CLOUD ACCOUNTABILITY PROJECT

D:A-5.1 Report on A4Cloud contribution to standards

Deliverable Number	D15.1
Work Package	WP 15
Version	Final (Version 1.1)
Deliverable Lead Organisation	CSA
Dissemination Level	PU
Contractual Date of Delivery (release)	30/09/2014
Date of Delivery	30/09/2014
	17/10/2014 updated version

Editor
Jesus Luna (CSA), Daniele Catteddu (CSA)

Contributors
Vasilis Tountopoulos (ATC), Carmela Asero (CSA), Jean-Claude Royer (EMN), Michela D'Errico (HP), Frederic Gittler (HP)

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

List of acronymns

Abbreviation	Meaning
AB	Advisory Board
CSA	Cloud Security Alliance
CSA STAR	Cloud Security Alliance's Security Trust and Assurance Registry
CSC	ETSI Cloud Standards Coordination
CSP	Cloud Service Provider
EC	European Commission
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
EU27	27 EU Member States
FP7	The Seventh Framework Programme (2007-2013)
H2020	Horizon 2020
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
ICT	Information and communications technology
ISO	International Organization for Standardization
ISP	Internet service provider
MS	Member States
PaaS	Platform as a Service
RD&I	Research, Development and Innovation
RTD	Research and Technological Development
SaaS	Software as a Service
SDO	Standardization Development Organization
SME	Small and Medium-sized Enterprise
SLA	Service Level Agreement
WD	Work Document
WG	Working Group
WP	Work Package

Executive Summary

Standardization is a core activity within A4Cloud, guaranteeing that the contributions from the different research tasks can have a broader community impact through standards and best-practices. In order to achieve this vision, it is necessary to have a clearly defined methodology that allows partners to focus on a well-defined set of standardization activities related to A4Cloud's core topics. This deliverable documents the progress achieved by WP:A-5 "Contribution to Standards" after the initial 24 months of the project's duration.

In particular this deliverable presents (i) the overall standardization strategy defined by WP:A-5, (ii) the rationale behind the evolving list of standards being considered by A4Cloud, and (iii) the initial results obtained by WP:A-5 in relationship with relevant standardization/best-practices activities where A4Cloud has participated.

The next version of this deliverable will present the final results obtained by WP:A-5, and most specifically will focus on providing a roadmap and strategy for relevant standardization activities extending beyond the project's duration. Preliminary engagement with relevant standardization bodies suggest that (industrial) partners might be willing to continue their involvement in identified standardization bodies as part of A4Cloud's sustainability plan.

Table of Contents

List of Figures.

List of Tables.

1 Introduction

Nowadays, the topics of standardization and certification are being considered as a priority within the cloud security and data protection community. Since the advent of the cloud, practitioners started to rely on best-practices in order to manage the lack of cloud-specific security and data protection standards able to bridge gaps being identified in the state of the art. However, recent reports (e.g., from the European Telecommunications Standards Institute (ETSI) [14] and the US National Institute of Standards and Technology (NIST) [15]) and relevant EC FP7 projects (e.g., Cirrus [16] and CloudWATCH [17]) have shown the need for cloud-specific standards in very specific areas of security and data protection. In the case of ETSI, it is clearly highlighted *"the need for further standardization efforts in the area of accountability and cloud incident management (e.g., related with a SLA infringements). Such work would greatly benefit the whole cloud supply chain, although once again the main challenge is trust/security assurance among the involved stakeholders."* [18].

This deliverable discusses A4Cloud's approach and initial results in the area of cloud accountability standardization. More specifically, on one hand this document presents the methodological approach developed to identify gaps and prioritize contributions to standards that are relevant in the context of A4Cloud. On the other hand, are discussed the initial standardization-related results obtained during the initial 24 months of the project, with a particular focus on influencing efforts from relevant standardization bodies and best-practices organizations.

The final version of this deliverable (month 48) will be built on top of the present document, and is expected to contain a more refined/validated version of the approach to standardization along with a complete list of standards where A4Cloud contributed during its life-time. Furthermore, the final version of this deliverable will provide a long-term vision for the sustainability of A4Cloud's standardization efforts, mainly thought the involvement of the non-SME industrial partners (i.e., HP and SAP).

1.1 Scope of the document

The present deliverable documents the activities performed by WP:A-5 during the initial 24 months of the A4Cloud project, namely:

1. The gap analysis performed to identify in which relevant standards the notions of accountability are missing. This is related to Task T:A-5.1 and targets to provide some initial guidance to A4Cloud's Standardization Development Organization (SDO) contributions.
2. The actual set of activities related with the orchestration of A4Cloud contributions to identified and prioritized standards (i.e., Task T:A-5.2). For the activities contributing to identified standards (as reported on this deliverable), we also document and discuss the outcome/feedback received from the relevant standardization body.

1.2 Positioning of WP:A-5 within the A4Cloud project

The WP on standardization (WP:A-5) 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:A-5 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:A-5 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:A-5 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:A-5 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 (e.g., either a "preliminary work item" –PWI- or "draft international standard" –DIS- in ISO/IEC terminology). Once again, WP:A-5 is used by the rest of the WPs as a unique point of contact to be constantly updated about relevant standardization initiatives.

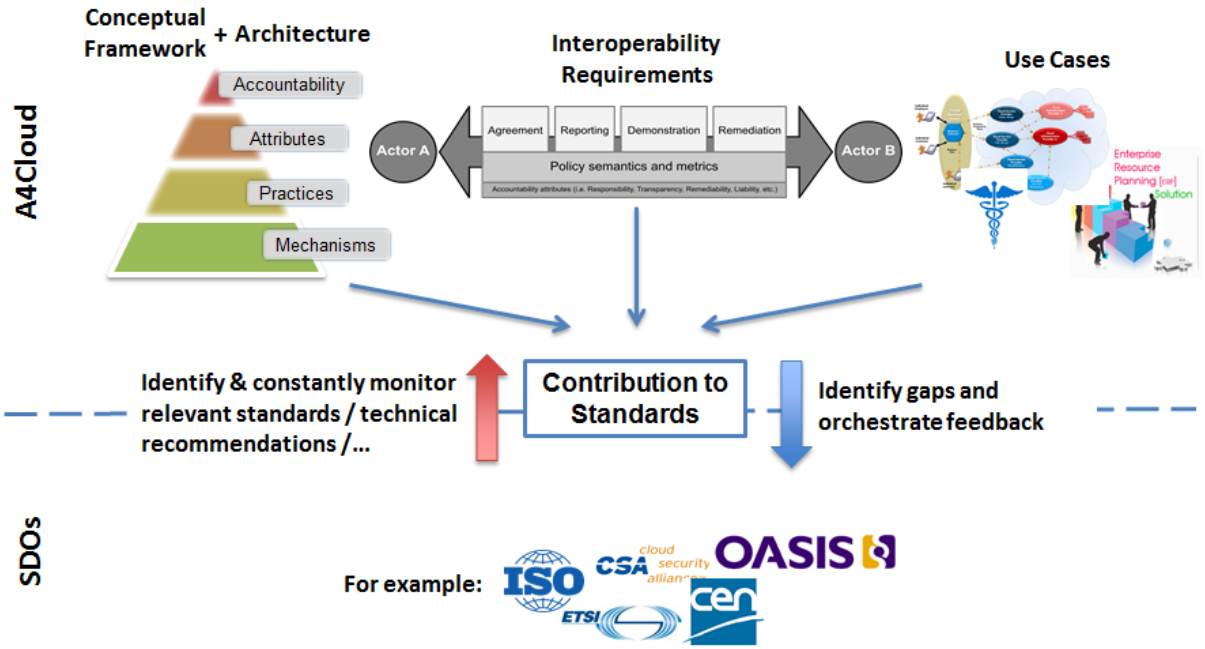

Figure 1. The role of standards in A4Cloud.

1.3 Outline of the document

The rest of this deliverable is organized in the following way:

- Chapter 2, describes the strategy developed by WP:A-5 to identify and prioritize the standards that are relevant to A4Cloud, and where contributions are feasible to orchestrate during the project's lifetime.
- Chapter 3, summarizes the results obtained in Task T:A-5.1, where standards are actually identified and organized according to the methodology described in the previous chapter.
- Chapter 4, presents the main results of Task T:A-5.2, where actual contributions to identified SDO took place. Where applicable, this chapter also discusses the feedback received from the respective standardization body.
- Chapter 5, discusses the specific standards where A4Cloud efforts will be focused.
- Chapter 6, discusses the main conclusions of this deliverable and presents an overview of the activities to be performed during the last 24 months of the project.

2 Overview of the strategy for standardization

This section overviews the approach developed by WP:A-5 to systematically analyse relevant standards and orchestrate contributions from the A4Cloud activities.

2.1 Approach

The orchestration of contributions to standards (i.e., Task T:A-5.1), followed a methodological approach within WP:A-5 to guarantee the impact of A4Cloud's research-related WPs. A high level view of the developed approach is shown in Figure 2. The individual building blocks of the WP:A-5 strategy are presented next.

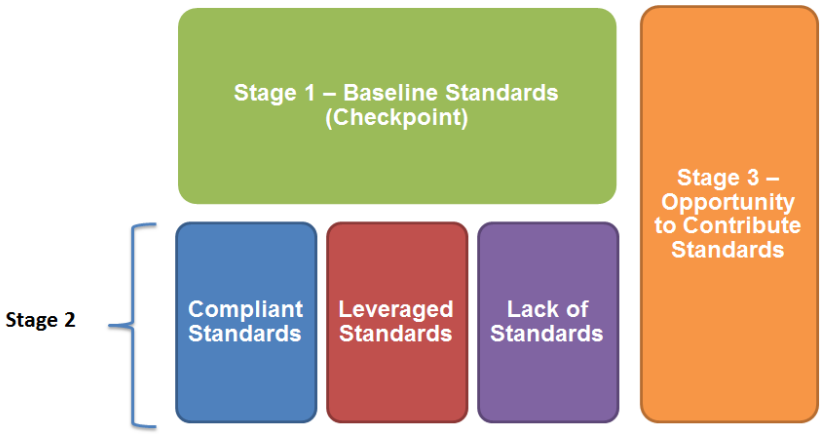

Figure 2. Strategy for standardization in A4Cloud.

During the first stage ("Baseline Standards – Checkpoint" in Figure 2), were identified those standards (cloud and non-cloud specific) considered as relevant to the core topics in A4Cloud e.g., accountability, data protection, privacy, security, and incident management. This *baseline* was reported as WP:A-5's initial checkpoint at month 9 (as required by the Description of Work). The baseline consists of 109 entries and will be further discussed In Section 3.1.

