption of a common structure for the disclosure of privacy related measures. A PLA is meant to be provided as an appendix to a Service Level Agreement (SLA). PLA as a research initiative was launched only in 2012. The last version of the PLA has been released in June 2015.

A4Cloud Contribution
The A4Cloud project joined the CSA Privacy Level Agreement (PLA) v2 WG and contributed to the specification of PLA for Europe V2 (PLA4EU v2) that has been officially released in June 2015 [1].

A4Cloud produced a contribution to bring into the PLA the view of accountability as developed within the project. A4Cloud reviewed and revised the last version of the section in PLA dealing with accountability practices [3] (content provided in Appendixes A.1 and A.2). A4Cloud introduced in the new version of the Accountability section [1] the notion of evidence, whose provision plays a central role for the adoption of an accountability-based approach.

A4Cloud contribution (content provided in Appendix 0) explains what the concept of evidence means and why the CSPs should provide evidence. The view of evidence, seen within A4Cloud as pertaining to three different levels, has also been introduced along with examples of evidence elements that could be used to demonstrate accountability at those different three levels. In the A4Cloud contribution additional footnotes were also added, in particular to highlight that the concept of evidence was also present in an opinion of A29WP.

Value for A4Cloud
The A4Cloud project carried out an interdisciplinary analysis of accountability, developing a complete view of accountability practices and, in particular, elaborating a view around the concept of evidence. To have this view reflected in the PLA consolidates one of the outcomes of the A4Cloud project.

PLA has been leveraged within the D3 work package as the reference agreement where privacy related policies reflecting legal requirements are disclosed. A4Cloud modeled a subset of the policies to be

[3] Please refer to https://cloudsecurityalliance.org/isc/

included in a PLA using a formal representation. This representation has enabled the development of an automated process for the enforcement of the policies specified in the PLA.

Received feedback
The contribution provided by A4Cloud was reviewed and discussed with the PLA v2 WG members and was accepted. The contribution has replaced the previous version in the Accountability section and is now part of the PLA4EU v2 [1].

Plans after the finalisation of the project
Next step for PLA WG will be to seek the endorsement of WP29 on a PLA Code of Conduct. A4Cloud has been contributing and will keep contributing within the PLA WG in order to achieve this goal. Part of the required work is the revision of the PLA v2 to reflect new requirements from the new General Data Protection Regulation (GDPR) that is set to come into force in early 2018.

3.5 CSA Cloud Trust Protocol

Cloud Trust Protocol (CTP) is a CSA initiative that seeks to provide cloud service providers and cloud customers with a mechanism to request and receive information about the service levels. CTP is a tool enabling CSPs to provide transparency with respect to the fulfilment of the service levels that have been agreed with a customer.

A4Cloud contribution
A4Cloud reviewed the "Cloud Trust Protocol Data Model and API" proposal, which addresses one of the five tasks CTP project has been structured into in order to provide an implementable specification of the protocol.

Comments and suggestions provided can be summed up in the following list of points:

- The CTP specification, as it is, allows to exchange information about different kinds of attributes, and the description shouldn't be limited to "security attributes". Based on the monitoring capabilities of the infrastructure set up by the CSP, the customer and the provider can exchange information about other attributes, for example related to performance indicators. Reviewing the specification, it seems that replacing "Security Attributes" with the more general concept "Attribute" wouldn't require implementation changes.
- The specification could include a descriptor of the capabilities offered by a provider through the implementation of CTP. This descriptor could help customers who want to know whether providers adhere to a specific standard for describing attributes, measurements and metrics, or enabled controls over the status of the attributes.
- Even if the overall level of a security attribute for a service composed of different units is not in the scope of the CTP specification, it's worth clarifying that further steps are required for its evaluation. CTP enables to retrieve information about the different service-units involved in a supply chain, thus moving toward a more transparent approach in the provision of a service. What is required for the evaluation of an attribute related to a composite service is the definition of a composition function which takes into account the role and the service models of the service-unit involved.
- Some scenarios may require the highest level of security. The choice of the underlying security mechanisms is said not to be the scope, but the specification should enable the addition of security mechanisms possibly relying on standard implementation.