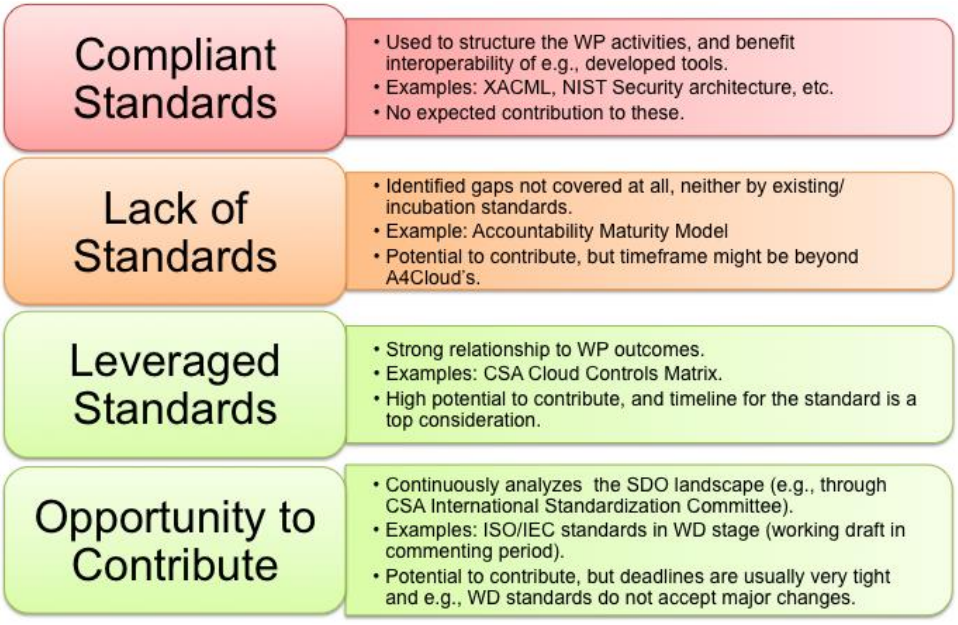

Figure 3. Suggested classification of standards in A4Cloud.

The second stage in the developed WP:A-5 methodology, further refined and classified the baseline (Stage 1) thanks to two rounds of feedback received from all the WPs in A4Cloud (the first round in

October 2013, and the second took place in February 2014). During this second stage, WP-selected standards were classified as any of the following (cf., Figure 3):

- Compliant i.e., standards that are followed by the tasks within a WP but that are not being extended by the research activities. Most of these standards (e.g., XML) allow for interoperability of the contributed technologies. The compliance with standards will be presented in Section 3.2.
- The WPs also provided an initial assessment on the lack of standards related to specific topics within A4Cloud. This category of standards is critical for the long-term sustainability of the project. The identified "lack of standards" will be presented in Section 3.3.
- Leveraged standards, which were identified by the WP leaders as being directly in the scope of their activities and foreseen outcomes. Furthermore, these standards are of great importance to WP:A-5 because A4Cloud can actively provide a relevant contribution to them in order to bridge identified gaps. The leveraged standards will be presented in Section 3.4.
- A fourth category (i.e., "Opportunity to Contribute") is continuously maintaining up-to-date the list of standards by analysing the relevant SDO initiatives and, requesting (when necessary) feedback from the WP leaders. A detailed discussion on the "opportunity to contribute" standards will be presented in Section 3.5.

2.2 Relationship with compliance and certifications

Standards are only useful to the extent they are adopted and adhered-to. While the conformance to specification-type standards can be identified during the engineering phase of a project through interoperability testing, it is much more difficult to assess if a third-party is operating in compliance with organization-type standards (see [28] for a definition of standard classes). Yet, the level of assurance conferred by the conformance to organization-type standards is important: for accountability, organisations need to use privacy and security controls appropriate to the context. Standards like ISO 27001 (cf., [ISO11] in Appendix A) or CSA Cloud Control Matrix (cf., [CSA06] in Appendix A) are particularly relevant as they define a baseline operational standard for handling security, trust, and related topics at the level of the organization. The associated certifications (and attestations) are the only practical ways to assert the level of compliance of a third party.

However, an accountability-based approach to compliance goes beyond the audit-based certification, such as what is currently used for ISO 27001: it requires a certain level of transparency in demonstrating compliance to the third-party user. We aim to inject this approach to existing certification schemes, when appropriate.
Furthermore, it must be noted that the stakeholders have identified the following requirement within A4Cloud "Standards body must say: this is the list of certifications you need to look for" [R-B2B-015z]. The CSA CCM and the associated CSA STAR scheme aim at being a "one-stop-shop in the cloud provider assessment process," [30]. Further details on this scheme can be found in Section 4.4.

2.3 Diligent nature of WP:A-5 approach

At this point it is important to highlight that WP:A-5 seeks to influence relevant standardization/best-practices activities based on the methodology described in the previous section. Nevertheless, it is not possible to guarantee neither by WP:A-5 or the overall A4Cloud consortium, that the feedback being provided to SDOs will become part of the final version standard/technical recommendation. There are many factors that might affect the SDO decision related to integrating provided feedback, and some of these are out of A4Cloud's reach. Let us take for example the following six stages of the process adopted by ISO/IEC for the development of their standards [19]:

- Stage 1: Proposal stage

  The first step in the development of an International Standard is to confirm that a particular International Standard is needed. A new work item proposal (NP) is submitted for vote by the members of the relevant committee to determine the inclusion of the work item in the programme of work.

- Stage 2: Preparatory stage

  Usually, a working group of experts, the chairman (convener) of which is the project leader, is set up by the TC/SC for the preparation of a working draft.

- Stage 3: Committee stage

  As soon as a first committee draft is available, it is registered by the ISO Central Secretariat. Successive committee drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is finalized for submission as a draft International Standard (DIS).

- Stage 4: Enquiry stage

  The draft International Standard (DIS) is circulated to all ISO member bodies by the ISO Central Secretariat (SC) or voting and comment within a period of five months. It is approved for submission as a final draft International Standard (FDIS) if a two-thirds majority of the members of the SC are in favour and not more than one-quarter of the total number of votes cast are negative.

- Stage 5: Approval stage

  The final draft International Standard (FDIS) is circulated to all ISO member bodies by the ISO Central Secretariat for a final Yes/No vote within a period of two months. *If technical comments are received during this period, they are no longer considered at this stage, but registered for consideration during a future revision of the International Standard.*

- Stage 6: Publication stage

  Once a final draft International Standard has been approved, only minor editorial changes, if and where necessary, are introduced into the final text. The final text is sent to the ISO Central Secretariat which publishes the International Standard.

- Review of International Standards (Confirmation, Revision, Withdrawal)

  All International Standards are reviewed at the least three years after publication and every five years after the first review by all the ISO member bodies. A majority of the members of the SC decides whether an International Standard should be confirmed, revised or withdrawn.

From WP:A-5 perspective, contributing to ISO/IEC standards during their DIS stage (cf., “Opportunity to Contribute” in Figure 2) might be seen as timely (it takes less than 5 months to receive a decision with respect to the provided feedback). However, from a practical perspective most DIS drafts only expect very few/minor changes to be integrated into the FDIS release. In the case of ISO/IEC, the higher chances to influence standards of interest (cf., “Leveraged” in Figure 2) will appear during the two initial stages of the process (i.e., before DIS, while the actual topic is being discussed by the members). Once again, there are no guarantees that the provided feedback will fully make it into the final version. Furthermore, the strategy adopted by WP:A-5 to identify and contribute to relevant SDOs is by no means complete (i.e., it is not possible to observe/contribute to all existing SDOs). However, our approach aims to be comprehensive and diligent enough in order to monitor well-known SDOs thanks to WP:A-5 interactions with groups like Cloud Security Alliance’s International Standardization Council (CSA ISC) [20]. This same approach for identifying and monitoring SDOs where members of WP:A-5 participate, is also the basis for *channelling* A4Cloud’s contributions. For example, in the particular case of CSA ISC the following SDOs are being monitored and it is possible for A4Cloud to contribute: ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 38, ITU-T (A.4, A.5), DMTF, OCDA, Cloud Standards, CCSA-China, CJK working groups, and the RAISE Forum.

3 Defining the standards gap per-Work Package

Based on the strategy for standardization adopted by WP:A-5 (cf., Section 2), this section describes in further detail the A4Cloud-specific rationale behind each group of standards. Also, in Appendixes A-D of this deliverable are included the current versions (M24) of the A4Cloud's lists of standards (i.e., checkpoint, compliant, leveraged and opportunity to contribute respectively). An overview of the considered standards per class is shown in Figure 4.

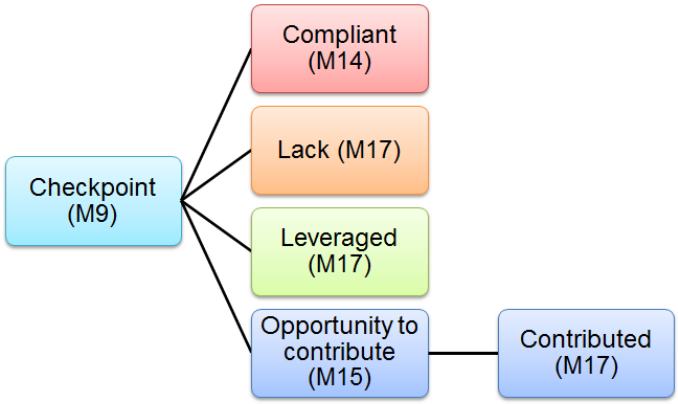

Figure 4. A4Cloud standards per-class (last update M24).

3.1 Checkpoint standards

The initial list of standards, referenced as "Checkpoint" through this deliverable, was created thanks to the collaboration of all partners involved in WP:A-5 and reported at month 9 to the rest of the consortium. The checkpoint list contained 122 entries (cf., Appendix A), and was gathered from partners' interactions and activities with relevant SDOs and technical recommendation groups. Furthermore, it is worth to highlight that the checkpoint list was also a contribution of the A4Cloud consortium to the ETSI Cloud Standards Coordination (CSC) [14] working group and an extended version of it (complemented with e.g., non-accountability related entries) appeared in the final report of the CSC group.

Following the same rationale adopted by ETSI, the checkpoint list contained not only standards (25 entries) and technical recommendations (39 entries), but also reports/white papers/others (54 entries). The latter were considered for completeness and are mostly used for structuring the research activities of the different WPs (i.e., state of the art), however it is also true that those publications (contrary to standards and technical recommendations) do not have a revision period that A4Cloud could use to contribute. *The main focus of WP:A-5 is therefore focused only on standards and technical recommendations*.

The checkpoint list (only standards and technical recommendations) took into account the work from 16 different SDOs, the most relevant being CSA and IETF (6 entries each), ISO/IEC (17 entries), NIST (10 entries), and W3C (5 entries).

With respect to their degree of adoption, basically all of the checkpoint standards range from "adopted" to "widely adopted" (95%). For the actual gap analysis performed by WP:A-5, it was also interesting to notice that only approximately 21% of the reported standards had a cloud-specific focus. A similar conclusion with respect to cloud-specific security standards was also drawn by the ETSI CSC group [14]. We should also notice that the checkpoint list contained almost 50% of organizational-related standards, and not only technical ones (e.g., specifications of APIs, protocols and data formats).

The "checkpoint" list is considered as the baseline/master set of standards relevant to A4Cloud, and is constantly maintained through e.g., periodic feedback coming from the technical WPs, and the constant monitoring of relevant SDOs.

3.2 Compliance with standards

A first revision of the checkpoint list (cf., Section 3.1) took place in October 2013. This initial list was distributed to partners from other work packages for feedback. WP:A-5 requested all other technical WPs to provide their inputs on the standards are compliant with. This activity received information from eleven work packages (B-3, C-2, C-3, C-4, C-5, C-6, C-7, C-8, D-3, D-4, D-5, D-6, D-7), that is 67 standards identified (including 19 not in the original list). We also set up a specific working session during our plenary meeting in October 2013. We note that the following work packages: C-2, C-4, C-6, D-3 and D-6 mentioned CSA's CTP & PLA.

A second review round took place in February 2014, once again requesting technical WPs for their feedback related with those standards they are still compliant with. After this second round, we observed that all 14 WPs replied with an overall set of 31 standards they are following. This list of standards is shown in Appendix B.

As mentioned in Section 2, the identification of compliance with standards was done for the sake of completeness, because this guidance is not under the scope of WP:A-5.

3.3 Identified lack of standards

Through the analysis of the baseline standards that relate to the work conducted in A4Cloud, in this section we describe the gaps that have been identified so far in the standardisation activities, which could draw a roadmap of project initiated potential contribution to the standards landscape. The gap analysis has been carried out following a constructive approach and collaboration with all the WPs in the A4Cloud project. More specifically, as soon as the baseline list of standards related to the A4Cloud work has been developed, a set of questions was circulated to the various WPs, aiming to receive feedback on how the project work is adequately reflected in the current standardisation landscape. Through the analysis of responses, the main categories corresponding to the lack of standards have been reported.

In the area of service level agreement specification and the extension of it to address the accountability problems, the standardisation efforts lack on the proper extension to the accountability dimension. SLANG [1] has been proposed by University College London (UCL) to describe the principal semantics in SLAs for application service provisioning scenarios. WS-Agreement [2] has been introduced by the Open Grid Forum (OGF), but it is rather limited in the management of an agreement life-cycle. Then, Privacy Level Agreement (PLA) [3] is proposed by CSA to offer compliance with data protection legislation and best practices when dealing with the level of data privacy that is being processed in the cloud, but PLA specification seems to lack flexibility and obligations expressed in PLA cannot be translated into machine readable formats, which could be subsequently handled by policy management tools. To conclude, the current standards landscape lacks appropriate specifications that could adequately describe the accountability requirements in the specification of service level agreements.

Cloud auditing is another area of interest for A4Cloud, in which current standards seem to lack on addressing market needs. CSA and DMTF have proposed specifications on how to access and formulate the audit records (see CloudAudit [4] and Cloud Auditing Data Federation [5] respectively). However, the actual auditing process and the provisional rights for accessing the products of the process itself have not been standardised. Such a process could identify the responsibilities of the auditors and the cloud providers and clarify the level of abstraction that is needed so that auditors can request only the relevant auditable information that is subject to the limitations in data protection as arising from existing regulations.

Measuring and assessing the current behaviour of cloud services has been extensively analysed in the standards promoted by several organization bodies, like NIST and ISO (see [6][7][8][9][10][11]). The measuring process is strongly associated to the definition of low level metrics for assuring the behaviour of software and systems, while specific provisions for the security assurance have also been introduced and are currently adopted in the industry. Although current standards may adequately approach the definition of the measurement procedures and the related metrics to be involved, it is still open how these metrics can be aggregated to realise the conformance to an accountability based approach for cloud service provisioning.

Of particular focus for A4Cloud is to provide tools that enable organisations dealing with the cloud to be accountable. Existing efforts in the standardization organisations have delivered maturity models, focusing on how organisations adopt practices to address the security and privacy issues [31]. In the area of cloud security-aware maturity models, CSA has produced the Cloud Control Matrix (CCM [12]), which provides fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. Furthermore, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have worked on a Privacy Maturity Model (PMM), which defines categories of generally accepted privacy principles. Both efforts can partially cover accountability, but not all of the A4Cloud defined accountability attributes are well represented in these maturity model frameworks. Towards this direction, the A4Cloud project identifies a significant gap in the area of Accountability Maturity Models (AMM), that could be used to demonstrate the maturity of organizations to be accountable. This work is being performed through WP:C-2 and WP:C-5. The outcomes will be contributed to relevant SDOs through WP:A-5.

As reported in ITU-T SG17, it is still under study which are the most suitable security solutions for cyber security in order to foster accountability, incident response, and threat monitoring and risk communication in ICT systems (Q4/17), while in Q8/17 the need for further investigation on the cloud computing security aspects is highlighted, in particular for best practices and guidelines around the security management concepts.

The joint technical committee (JTC) on security techniques (SC27), as formed by the ISO and IEC SDOs is another field for further investigation on the lack of standards in the area of cloud computing and future internet security. This SC27 is divided into five working groups, each one dedicated to the study of current open issues in specialised security aspects. Of particular importance for A4Cloud is the work conducted in WG1, WG4 and WG5, which reveals the requirement for a more coherent approach on the standardisation of the information security activities, especially in the area of cloud computing.

Finally, the privacy mechanisms being developed in the context of WP:C-7 advance the current state-of-the-art in the respective research discipline. Most of the work conducted there has not been standardised, since a lot of work can be done towards assessing the privacy risks and establishing adequate protection levels, as it is also identified in the ITU Technology Watch Report [13].

3.4 Leveraged standards

Based on the approach developed by WP:A-5 to structure and focus its standardization activity (cf., Section 2.1), the group identified along with the WP leaders a set of 12 technical recommendations and 16 standards where A4Cloud contributions can be expected. These 28 entries are shown in Appendix C, and were refined through a couple of interactions with the WP leaders (at month 14 and 17). This is a good progress towards focusing WP:A-5 efforts, because it means to centre only on approximately 23% of the original baseline list (cf., Section 3.1 and Appendix A).

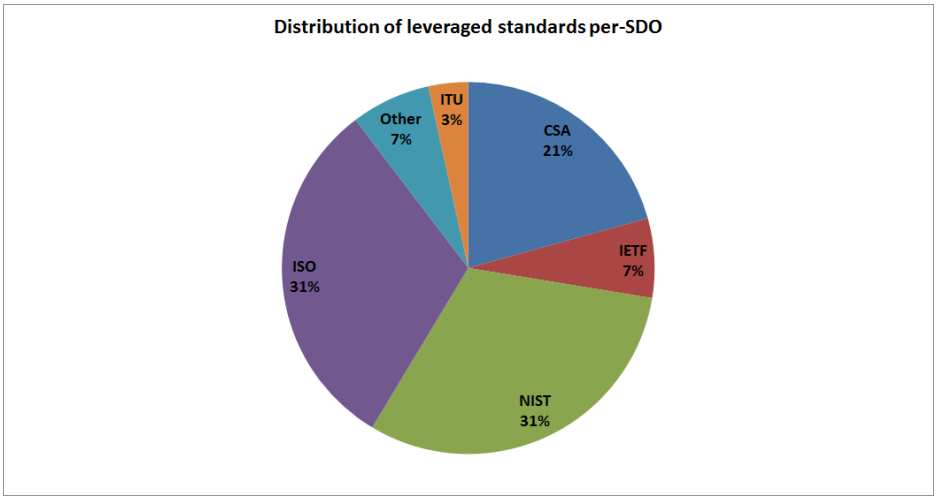

Figure 5. Leveraged standards per-SDO.

Leveraged standards are of special importance to A4Cloud, because these are directly targeted by the project's technical contributions. The leveraged standards/recommendations are distributed in the SDOs shown in Figure 5, where we can observe that most of them (approx. 83%) are maintained by either CSA, ISO or NIST. This is an important fact that can be used to further focus the A4Cloud contributions to identified standards in the following months.

Furthermore, it is also interesting to notice the most commonly referenced standards/recommendations, namely:

- SLA Language Spec: referenced by WP:C-4 and WP:D-3 as part of their research on Service Level Agreements and policy specification languages.
- Cloud Controls Matrix: referenced by WP:C-5 and WP:C-6 as base for building the metrics associated with the Accountability Maturity Model (cf., Section 4.1).
- Cloud Trust Protocol: considered by WP:C-2 and WP:C-6 both as part of the accountability management life-cycle, and continuous/automated risk assessment respectively.
- Common Event Format: being studied by WP:C-4 and WP:D-3, also as core component of the incident notification part of the accountability management life-cycle and the respective tool being developed by the later.
- Messaging abuse reporting format: applied the same rationale than for the "Common Event Format" above, except that in this case this standard is also considered by WP:D-3 for technical interoperability reasons.
- Privacy Level Agreements (PLA): this was the most referenced technical recommendation, cited by WP:C-2, WP:C-4, WP:C-6 and WP:D-3. PLA is actually aligned with some of the ongoing contributions of these WPs in the area of (cloud) data governance and data protection.

Once this subset of standards/recommendations was identified, the next step taken by WP:A-5 was to prioritize them based both on their relative importance for the technical WPs (see above), and also on the information available with respect to their expected maintenance life-cycle (when available). From these two perspectives, the prioritized list where WP:A-5 will focus its efforts during the following months is shown in Table 1.