Additional, more detailed comments were given in an annotated document.

Value for A4Cloud
Transparency is one of the key attributes of accountability. Transparency can be referred to different aspects of a service provision. CTP addresses the problem of transparency in the communication of the service levels monitored by the CSP. CTP enables the exchange of information related to the actual status of the attributes agreed with a customer. The customer is also enabled to define events (conditions over attribute measurement results) that require the CSP to send an alert.

Received feedback
The feedback received from A4Cloud was fully integrated into the updated version of CTP [4].

Plans after the finalization of the project
As a volunteer contributor/reviewer to CTP, A4Cloud has been given an early access to the source code of the CTP prototype. There is no plan at the moment for its usage, as the demonstrator has already been finalized. However, the chance to use it after the finalization of the project could still be considered.

3.6 CSA Cloud Control Matrix (CCM) and Open Certification Framework (OCF)

CSA's Cloud Controls Matrix (CCM) [5] is a control framework specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The foundations of the CCM rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI DSS, and NIST SP 800-53. The current version of CCM (version 3.01) is described in the form of a matrix consisting of 133 controls divided in 16 domains.
In addition, CSA has defined a certification scheme through which cloud providers can assert their compliance to CCM. This scheme, called the Open Certification Framework (OCF) [6], defines the CSA Security, Trust & Assurance Registry (STAR) programme [7], with three levels of compliance:

- Level 1 - CSA STAR Self-Assessment
- Level 2 - CSA STAR Attestation or Certification
- Level 3 - CSA STAR Continuous Monitoring

Levels 1 and 2 are fully defined and operational. Level 3 is currently being defined by the CSA OCF Working Group. Two project principals are actively involved in this working group, from CSA (with the role of Open Certification Advisor) and HPE (as a contributing working group member). CSA STAR level 3 should be operational in 2017.

A4Cloud Contribution & Received Feedback
A4Cloud contributed to the revised charter of the OCF working group in 2014 (cf. Deliverable D:A-5.1), contributing four objectives to STAR level 3. These objectives have been adopted and transcribed in the final version of the charter.
A4Cloud has been provided with an early copy of the CSA STAR Level 3 – Continuous (Vision and Roadmap) white paper which provides a frame of reference for the working group activities. These comments have been assessed by CSA, and a formal response has been provided. The comment sheet with comments disposition is included in the Appendix A.3 for reference. These comments were later discussed, and further input was provided during the CSA EMEA Congress in November 2015.
The whitepaper is currently going through an in-depth revision, and we intend to provide further input, as appropriate. We believe that our comments, in both a written and oral form, are a significant contribution to the STAR Level 3 programme.

Value for A4Cloud
As highlighted in Deliverable D:A-5.1, CSA STAR Continuous is particularly relevant to accountability. Most certification schemes, including CSA STAR Attestation/Certification, are based on conducting periodic audits. In our context, let's consider the case of a certified Cloud provider. If it acts in the most transparent manner, the best it can provide to its customers is the certification audit report, which is a static view of the enterprise and can be a year old. In most cases, though, the only document made available is a copy of the certificate itself, which has no details. This is far from what is required in an accountability-based approach. In contrast, CSA STAR Continuous is designed to "enable automation of the current security practices of cloud providers. Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts." CSA STAR is also related to the scientific contributions from the C6 risk and trust model, where A4Cloud proposes and experiments with an approach for privacy preserving continuous monitoring for cloud risk indicators (see D:C-6.1 Section 7.6 and Appendix D). This is very close to what is required for an accountability-based approach. We have therefore decided to contribute to shaping CSA STAR Continuous.

Plans after the finalisation of the project
There are a number of significant challenges facing STAR Continuous besides technology and implementation. While a natural interpretation of the 3 layer approach to STAR would lead to assuming that each level provides a higher level of trust than the level below, a more detailed analysis leads to a different conclusion. In fact, continuous monitoring reports on a much smaller set of controls than self-assessment, attestation or certification. Furthermore, the open publication of the current status of the

system in terms of security breaches, ongoing attacks, or of other sensitive security data might lead to attracting hackers, which is an undesirable side-effect. Further work is required to identify the optimal structure of the STAR programme in regards to level 3. CSA, in its role of advisor to the OCF working group, and, to a lesser degree, HPE in its role of active working group member, will continue to work on shaping STAR Level 3.

Addendum
While not strictly related to the standardisation activities supported by this work package, it is important to report that the definition of the Simplified Accountability Control Framework, described in the D:D-2.4 Cloud Accountability Reference Architecture, is the result of a collaboration with principals of CCM. More detailed information on the mapping between the two control frameworks is available in D:D-2.4 section 4.9. A higher level of integration of accountability controls is being considered for future releases of CCM. This will involve both CSA and HPE (cf., Section 4).

4 Sustainability of A4Cloud's standardisation activities

The duration of the A4Cloud project is finite, but its legacy to the different topics covered by the project will remain through activities that include standardization. During the lifetime of the project, the standardization WP contributed to an overall set of 11 initiatives (including both standards and best practices). As described in both standardization deliverables, namely D:A-5.1 and D:A-5.2, the orchestrated contributions followed an strategic approach that allowed the WP A5 to receive feedback from the other work packages in order to identify the areas of interest presented in Section 2.

The following initiatives will continue to receive feedback after the finalization of A4Cloud:

- ISO/IEC 19086 (Parts 1 to 4)
- CSA PLA
- CSA OCF
- CSA CCM

Therefore, it is expected that in particular A4Cloud partners HPE and CSA will continue contributing to these under the umbrella provided either by the CSA International Standardization Council (CSA ISC[4]), or the corresponding CSA working groups. Listed CSA initiatives have implemented charters defining procedures for providing contributions and collaboratively approve submitted content. These established procedures guarantee a structured and sustainable approach to continue partner collaborations and contributions even after the finalization of A4Cloud. Also, due to the volunteer-driven nature of CSA working groups, A4Cloud partners can continue contributing to the identified initiatives. This is the case of partner UMA, which is a main contributor to the newly created CSA CloutTrust[5] working group on the topic of privacy metrics (initially developed within the context of A4Cloud WP C6).

The future sustainability of the project is also related to the standardization roadmap documented by WP C3 in its deliverable "D:C-3.3 Roadmap for framework for cloud accountability standardisation". That report proposed a roadmap that describes standardisation options for the outputs of the A4Cloud project, with a view of driving accountability through interoperability. The C3 roadmap identifies 13 artefacts as candidates for standardisation, which are further analysed from the A5 perspective in order to find potential standardisation venues for (some of) these. The following table summarizes the main findings of the C3 report's analysis mapped to A5's areas of interest:

Table 4. Sustainability of A4Cloud outcomes through standardisation activities

Documented A5 Area of Interest	Documented C3 candidate for standardization	A5's legacy and sustainability venue
Service Level Agreements	A model contract for accountability	Despite that a model contract is not within the scope of the ISO/IEC SLA initiative (cf., Section 3.1), A5 has contributed to the 19086-1 standard with the corresponding SLA terminology and guidance identified by A4Cloud. Contributions to ISO/IEC 19086 will continue after the duration of A4Cloud, mainly driven by HPE and CSA.
Assessment and Certification	Data protection level agreement ontology (COAT tool)	This topic was actively contributed to the CSA PLA wg (cf., Section 3.4) during the duration of A5. HPE is an active contributor to CSA PLA wg, therefore it is expected that after the finalisation of A4Cloud the COAT-related contributions will continue.
Risk Management	N/A	This particular area of interest for A5 could not be mapped by C3 to the analysed A4Cloud outcomes.