Table 1. Focusing WP:A-5 efforts

SDO	Full Name	Comments
ISO/IEC	Information security management – Monitoring, measurement, analysis and evaluation (ISO/IEC 27004)	Feedback expected to be sent for the revision period (Q4/2014)

	Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology (ISO/IEC 19086-1) Privacy impact assessment – Methodology (ISO/IEC WD 29134)	
CSA	Privacy Level Agreements Cloud Trust Protocol Cloud Controls Matrix	Feedback expected to be sent for the revision period (Q3-Q4/2014)

At the moment of writing this deliverable, the timeline information related with the rest of standards/recommendations on the "Leveraged" list was not available. Nevertheless, WP:A-5 members are working closely with relevant groups (e.g., CSA International Standardization Council) to retrieve the missing information.

3.5 Opportunity to contribute

Based on the adopted WP:A-5 strategy for contribution to standards, this section analyses the opportunity of the A4Cloud project to contribute to ongoing standardisation activities. In that sense, it makes an overview of the areas of interest for the project and identifies those standardisation activities, in which A4Cloud could actively contribute, considering the timing scale of the expected study period and deliberation process. In order for the plan for contribution to be realistic and feasible, the project has decided to give priority to those standardisation efforts that the project partners are closely following, either as part of their everyday business (such as in the case of HP and CSA) or due to their participation in at least one of the working groups of the standardisation bodies. In that respect, the process for selecting the standardisation activities as the opportunities for contribution to standardisation is illustrated in Figure 6.

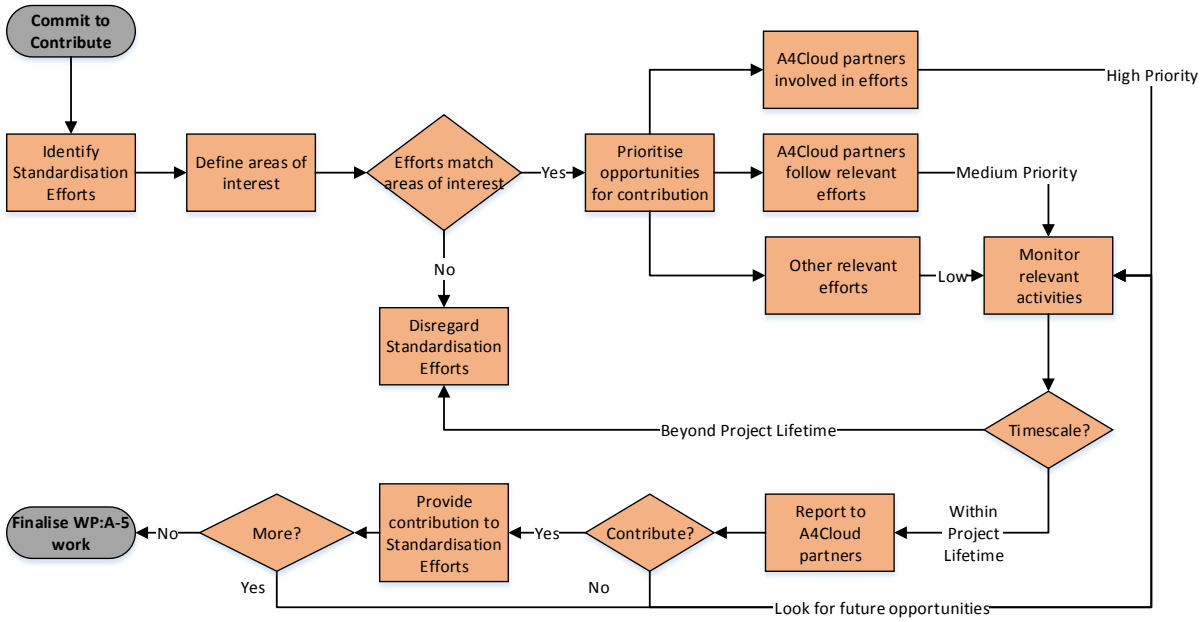

Figure 6. The process for identifying the opportunities for contribution

In the following lines, we analyse the process of Figure 6 and describe the rationale for the listed opportunities for contribution to standardisation effort.

Taking as granted the "identify standardisation efforts" step, in which we prepare the list of relevant standards and their gap to ongoing research and industrial activities (cf., Section 3.1), we define the areas of interest in which A4Cloud is conducting research and in which the standardisation effort could be supported by the project. Based on the "Description of Work" document, A4Cloud advances the state-of-the-art in the following research disciplines organized in Areas of Interest (AoI):

- AoI-1: Trustworthy architecture and protocols for interoperability

- AoI-2: Privacy assurance
- AoI-3: Architectures, protocols and models for trust assurance
- AoI-4: Management and governance frameworks
- AoI-5: Socio-economic framework to improve security and trust economics
- AoI-6: Interoperable governance and security policies and measures
- AoI-7: Transparent security

Thus, we limit the scope of potential contribution around these disciplines and we then define a strategy to narrow down the list of available organisations that we should monitor in order to identify the contribution opportunities (cf., Section 2.3). According to this strategy, A4Cloud is prioritising the monitoring of relevant standardisation activities around these seven AoI, based on the partners' involvement and engagement with the standardisation bodies. Then, the priority ranking is as follows:

- High priority: standardisation activities from relevant bodies, in which partners are members and are active contributors to standardisation efforts. In this category, the standards promoted by CSA, as an A4Cloud partner, are considered.
- Medium priority: standardisation activities, which partners actively follow as part of their academic or commercial activities
- Low priority: all the other standardisation activities being conducted in similar disciplines. Although it is too optimistic and rather hard to follow every single standardisation effort, we do not exclude from our future contribution such activities, in order to cover any arising opportunity for raising impact to certain communities.

The involvement of CSA in the A4Cloud Consortium acts as the dominant pole to orchestrate the identification of "opportunity to contribute" standards. In particular, CSA ISC is being exploited to speed up and optimise the process for monitoring opportunities for potential short-term contributions (usually with periods less than 6 months). As such, the CSA ISC have already prepared a list of standards being observed, which in many cases matches identified AoI and has become the de-facto basis for A4Cloud's "opportunity to contribute". The time scale for contribution is an important factor to determine which activities to monitor.

Taking into account the above, currently WP:A-5 focuses its potential chances for short-term contribution to the CSA-ISC list, which monitors the ongoing work performed by the Study Groups of International telecommunications Union (ITU) [32] and the subcommittees [33] of the Joint Technical Committee (JTC) of the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC). These two bodies concentrate much of the opportunities for contribution to the ongoing standardisation efforts and they are characterised by the fact that the work in these groups has an impact to other standardisation organisations with which they establish liaisons. Furthermore, we broaden our chances for potential contributions by monitoring the activities from other SDOs, which, mainly CSA and HP are closely following, such as the National Institute of Standards and Technology (NIST) [34] and the European Telecommunications Standards Institute (ETSI) [35].

In summary, the project is monitoring the following standardisation groups:

- The ongoing CSA standardisation efforts through the ISC. This is an important driver for the work performed in WP:A-5, since the CSA-ISC has already established liaisons with relevant working and study groups with the ITU-T and the ISO/IEC, while other SDOs, such as DMTF, OCDA, etc. are tracking the respective activities.
- The ITU-T Joint Coordination Activity on Cloud Computing (JCA-Cloud), which is responsible for leveraging standards on cloud computing inside the ITU-T community and coordinate the communication with other SDOs on similar topics.
- The ITU-T Study Group 13 (SG13) - Future Networks: this study group, currently, works on a set of questions around Security and Identity Management aspects (question Q8/13).
- The ITU-T Study Group 17 (SG17) - Security: this study group, currently, works on a set of questions around Cyber-security (Q4/17) and Cloud Computing Security (Q8/17). In particular for Q4/17, the group is working towards topics related to requirements and solutions for ICT accountability, incident response for cross domain boundaries applications, threat monitoring and risk communication.

- The technical committees of the ISO/IEC, including the joint technical committees (JTC), which are activated to examine the possibilities for revisions to standards, leverage the production of Draft international standards (DIS) and orchestrate the work in the different committees.
- The ISO/IEC-JTC 1/SC 27: this is a sub-committee on IT security techniques, which is split into five working groups (WG), of which only three are of relevance for A4Cloud:
  - The work in WG1 about Information Security Management Systems (ISMS), which involves the development and maintenance of the ISO/IEC 27000 ISMS standards family and the identification of requirements for future ISMS standards and guidelines.
  - The work in WG 4 about Security controls and services, which involves the refinement to the Information security incident management standard (ISO/IEC 27035) and the identification of requirements for and development of future service and applications standards and guidelines, for example in the areas of Business Continuity, Cyber Security and Outsourcing.
  - The work in WG 5 about Identity management and privacy technologies, which involves the definition of a Privacy Impact Assessment, Privacy Framework and the relevant Privacy Reference Architecture and the work around specific Privacy Enhancing Technologies (PETs) and privacy engineering.
- The ISO/IEC-JTC 1/SC 38: this is a sub-committee on Distributed application platforms and services (DAPS), which is split into three working groups (WG), of which the third one (WG3) is of relevance for A4Cloud, as it is about cloud computing. A dedicated study group on cloud computing has been announced from this SC 38, which aims to coordinate the liaison activities with other standardisation organisations.
- The NIST Cloud Computing program, which has developed an online collaboration site [36], to coordinate the publication of special reports around the work on cloud computing. For A4Cloud, of particular interest is the formation of the NIST Cloud Computing Security Working Group (NCC-SWG).
- The Cloud Standards Coordination (CSC) [37] of ETSI, which has been created to support the European Commission to produce the roadmap to cloud standardisation.

The above list of monitoring activities is enriched by following ad-hoc communication with SDOs and other working groups. The participation of the A4Cloud partners in these activities or the maintenance of good communication channels with such groups is a key point in order to effectively deliver a timely coordinated contribution to these groups. In Appendix D, we match the SDO monitoring activities with the A4Cloud areas of interest, while it, also, identifies specific topics for contribution and sketches a time plan for this (when available).

4 Orchestrating contribution to standards

The strategy discussed in Section 2 and further detailed in Section 3, has resulted on an initial set of contributions to SDO/standards/recommendations that were of interest to the consortium. Because most of these contributions occurred (or started) during the initial 15 months – 18 months of the project's duration, it can be expected that most of them relate to the "Opportunity to Contribute" list (cf., Section 3.5). However, we also highlight that two of the initiated actions (CCM and ISO/IEC 19086) actually corresponded to entries contained on the "Leveraged Standards" list (cf., Appendix C).