[4] It is worth to notice that HPE is a voting member within CSA ISC.
[5] It is worth to notice that HPE is a voting member within CSA ISC

Documented A5 Area of Interest	Documented C3 candidate for standardization	A5's legacy and sustainability venue
Privacy Impact assessment (PIA)	Data Protection Impact Assessment methodology	Contributions related to this particular topic were provided to ISO/IEC 29134 (cf., Section 3.3), mainly driven by partners ATC and SAP. Given the fact that ISO/IEC 29134 is still on a "working draft" stage (WD), it can be expected that its maintenance period will be established well beyond the duration of A4Cloud. At the time of writing this deliverable, partner SAP was agreeing with CSA on the mechanisms to become a voting member within CSA ISC. If successful, this measure will allow SAP to provide contributions to ISO/IEC 29134 based on the outputs from A4Cloud.
	Protocol for secure asynchronous messaging (TL)	Based on A4Cloud's Description of Work document (DoW), the standardization of protocols, APIs and prototypes is out of A5's scope.
Not identified[6]	DB engine for an accountability enforcement	Based on A4Cloud's Description of Work document (DoW), the standardization of protocols, APIs and prototypes is out of A5's scope. Both schemas may fit within upcoming study periods (SP) planned by ISO/IEC SC27 after the finalization of A4Cloud. Both HPE and CSA, under the auspices of CSA ISC, will follow up on those SP by the time they appear.
	Personal data access API	
	Lightweight incident notification API	
	Schema for data transfer restrictions	
	Schema for evidence records	Both schemas may fit within upcoming study periods (SP) planned by ISO/IEC SC27 after the finalization of A4Cloud. Late 2015 NIST started a new working group called "Open Security Controls Automation Language (OSCAL)", where the topic of policies and automation play a central role. CSA is part of the NIST OSCAL wg and will follow up on a potential contribution of the accountability policy machine-readable language.
	Accountability policy machine-readable language	
	Extension of the NIST cloud reference architecture (CRA) to accountability	At the time of writing this report, there were not plans from NIST to extend their CRA.

[6] The list of topics listed under this category did not have a direct match to A5's Areas of Interest

Documented A5 Area of Interest	Documented C3 candidate for standardization	A5's legacy and sustainability venue
	General reference architecture for accountability	The reference architecture contributed by WP D2 has been analysed from the standardization perspective. In particular the proposed Accountability Maturity Model, and the Simplified Accountability Control Framework are being considered for contribution to CSA Cloud Control Matrix (CSA CCM). Initial validation of the D2 outcomes and CSA CCM has taken place in A4Cloud, although the actual contribution will occur after the duration of the project. Partners HPE and CSA will be involved in this future activity.

In this section several standardization actions aimed at supporting the sustainability of A4Cloud outcomes after the finalization of the project have been presented. Some of these activities have already started (cf. Section 3), and the contributing partners have committed to continue their contributions even after the project's timeframe. A second set of sustainability activities will start after the finalization of the project. These actions have been already planned in the context of both WP A5 and WP C3, contributing partners have been identified (mainly HPE, SAP and CSA), and potential SDO/SSO initiatives are being followed-up to timely and efficiently orchestrate the respective contributions. In this context, the CSA ISC will play a central role as a facilitator for developing and discussing the expected A4Cloud-related contributions.

5 Conclusion

This deliverable has summarised the contributions to standards and best practices that A4Cloud has performed during the last 18 months of its duration. The performed contributions have been orchestrated based on a revised version of the standardisation strategy presented in the first standardisation deliverable (D:A-5.1), which follows a refinement process to identify a set of areas of interest where standardisation efforts were focused.

Furthermore, apart from reporting performed contributions, this deliverable also introduced a set of standardisation actions aimed to support A4Cloud's sustainability after the finalisation of the project. The planned set of sustainability actions clearly identify the A4Cloud outcomes to be contributed, the partners to participate, the channel to provide the contributions, and potential SDO/SSO to be observed. The foreseen sustainability actions do not imply any commitment of the potential contributors after A4Cloud duration, however these actions were built considering the contributing partner's interests and exploitation plans.