4.1 ISO/IEC DIS 17788/17789

ISO, IEC and ITU-T have decided to join forces to create fundamental standards addressing cloud computing. ISO/IEC has created a specific working group for cloud computing as part of the ISO – IEC Joint Technical Committee (JTC 1) Subcommittee on Distributed Application Platforms and Services (SC 38). The ITU-T Study Group on Future Networks and NGN (SG 13) has a Working Party on Cloud Computing which collaborates with ISO/IEC JTC 1 SC 38 to create two new standards which are currently in their final approval stage:

- ISO/IEC 17788 (aka. ITU-T Y.ccdef and Y.3500) [25] – provides an overview of cloud computing, and defines related terms.
- ISO/IEC 17789 (aka. ITU-T Y.ccra and Y.3502) [26] – specifies the cloud computing reference architecture, which includes the cloud computing roles, cloud computing activities as well as the cloud computing functional components and their relationships.

Both standards address Cloud Computing at a general level: ISO/IEC 17788 includes most of the security topics by reference, importing most definitions from ISO/IEC 27000 [27], while ISO/IEC 17789 makes reference to security, trust, and related concepts as cross-cutting aspects and addresses them in only a few paragraphs. Neither of these two standards is intended to be focused on security or any other cross-cutting aspects. Actually, ISO/IEC 17789 specifies that it "focuses on the requirements of "what" cloud services provide and not on "how to" design cloud-based solutions and implementations" and that it is "to enable the production of a coherent set of international standards for cloud computing" -a security and trust architecture would be an example of such a standard-.

We have however considered that it is important that the topic of accountability be addressed as one of the cross-cutting aspects, either independently or as facets of existing ones. Our review of the October 2013 drafts of the standards, then in DIS stage, highlighted that:

- There was no reference of the concept of accountability in ISO/IEC DIS 17788
- Accountability was only described in the context of data protection strategy and responsibility (section 8.5.12.5)[1] in ISO/IEC DIS 17789

Due to the very advanced development stage of the standards, substantial change requests would almost certainly not be granted. We nonetheless submitted a full set of comments for both standards (see Appendix E), which were submitted to the authoring teams through the CSA ISC [19].

Not unexpectedly, the review committee retained none of our proposals (see Appendix E). However, in updating the reference to the newer version of ISO/IEC 27000, the current FDIS version of ISO/IEC 17788 does now contain a reference to accountability in the context of Information Security (cf., Section 3.1.3 in [25]), which meets our objective. No changes in regards to accountability were detected in ISO/IEC 17789; it must however be noted that while we would have preferred to see a more holistic treatment of the topic, the current text does not preclude the creation of further cloud standards, *eg*. on security architecture or governance, which would introduce an in-depth treatment of the accountability topic.

[1] Accountability was also referenced once in the "CSC:Business manager" role description (section 8.2.1.3), but this was understood as financial accountability, which does not correspond to our definition of the term.

Both FDIS have been consented to (approved) by ITU-T on 7 July 2014. It now needs to get the final approval from ISO/IEC.

4.2 ISO/IEC WD 19086

Contracts and Service Level Agreements (SLAs) are key components defining cloud services, and are of particular importance for accountability and data protection. However, SLAs are arguably the least understood cloud attributes because of the complex language and terms of service from both a technical and legal perspective. This situation is exacerbated by the lack of widely accepted standard frameworks, vocabularies, along with a paucity of metrics and measurements associated with Service Level Objectives (SLOs) to assist cloud customers in meaningfully making decisions. This conspicuous gap in the field of cloud SLAs is recognized by the international cloud community, and has resulted in a process to develop of a related set of standards within ISO/IEC [20]. The first of these documents, focused on the creation of a common vocabulary/terminology for cloud SLAs, started more than one year ago and since then has been in the scope of WP:A-5 (cf., Appendix C).

Being an ISO/IEC initiative, the feedback from A4Cloud will have a greater impact if provided through organizations with a formal liaison with this SDO. This is the case of Cloud Security Alliance, which has a “CAT A” liaison with ISO/IEC (through its International Standardization Council [19]). It is expected that during October 2014, WP:A-5 lead partner CSA will be directly contributing with A4Cloud’s feedback to ISO/IEC 19086 “Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology” via this working group.

Furthermore, given the recognized importance of ISO/IEC 19086 to the objectives pursued by the European Cloud Strategy [21], the Cloud Special Industrial Group on Service Level Agreements (C-SIG SLA) has been devoting several efforts also to develop the EC input to this draft standard. A4Cloud (through WP:A-5) has been the main driver within the C-SIG SLA working group in the topics of security and data life-cycle SLOs. In particular, A4Cloud has provided relevant feedback to the C-SIG SLA/Gartner report on common terms of service [22] and also to the recently published standardization guidelines [23].

4.3 NIST Cloud Computing Cloud Service Metrics Description

Closely related to ISO/IEC 19086 (cf. Section 4.3), is also NIST’s work on cloud service metrics [24]. This draft document was identified within WP:A-5’s “Opportunity to Contribute” strategy (cf., Section 3.5), in particular given its relevance to the work performed by WP:C-5 on accountability metrics. A4Cloud started to collaborate with this NIST initiative on October-2013, and on January-2014 sent its initial feedback to the draft version of the metrics document. Provided feedback is shown on Appendix H.

The next version of the NIST draft document integrates part of the feedback sent by A4Cloud, in particular related with the initial alignment of the proposed cloud service metrics conceptual model and the one proposed by WP:C-5. The final version of the NIST recommendation is expected to be released late 2014/early 2015.

4.4 CSA Cloud Control Matrix and Open Certification Framework

In July 2013, the project provided a coordinated feedback to the open consultation period for the CSA Cloud Control Matrix so that version 3.0 could be released in September 2013. In Appendix G are shown the submitted comments in the control domains identified by CSA in this version of the CCM.

In order to consolidate this feedback to the CSA CCM, mainly WP:B-5, WP:C-2, WP:C-6 and WP:-D-2 contributed, but with the support of the work conducted in the other WPs as well.

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), defines the CSA Security, Trust & Assurance Registry (STAR), with three levels of compliance:

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

The process for levels 1 and 2 is already defined, while the process for level 3 is in the early stages. CSA has created the OCF Working Group, which is chartered to research in the area of cloud assurance and transparency certification [29]. The project has had the opportunity to appoint a representative to this working group.

CSA STAR Continuous Monitoring is particularly relevant to accountability. Most certification schemes, including CSA STAR Attestation and 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 Monitoring 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 C6 risk and trust model, where A4Cloud proposes and experiments with an approach for privacy preserving continuous monitoring for cloud risk indicators (see Deliverable 36.1 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 Monitoring.

CSA Continuous Monitoring has been announced for a 2015 availability. The OCF Working Group has revised its charter in February 2014, and A4Cloud through WP:A-5 have submitted four objectives. **These objectives have all been adopted** (as shown in the table below) and are therefore part of the design-objectives for the STAR schemes. It must be noted that these objectives address not only the functional aspects of accountability, but also the economic aspects (ROI) which are required for the scheme to be effectively adopted by Cloud providers.

Table 2. Objectives contributed to CSA's Open Certification Framework (Feb-2014)

Comment to the OCF WG Charter	Disposition of comment
We believe that there will be an increasing demand from Cloud users to select Cloud providers which offer a high level of accountability. We should investigate on how to relate/merge/cross-leverage the monitoring and reporting mechanisms used to demonstrate and track accountability with the mechanisms to be deployed as part of the OCF Level 3 – STAR Continuous, as applicable	ADOPTED
We should work with the GRC Stack and associated WG to ensure the controls and measures relevant to accountability are specified and integrated	ADOPTED
We should assess and monitor the economic feasibility and ROI (cost vs. benefits for an organization seeking certification) of the OCF. This is relevant for level 1 in terms of the controls to be deployed, but is even more important in regards to levels 2 and 3.	ADOPTED
Work with GRC Stack WG to define "OCF compliance profiles" (*eg.* subsets of CCM relevant to a certain sector, service offering, or compliance framework)	ADOPTED

[2] STAR Attestation is for the US market and is performed in association with a SOC2 Attestation, while STAR Certification is for the rest of the world and is associated with an ISO 27001 Certification.

4.5 ETSI CSC

The European Telecommunications and Standards Institute (ETSI), created in 2013 the Cloud Standards Coordination task force (CSC) following the request from the European Commission to develop a mapping of cloud standards for Europe (in particular for security, interoperability, data portability and reversibility). Since CSC was an open group, CSA participated on behalf of A4Cloud by providing feedback in relationship with the cloud standardization landscape (including relevant work and gaps). A4Cloud provided two main contributions to ETSI through WP:A-5:

1. The list of A4Cloud's checkpoint standards (cf., Section 3.1), which was extensively discussed and partially integrated into the final CSC report [14].
2. A gap analysis from the cloud security perspective, which concluded that "*…our analysis has shown that cloud computing governance and assurance standards specifically developed for and aimed at the cloud already exist (e.g., cloud controls framework, security cloud architectures, continuous monitoring of cloud service provider's) and some of them are considered as sufficiently mature to be adopted. Further standardization work may be helpful as a supplement to best practices in areas such as incident management, cloud forensics, and cloud supply chain accountability management."* [14]

Despite that the final ETSI CSC report is not a standard, its goal is to shape the research and standardization agendas of ETSI and other relevant SDOs. That is the main rationale behind A4Cloud's participation on this task force.

5 Focusing A4Cloud standardisation efforts

The methodology presented in Section 2 proved useful for identifying an initial set of standards of interest for A4Cloud (cf., Appendixes C and D). However, acknowledging the need to optimize the finite resources of work package A-5 on a realistic set of standardization activities, during the 4th A4Cloud General Meeting in Athens (September 23rd – 25th) the consortium agreed on focusing efforts on a *significant* set of standards. This section reports the major results from the General Meeting (including the A-5 working session), in particular related to the criteria used to qualify the significance of a standard with respect to A4Cloud, the results of the performed analysis (i.e., the selected set of standards), and the actions to be taken by A-5 in order to engage with each one of the chosen standards.

5.1 Methodology for the analysis

In order to further analyze and refine the lists of standards presented in Appendixes C and D, the methodological approach presented in this section (and shown in Figure 7) was proposed by A-5 and agreed with the rest of the consortium during the 4th General Meeting. The proposed approach seeks to qualify[3] the relative significance of each identified standard based on three main criteria:

1. Relevance: this criterion is useful to identify if a selected standard directly related to both accountability and any of A4Cloud's Areas of Interest or AoI (cf., Section 3.5). If after the analysis a standard obtained a "high" relevance score, this means that a related and relevant contribution is likely to be achieved by any of A4Cloud's WPs.
2. Opportunity/feasibility: this second criterion directly relates to the "Opportunity to contribute" presented in Section 3.5, where we analysed existing liaisons with standardization bodies and the timeliness of potential contributions[4]. A standard qualified with a "high" opportunity/feasibility means that an A4Cloud contribution has a high chance to be submitted to the SDO, and also is likely to be considered for further study by the standardization body.
3. Impact: this final criterion qualifies both the degree of maturity associated with a potential contribution from A4Cloud, and the actual importance (from the standardization perspective) of such contribution. For example, a standard with a "high" impact score means that the technical contribution has been developed/validated by A4Cloud, and the principles associated to this contribution are missing from the current version of the standard.

The full results of the analysis are shown in Appendix H and Table 8. The rest of this section will focus on presenting those standards that scored "high" in all three criteria, and which were also validated with the rest of he consortium during the 4th GM. The six selected standards (CSA Privacy Level Agreements, CSA Open Certification Framework, CSA Cloud Controls Matrix, ISO/IEC 19086, ISO/IEC 27005 and ISO/IEC 29134) are discussed also in terms of the strategy to follow for engaging with them i.e., point of contact within A-5, expected contribution/contributors, and timeline established by the respective SDO.

[3] With any of the *high, medium,* or *low* labels.

[4] Timeliness refers to identifying if the standard is accepting contributions (e.g., it is on a revision stage or it has started to be discussed on the standardization body).

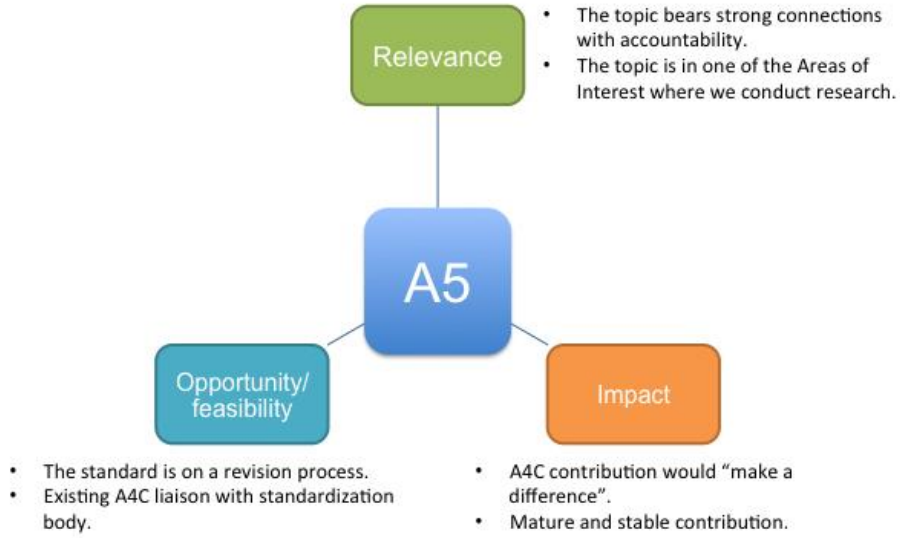

Figure 7. Focusing A4Cloud's standardization scope.

5.2 CSA Privacy Level Agreement

The Cloud Security Alliance (CSA) published in February 2013 a first version of the Privacy Level Agreement (PLA), PLA4EU v1 [3], as an output from its PLA Working Group (WG). The PLA is a standard that aims to provide a structured way for organisations to disclose information about privacy and data protection practices undertaken to comply with applicable data protection laws. PLA is intended to be used by cloud providers and (potential) cloud customers. Cloud providers would use PLA to disclose their offerings in terms of privacy and data protection measures; (potential) cloud customers would use PLA to assess the level of compliance of the cloud provider offerings with applicable data protection laws. Information to be disclosed in the PLA will differ depending on the data protection role played by the cloud providers.

Since July 2014 the PLA v2 WG has been working on the second version of the PLA with the ultimate objective to create a certification/seal for the worldwide cloud services market. The next step towards this goal will be turning PLA4EU v1 into a privacy compliance tool for cloud service providers offering services in the EEA.

EU Data protection law provisions are one of the sources of obligations considered within A4Cloud, and therefore it seems opportune to leverage the PLA standard to link the practices disclosed by cloud providers with the accountability mechanisms, tools and services that A4Cloud are building in order to support cloud providers in enforcing and monitoring what is agreed with their customers. In particular, C-4 has defined a policy language (A-PPL) for expressing obligations and D-3 has developed an engine (A-PPLE) able to enforce them, so it would be relevant to show how these can be linked to PLAs.

Within A5, HP has been taking part on the CSA PLA v2 WG, with the main contribution being related to the structure and the content of the accountability section that is being discussed. With regards to this section, another contribution is related to the introduction of the concept of evidence as defined and used within C-2 and C-8. The first draft of the PLA4EU v2 is expected to be created by the middle of October 2015; in the follow-up discussion there will be additional opportunities to contribute.
With regards to the relationship with other standardization activities, the PLA certification is planned to be used for assessing the feasibility of a Privacy Certification within the context of the CSA Open Certification Framework, which again is relevant for the A4Cloud project in terms of linkage to cloud monitoring, accountability evidence and certification.

5.3 CSA Open Certification Framework

The background and project objectives in regards to the CSA Open Certification Framework (OCF) can be found in Section 4.4. CSA STAR Continuous Monitoring, which is to provide a continuous auditing/assessment of relevant security properties[5], is of particular interest to the A4Cloud project, and will be the focus of our involvement. As highlighted in the objectives we contributed in February 2014 (cf., Table 2), and our aim is to ensure that, to the extent possible, the mechanisms deployed for this certification also provide a level of transparency and accountability in the cloud provider operations.

We envision our contributions will be through an active collaboration with the team developing the OCF –mainly to provide input on shaping the functionality of the tools and processes- rather than the direct contribution of material prepared by the A4Cloud project. While CSA STAR Continuous is announced for a Q1 2016 release, it has dependencies on two other working groups (CSA SLA and CSA CTP) which have not allowed the OCF chairs to propose a more concrete timeline.

5.4 CSA Cloud Controls Matrix

The Cloud Controls Matrix (CCM[6]) provides fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a CSP. It provides a control framework that gives detailed understanding of security concepts and principles that are aligned to the CSA guidance in 14 domains and is mapped to other industry-accepted security standards and regulations (e.g., ISO 27001/27002).

From the A4Cloud perspective, CSA CCM scored “high” in all three criteria defined in Section 5.1 given its significance related to the “Accountability Maturity Model” (AMM) jointly developed by C-2 and C-5. The AMM proposes a controls framework that captures the notions of accountability through the attributes defined by C-2, and the corresponding metrics defined by C-5. The AMM aims to guide organizations (in particular small and medium-sized enterprises -SME’s-), in assessing their level of accountability and identifying those particular aspects that need to be improved based on their organizational context.

The developed AMM (in particular the accountability controls) will be contributed to CSA CCM in order to enrich the current set of controls present on this framework with A4Cloud’s accountability attributes. Furthermore, A4Cloud expects that thanks to the foreseen validation in CSA CCM, the AMM can be also contributed during the duration of the project to other widely used cloud control frameworks like “ISO/IEC 27017 Information technology - Security techniques – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002”.

CCM provides major releases every year. The most recent release of CCM (version 3.01) was recently announced by CSA (July-2014), and A-5 is actively engaged in the development of the next major version (version 4.0, foreseen Q3 2015) where it is expected to contribute the refined AMM.
Because both C-2 and C-5 have finished (month 24), partners HP, CSA and UMA have agreed to continue collaborating through D-2 in order to develop the expected contributions to CSA CCM. It is worth to notice that these three partners (HP, CSA and UMA) were the major developers of the AMM.

5.5 ISO/IEC 19086

Nowadays, possibly the most well-known activity in the area of Cloud SLA standardization is being carried out by ISO/IEC JTC 1/SC38 on “19086 - Information Technology (Cloud Computing) Service Level Agreement (SLA) Framework and Terminology”. This prospective standard will be subdivided in three different parts:

1. The first part targets the definition of a standardized framework for Cloud SLAs (not only security-related), including both a vocabulary and comprehensive catalogue of commonly used SLO’s.
2. The second part plans for the definition of a conceptual model for Cloud SLA-related metrics.

[5] Please refer to https://cloudsecurityalliance.org/star/continuous/
[6] Please refer to https://cloudsecurityalliance.org/research/ccm/

3. The third part will discuss core requirements, related to the implementation of the proposed Cloud SLAs.

However, in the current version of the draft ISO/IEC 19086 standard, security aspects are not explicitly developed and instead the reader is referred to security controls catalogs such as ISO/IEC 27002 or NIST SP 800-53 R4 applicable to US Government agencies. From A4Cloud perspective, this is a major lack in this prospective standard because the actual challenges associated with the specification and usage of accountability in SLA's are never discussed. However, this gap also represents for A4Cloud the chance to make a "high impact" contribution to 19086. During the October-2014 ISO/IEC SC38 meeting, the Technical Committee decided to create a liaison to ISO/IEC SC27 over the idea of a new working document (ISO/IEC 19086-4) for security and privacy. This was A4Cloud desired outcome, and the final decision from SC27 is expected early November.

A-5 has identified ISO/IEC 19086 as a highly relevant standard for the project[7], given its direct relationship to C-2 (notions of accountability), C-5 (metrics), C-8 (evidence) and D-4 (contracts and SLA's). Also the "opportunity" to contribute is high, given the CAT-A liaison of CSA with ISO/IEC SC38 (the committee in charge of 19086), and the open working period for developing these three standards (expected to be released between Nov-2014 and Nov-2015).

It is also worth to notice that ISO/IEC 19086 is directly related to other standardization initiatives (e.g., NIST's cloud SLA and service metrics), and EU activities (including the C-SIG SLA, the FP7 projects SPECS[8] and CUMULUS[9], and H2020's SLA-Ready[10]). Therefore, A4Cloud's envisioned contributions on the field of accountability will also positively impact these related activities.
A4Cloud partners HP, UMA, CSA, and TiU have committed to develop the contributions to ISO/IEC 19086 through A-5.