References

[1] Cayirci, E.; Garaga, A.; Santana de Oliveira, A.; Roudier, Y., "A Cloud Adoption Risk Assessment Model", In procs. of the 7th International Conference on Utility and Cloud Computing , 2014
[2] CSA Privacy Level Agreement v2, https://cloudsecurityalliance.org/download/privacy-level-agreement-version-2/
[3] CSA Privacy Level Agreement v1, https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf
[4] Cloud Trust Protocol, https://cloudsecurityalliance.org/download/cloudtrust-protocol-data-model-and-api/
[5] CSA Cloud Control Framework, https://cloudsecurityalliance.org/group/cloud-controls-matrix/
[6] CSA Open Certification Framework, https://cloudsecurityalliance.org/group/open-certification/
[7] CSA Security, Trust & Assurance Registry (STAR), https://cloudsecurityalliance.org/star/

CLOUD ACCOUNTABILITY PROJECT

Appendix

Appendix A.1: Contribution to PLAv2 (Accountability section)

Appendix A.2: Contribution PLAv1 (Accountability section)

Appendix A.3: CSA STAR Level 3

The following is the comment sheet provided on the CSA STAR Level 3 – Continuous (Vision and Roadmap) document in April 2015, along with the initial disposition of the comments:

Document Review – Comment Sheet	
Comment Sheet Information ***(to be filled in by the Reviewer)***	
Comment Sheet Reference :	CSA C-STAR Scheme
Comment Sheet Date :	April 24, 2015
Document Information ***(to be filled in by the Reviewer)***	
Document Title :	CSA STAR LEVEL 3 - CONTINUOUS
Document Reviewed by ***(to be filled in by the Reviewer)***	
Organisation or Company :	HP Labs on behalf of the A4Cloud Project
Name :	Frederic Gittler and Michela D'Errico
E-mail :	frederic.gittler@hp.com and michela.derrico@hp.com

Conventions :

Type of Comment		**Assessment**		**Comment from author**	
G	General	**CN**	Correction necessary	**R**	Rejected
M	Mistake	**CE**	Correction expected	**A**	Accepted
U	Understanding.	**+**	Major	**D**	Discussion necessary
P	Proposal	**-**	Minor	**NWC**	Noted without need to change

Review Comments (if necessary add extra lines in the table) :

N°	Reference (e.g. PAR, Sentence	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author Only)	Author's justification for recommending rejection of change
		U/CE	Auditing, monitoring, assessment and certification are 4 interrelated processes. Their relation should be clarified at the start of the paper to make clear the baseline on top of which the vision described in this document is built. A diagram (e.g. a business process model) could be produced to clarify the dependencies between these processes.		DC: I agree we can add a diagram.
	Section 1, sentence "It shall be noted that the difference between "continuous auditing" and "continuous monitoring" is that the first one support the gathering of audit assertion while the latter provide capability for verifying on continuous	P/-	What can be gathered from this sentence is that there is a dependency between continuous auditing and continuous monitoring processes. Specifically the dependency is that the monitoring process verifies audit assertions, which are the result of the auditing process. If this view is correct, a use case example should be added to clarify how the monitoring process can use the results from the audit process to assess a control.		DC: good point. Time allowing we'll add an example.

N°	Reference (e.g. PAR, Sentence	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author Only)	Author's justification for recommending rejection of change
	basis that the assertions are really true."				
		G/-	With regard to the monitoring process it should be clarified that it entails the verification of actual status of properties/attributes related to different aspects of a service against their target status specified into an agreement (e.g. SLA).		DC: do you have any suggested wording?
	Section 2, second to last sentence "With CloudAudit we can answer questions such as "What was the evidence that the service implements control objective A1, on domain B, of framework C"."	U/-	As the result of the auditing is a set of auditing assertions (see comment 1), shouldn't Cloud Audit, as core feature, enable to answer questions like "What are the audit assertions for service S?"		DC: In principle I agree that the working following working is better: "What's the assertion for service xxx that provides information about the implementation of control objective A1, on domain B, of framework C"