5.6 ISO/IEC 27005

In this section we first give an abstract presentation of the ISO/IEC 27005 standard (Information technology – Security techniques – Information security risk management), and then we identify a possible contribution or interactions with respect to C-6. The ISO27005 standard is relevant to managers and staff concerned with information security risk management within an organization. It is based on previous standards for information security and part of the ISO/IEC 27000 families of standards. It is also strongly linked with ISO 31000, industry risk management, and some parts have been restructured according to it. The objective of ISO/IEC 27005 is to provide guidelines for information security risk management, and to assist the correct implementation of security based on a risk management approach. ISO/IEC 27005 is not an analysis method for IT by the contrary it is devoted to define a general, holistic process from analyzing risks to creating the risk treatment plan.

Our analysis of the potential A4Cloud synergies identified WP C-6 (Risk and Trust Modeling), as a potential contributor for this standard. In short, C-6 proposes and experiments with an approach for privacy preserving continuous monitoring for cloud risk indicators. Important key words are risk and trust model, and risk assessment. Clearly there is an overlap between C-6 and ISO/IEC 27005 that will be further explored during the following months. Referring to deliverable D:C-6.1 we can observe a proposition of process for an accountability-based approach to risk management. The deliverable addresses the first steps: establishing context, risk assessment and risk treatment. Risk monitoring will be the subject of a future deliverable. The current process described in D:C-6.1 is aligned with the one from ISO/IEC 31000, but it can be also aligned with ISO/IEC 27005. This later is more specifically devoted to IT risk management, and the process is particularly more detailed on the risk assessment part. Overall, our belief is that C-6 might have a higher impact on.

[7] Please also refer to Section 4.2 for a discussion on the current contributions being provided to ISO/IEC 19086.
[8] Please refer to http://specs-project.eu/
[9] Please refer to http://www.cumulus-project.eu/
[10] Please refer to http://www.sla-ready.eu/

The new version of ISO/IEC 27005 is on a DIS[11] stage, which means that there are still opportunities to provide contributions to the technical content.

5.7 ISO/IEC 29134

ISO/IEC 29134 has been produced by the Joint Technical Committee 1 of the Scientific Committee 27 (JTC 1/SC 27) and is about the methodology for the specification of the privacy impact assessment (PIA), when developing privacy related mechanisms and security techniques in the IT domain. The PIA in this standard is considered as a process for assessing the impact of the processing of the personal identifiable information (PII) on the privacy of an IT asset (i.e. project, technology, service, etc.). The privacy implications are analysed, according to legal and regulatory requirements and aim to decide on the appropriate remediation actions in order to avoid, mitigate or minimize the exposure of privacy risks with negative impact to the overall security of the IT asset. As a result, this standard offers a PIA framework to guide managers and other staff, responsible for or concerned with the lifecycle of IT assets involving the processing of PII, on how to conduct a PIA within their organisation and better manage the privacy risks arising from the processing of PII.

In this context, the work conducted in A4Cloud is highly relevant to this standardisation effort. Section 6 of the standard working draft refers to the process for implementing a PIA. This privacy oriented analysis can be extended with the accountability perspective, as it is introduced in the A4cloud accountability framework (see WP:C-2), focusing on the way that the Data Protection Impact Assessment process takes advantages of the risk and trust modelling to assess on the relevant data protection risks affecting privacy and security (see WP:C-6). For example, the implementation guidance on ISO/IEC 29100:2011 privacy principles that should be considered in the ISO/IEC 29134 could be instantiated in the case of the controls explaining the compliance with the accountability principle (see section 6.2.2 of the ISO/IEC 29134 standard).

On Section 6.1.3 of the standard, a sample PIA plan is still pending. A4Cloud could contribute with referencing to the necessary steps and necessary resources to run a data protection impact assessment process and connect these steps to the implementation of a PIA framework (see WP:C-6). Furthermore, Section 6.2.1 could be enriched with the actions involved in the accountability practice for demonstrating compliance with relevant policies. In this sense, the PII life cycle can take advantage of the process introduced in A4Cloud (see WP:C-8) about enforcing external auditing. Finally, in section 7 of the standard a recommended structure for the PIA report is presented, which can be reviewed by the work performed in WP:C-6 and enriched, in accordance to the structure of the DPIAT report structure. Potentially, this PIA report could be connected to the A4Cloud work on accountability maturity model (AMM), as it is described in WP:C-2

The ISO/IEC 29134 strongly relates to work performed in the ISO/IEC 29100 (on the privacy framework), the ISO/IEC 27000 (on the information security management systems) and the ISO 31000 (on the principles and guidelines on implementation of the risk management) standards. This standard is at 20.20 stage, meaning that it is under its 4th working draft (WD) edition and the committee is receiving comments on potential improvement. Thus, A4Cloud is continuously monitoring the provided time plan for technical contributions, exhibiting a chance to be involved in the commenting period for this standard, till it is advancing to the committee draft (CD) stage. The study initiated in this standard will be finalised by November 2016.

5.8 Summary

This section presented the methodological approach adopted by A-5 to identify a highly significant set of standards/best-practices, where A4Cloud's standardization efforts will focus for the remaining of the project's duration. The performed analysis identified three best practices from the Cloud Security Alliance (i.e., Privacy Level Agreements, Cloud Controls Matrix, and Open Certification Framework), and three ISO/IEC standards (19086 – Service Level Agreements, 27005 – Risk Management, and 29134 – Privacy Impact Assessment). For each identified entry this section discussed the rationale for selecting it, a summary of the expected A4Cloud contribution, and the partners/work packages that will be providing the contribution through A-5. Furthermore, we also identified other related initiatives

[11] Please refer to http://www.iso.org/iso/home/standards_development.htm

(including standards and EU projects) that will indirectly benefit from the expected A4Cloud contributions.

The next version of this deliverable (D:A-5.2) will report in detail the overall SDO engagement process, and outcomes obtained from A4Cloud's contributions to the identified standards and best practices.

6 Conclusion

This initial deliverable on A4Cloud standardization presented the methodological approach developed by WP:A-5 to (i) map/analyze the relevant standardization landscape, and (ii) orchestrate the project's contributions to a well-defined set of standards and technical recommendations. Furthermore, this deliverable also discussed some initial collaboration with identified SDOs, in particular within the areas of assurance, cloud accountability metrics and cloud service level agreements.

As discussed in Section 2, it is important to notice that WP:A-5 cannot guarantee that the feedback provided to identified standardization/best practices activities will actually become part of the finalized version of the document. The strategy developed by WP:A-5 is based on due-diligence and aims to focus the efforts of the group in orchestrating feedback to relevant SDOs, but there are many factors (some of which are outside of A4Cloud control) involved in the actual final decision of the standardization body.

Many SDOs currently exhibit a period of "work under study" for their standardisation activities. This is a primary pool of potential chances for the A4Cloud project to contribute the identified lack of the existing standardisation activities to control and drive the implementation of secure ICT systems. The opportunities for A4Cloud contribution in the enhancement of the future standardisation results is based on the fact that the project exploits the strong relationships of some partners with these SDOs, which enables active monitoring of the relevant activities and reporting back to the project for any potential opportunity for contribution. As already mentioned, the project goes beyond that and diligently considers also "external" activities from the pool of existing SDOs that are periodically monitored to identify any chances to broaden the contribution potentials beyond the partners' communication channels. The study period being established for some bodies is an excellent opportunity for the project to actively participate in the discussions about the roadmap to shape the standardisation for the next years, including establishment of new standards and revision of obsolete ones.

The next (and final) deliverable in WP:A-5 will have two main outcomes. On one hand, will summarize the results (*e.g.*, which basic notions developed in A4Cloud were *injected* into relevant standards?) of our contribution to identified standards as performed during the rest of A4Cloud's duration, and based on the strategy depicted in Section 2 and Section 3. On the other hand, the final WP:A-5 deliverable will provide a roadmap for cloud accountability standardization, which can be adopted by (industrial) partners that would like to continue engaging with identified SDOs after the project's duration. This activity will be part of A4Cloud's sustainability plan.

References

[1] Online: http://uclslang.sourceforge.net
[2] Online: http://www.ogf.org/documents/GFD.192.pdf
[3] Online: https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf
[4] Online: https://cloudsecurityalliance.org/research/cloudaudit/#_downloads
[5] Online: http://dmtf.org/sites/default/files/standards/documents/DSP0262_1.0.0b.pdf
[6] Online: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44344
[7] Online: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106
[8] Online: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
[9] Online: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[10]Online: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf
[11]Online: http://www.veriscommunity.net/doku.php
[12] Online: https://cloudsecurityalliance.org/research/ccm/
[13]ITU-T Technology Watch Report , Privacy in Cloud Computing, March 2012
[14]European Telecommunications Standards Institute. “ETSI Cloud Standards Coordination Final Report”. Technical Report. November 2013. Online: http://www.etsi.org/images/files/Events/2013/2013_CCs_Delivery_WS/CCs-Final_report-013-CCs_Final_report_v1_0_PDF_format-.PDF
[15]National Institute of Standards and Technology. “NIST SP-291: Cloud Computing Standards Roadmap”. Technical Report. NIST, 2011. Online: http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
[16]EU FP7 Project CIRRUS “Certification, InteRnationalisation and standaRdization in cloUd Security”. Online: http://www.cirrus-project.eu/
[17]EU FP7 Project CloudWatch. Online: http://www.cloudwatchhub.eu/
[18]International Organization for Standardization. “Stages of the development of International Standards". August, 2007. Online: http://www.iso.org/iso/home/standards_development/resources-for-technical-work/support-for-developing-standards.htm
[19]CSA International Standardization Council. Online: https://cloudsecurityalliance.org/isc/
[20] International Organization for Standardization. “ISO/IEC 19086: Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology”. Working document. ISO/IEC, March, 2014.
[21]European Cloud Strategy. Online: http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[22]Gartner research. “Cloud service provisions: Draft suggestions for common terms of service and SLA’s for cloud service contracts”. Technical Report. European Commission - DG Communications Networks, Content & Technology. 2014.
[23]European Commission, “Cloud Service Level Agreement Standardisation Guidelines”, Technical Report, Cloud Select Industry Group (C-SIG), June 2014. Online: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[24]National Institute of Standards and Technology .“NIST Cloud Computing: Cloud Service Metrics Description (RATAX)”. Working document. 2014
[25]ISO/IEC DIS 17788 “Information technology -- Cloud computing -- Overview and vocabulary”. ISO online store http://www.iso.org/iso/catalogue_detail.htm?csnumber=60544 (expected to become available at no charge once finally approved and released)
[26]ISO/IEC DIS 17789 “Information technology -- Cloud computing -- Reference architecture”. ISO online store http://www.iso.org/iso/catalogue_detail.htm?csnumber=60545 (expected to become available at no charge once finally approved and released)
[27]ISO/IEC 27000 “Information technology — Security techniques — Information security management systems — Overview and vocabulary”. Online http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