N°	Reference (e.g. PAR, Sentence	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author Only)	Author's justification for recommending rejection of change
5	P.3, last sentence: "We may not be able to *constantly monitor* that the policy is up-to-date or that the technical backup mechanisms are in alignment with the policy"	U/+	If control A1 requires the implementation of a backup policy, and the alignment of the technical backup mechanism with the policy cannot be verified, what can be inferred about the implementation of control A1? Characteristics of the technical mechanisms can be monitored (like backup restoration frequency), as said in the document, but how does the result of this monitoring relate to the implementation of the control?		DC: this comment will be more effectively addressed in a discussion. But you are right there's a correction to made and we should not make reference to alignment with policy. The sentence could be rephrased as follow: We may not be able to *constantly monitor* that the policy is up-to-date, BUT we can monitor that the technical backup mechanisms are in alignment with the policy (e.g. backup restoration frequency, success rate, simulated restoration point actual (RPA) and contrast it with the RPO).
6	Page 4, text in the box: "continuous monitoring can be applied to simpler characteristics we refer to as "security attributes""	U/-	Continuous monitoring should apply to a larger set of properties that may come from an SLA, including performance related properties. Thus the scope of the continuous monitoring, in principle, should not be limited to "security attributes".		DC: correct. It's just that the scope of our work is security and privacy
7	Page 4, text in the box: "Monitoring these security	U/CE	In order to turn the monitoring of attributes into "valid" indications of the status of the controls implementation, two issues should be addressed:		DC: I agree we can add those to the list of challenges.

N°	Reference (e.g. PAR, Sentence	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author Only)	Author's justification for recommending rejection of change
	attributes provides indirect but valid indications of the state of implementation of controls and security requirements."		• How to link attributes to technical mechanisms and technical mechanisms to controls; • Alignment of technical mechanisms with controls to be implemented If these two issues haven't been tackled yet, they may be added to the list of challenges.		
	Section 3 "CSA STAR Continuous"	P/+	Current practices do not always allow a CSP to report on specific controls part of the CCM through CloudAudit and, to an even lesser degree, to report on the performance and status of the associated mechanisms through CTP. The introduction of a maturity model which would reflect the breadth, depth, and quality of what is reported as part of the STAR Continuous certification (or label?) for a given CSP is recommended.		DC: to be discussed
	Section on SCMC	P/CE	This description misses on the opportunity to provide data that is directly relevant to the service provided for the cloud customer making the request through CTP, rather than for data global to the service provider but which does not necessarily affect the specific customer. This level of service would correspond to the OCF WG Charter objective to "relate/merge/cross-leverage the reporting and monitoring mechanisms used to demonstrate and track accountability with the mechanisms to be deployed as part of OCF Level 3"		DC: to be discussed

N°	Reference (e.g. PAR, Sentence	Type/ Assess	Reviewer's Comments, Questions, Proposals	Comm. (Author Only)	Author's justification for recommending rejection of change
	Section 4 "Challenges"	P/CE	An analysis of the business risks associated with the proposal is missing and should be provided.		DC: to be discussed. This is not a scientific paper. There are many areas to be improved, but can't necessarily too much time to invest. It might be part of a v2 of this initial paper
	Section 4 "Challenges"	P/CE	An analysis of the feasibility and ROI (cost vs. benefits) for the proposed schemes is required, in accordance with the OCF WG Charter objective "Assess and monitor the economic feasibility and ROI (cost vs. benefits for an organization seeking certification) of the OCF"		DC; see comment above
	Section 4 "Challenges"	G/+	The challenge of defining a framework where it is possible to obtain a meaningful comparison of providers based on the data provided through CSA STAR Continuous should be recognized as a yet-unresolved issue. Such a scheme is required, in particular for the S2CB scheme.		DC: agreed.
	End		End of comments		