[28]CEN-CENELEC “Type of Standards” web page – http://www.cencenelec.eu/research/innovation/standardstypes/Pages/default.aspx
[29]CSA “Open Certification Framework - Working Group Charter”, working document, February 2014 Online: https://cloudsecurityalliance.org/research/ocf/#_overview
[30]CSA “Cloud Security Alliance Releases New Cloud Controls Matrix v3.0.1 and Consensus Assessments Initiative Questionnaire v3.0.1” – Online https://cloudsecurityalliance.org/media/news/csa-releases-new-ccm-caiq-v3-0-1/
[31]The Open Group “Open Information Security Management Maturity Model (O-ISM3)” The Open Group Technical Standard, Reference C102, US ISBN 1931624860, Feb 2011
[32]Online: http://www.itu.int/en/ITU-T/studygroups/2013-2016/Pages/default.aspx
[33]Online: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020&tab=structure
[34]Online: www.nist.gov/
[35]Online: www.etsi.org/
[36]Online: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome
[37] Online: http://csc.etsi.org/website/home.aspx

Appendix A. Checkpoint list of standards

Table 3. Checkpoint list of standards

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[AJAX01]	n/a	Asynchronous Javascript and XML	AJAX	Other	Widely Adopted	Public	Published	
[APEC01]	APEC	Cross-border privacy enforcement arrangement (CPEA)	APEC CPEA	Specification	Adopted	Public	Published	28 Feb 2010
[AS01]	ArcSight	Common Event Format	CEF	Standards	Widely adopted	Public	Published	17 July 2009
[CC01]	Common Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	CCMB-2012-09-001	Specification	Widely adopted	Public	Published	Version 3.1, Revision 4, September 2012.
[CC02]	Common Criteria	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components.	CCMB-2012-09-003	Specification	Widely adopted	Public	Published	Version 3.1, Revision 4, September 2012.
[CCUC01]	Cloud Computing Use Cases Discussion Group	Cloud Computing Use Cases White Paper	CC UC	report/white paper	Adopted	Public	Published	v4.0 - 2 July 2010
[CE01]	Council of Europe	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	n/a	report/white paper	Widely adopted	Public	Published	28 Jan 1981, amended on 15 June 1999, aditional protocol on 8 Nov 2001
[CIPL01]	CIPL	Galway Project, Accountability Project	CIPL Galway	report/white paper	Adopted	Public	Published	
[CIPL02]	CIPL	Data protection accountability: the essential elements. A document for discussion	CIPL DP	report/white paper	Adopted	Public	Published	October 2009

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[CIPL03]	CIPL	Demonstrating and measuring accountability: a discussion document	CIPL DEM	report/white paper	Adopted	Public	Published	October 2010
[CIPL04]	CIPL	Accountability: A Compendium for Stakeholders	CIPL	report/white paper	Adopted by IAPP	Public	Published	March 2011
[CIS01]	CIS	The CIS Security Metrics	CIS Security Metrics	Specification	Adopted by NASA.	Public	Published	v1.1.0 - 1 Nov 2010
[CNIL01]	CNIL	Methodology for Privacy Risk Management	CNIL	report/white paper	Adopted	Public	Published	June 2012
[CNSSI01]	CNSSI	National Information Assurance (IA) Glossary	CNSS Instruction No. 4009	report/white paper	Widely adopted in US	Public	Published	26 April 2010
[COSO01]	COSO	Enterprise Risk Management for Cloud Computing	n/a	report/white paper	Adopted	Public	Published	June 2012
[CSA01]	CSA	Cloud Trust Protocol	CTP	Specification	Adopted in cloud security.	Public	Published	v2.0 - Sep 2010
[CSA02]	CSA	Privacy Level Agreements	PLA	Specification	Adopted	Public	Published	Feb 2013
[CSA03]	CSA	CloudAudit	A6	Specification	Adopted	Public	Published	August 2010
[CSA04]	CSA	Guidance for Critical Areas of Focus in Cloud Computing	n/a	report/white paper	Adopted	Public	Published	V3.0 - 14 Nov 2011
[CSA05]	CSA	The Notorious Nine Cloud Computing Top Threats in 2013	n/a	report/white paper	Adopted	Public	Published	Feb 2013
[CSA06]	CSA	Cloud Controls Matrix	CCM	Specification	Widely adopted.	Public	Published	V3.0 - 26 Sep 2013
[CSA07]	CSA	Consensus Assessments Initiative Questionnaire	CAIQ	Specification	Adopted	Public	Published	v1.1 - 1 Sep 2011
[CSA08]	CSA	Open Certification Framework	OCF	Specification	Adopted	Public	Published	Rev 1 - August 2013
[CSA09]	CSA	Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0	n/a	report/white paper		Public	Published	

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[DMTF01]	DMTF	Cloud Auditing Data Federation (CADF) - Data Format and Interface Definitions Specification	CADF	Specification	Not adopted	Public	Draft/Incubator	v1.0.0b - 18 June 2013
[DMTF02]	DMTF	Cloud Infrastucture Management Interface - Common Information Model	CIMI - CIM DSP0264	Standards	Used as self-service interface for infrastructure clouds.	Public	Published	v1.0.0 - 14 Dec 2012
[EC01]	European Commission	Directive 1999/93/EC - advanced and qualified signature requirements	n/a	report/white paper	Adopted	Public	Published	19 Jan 2000
[EC02]	European Commission	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'	n/a	Specification	Widely adopted	Public	Published	24 Oct 1995
[EC03]	European Commission	Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'	n/a	Specification	Not adopted	Public	Draft/Incubator	25 Jan 2012
[EC04]	European Commission	Digital "to-do" list: new digital priorities for 2013-2014	n/a	report/white paper	Widely adopted	Public	Published	18 Dec 2012
[EC05]	European Commission	Digital Agenda Pillar III: Trust and Security	n/a	report/white paper	Widely adopted	Public	Published	
[ECRYPT01]	ECRYPT	Yearly report on key length and algorithms	ECRYPT	report/white paper	Adopted	Public	Published	Rev 1 - 30 Sep 2012
[EDPS01]	EDPS	Glossary of terms	n/a	report/white paper	Widely adopted	Public	Published	2001
[EDPS02]	EDPS	Opinion on the Data Reform Package	n/a	report/white paper	Not adopted	Public	Draft/Incubator	March 2013
[EDPS03]	EDPS	Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe".	n/a	report/white paper	Not adopted	Public	Draft/Incubator	16 Nov 2012

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[EDPS04]	EDPS	Responsibility in the Cloud should not be up in the air	n/a	report/white paper	Not adopted	Public	Draft/Incubator	16 Nov 2012
[ENISA01]	ENISA	Cloud Computing: Benefits, Risks and Recommendations for Information Security	n/a	report/white paper	Adopted	Public	Published	Rev B - Dec 2012
[ENISA02]	ENISA	Technical guidance on the incident reporting in Article 13a	n/a	report/white paper	Adopted	Public	Published	v2.0 - Jan 2013
[ENISA03]	ENISA	Privacy, Accountability and Trust - Challenges and Opportunities	n/a	report/white paper	Adopted	Public	Published	Feb 2011
[ENISA04]	ENISA	ENISA Cloud Computing Risk Assessment	n/a	report/white paper	Adopted	Public	Published	20 Nov, 2009
[EUJ01]	European DG of Justice	The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data	n/a	report/white paper	Not adopted	Public	Draft/Incubator	1 Dec 2009
[EUJ02]	European DG of Justice	Opinion 3/2010 on the principle of accountability	n/a	report/white paper	Not adopted	Public	Draft/Incubator	13 July 2010
[EUJ03]	European DG of Justice	Opinion 05/12 on Cloud Computing	n/a	report/white paper	Not adopted	Public	Draft/Incubator	1 July 2012
[GSMA01]	GSMA Mobile and Privacy	Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development	n/a	Specification	Adopted	Public	Published	Feb 2012
[GUI01]	n/a	A Guide to the Project Management Body of Knowledge	n/a	report/white paper		Public	Published	
[HN01]	Help Net Security (2012a)	The threat landscape continues to expand rapidly	n/a	report/white paper	Not adopted	Public	Draft/Incubator	31 Dec 2012
[HN02]	Help Net Security (2012b)	Guidance on cybersecurity, private clouds and privacy	n/a	report/white paper	Not adopted	Public	Draft/Incubator	21 Dec 2012

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[ICDPP01]	ICDPP	International Standards on the Protection of Personal Dat and Privacy - the Madrid Resolution	n/a	report/white paper	Adopted	Public	Draft/Incubator	5 Nov 2009
[ICO01]	ICO	Binding corporate rules	BCR	Specification	Adopted	Public	Published	8 April 2009
[ICO02]	ICO	Guidance on the Use of Cloud Computing	n/a	report/white paper	Adopted	Public	Published	version 1.1, 2012
[IDC01]	IDC	Removing Barriers to Cloud Computing in Europe Through Policy Action Could Generate up to €250Bn EU GDP Growth in 2020, says IDC	n/a	report/white paper		Public	Published	
[IETF01]	IETF	Abuse Reporting Format	ARF	Standards	Adopted	Public	Published	June 2012
[IETF02]	IETF	Messaging abuse reporting format	M-ARF	Specification	Adopted	Public	Published	26 Jan 2010
[IETF03]	IETF	Hypertext Transfer Protocol	HTTP	Specification	World wide adopted	Public	Published	June 1999
[IETF04]	IETF	oAuth	oAuth	Specification	Widely Adopted / Adopted	Public	Published	October 2012
[IETF05]	IETF	Transport Layer Security/Secure Sockets Layer (RFC 5246)	SSL/TLS	Specification	Adopted	Public	Published	Version 1.2 - Auguts 2008
[IETF06]	IETF	Javascript Object Notation	JSON	Specification	Adopted	Public	Published	July 2006
[IETF07]	IETF	Password-Based Key Derivation Function 2	PBKDF2	report/white paper	Widely adopted.	Public	Published	January 2011
[IETF08]	IETF	Terminology for Policy-Based Management (RFC 3198)	n/a	Other	Adopted	Public	Published	November 2001
[IIA01]	Institute of Internal Auditors	Managing and Auditing Privacy Risks - replaced by Practice Guide: Auditing Privacy Risks, 2nd Edition	n/a	Specification	Adopted	Public at cost	Published	July 2012
[IPC01]	IPC	Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers	n/a	report/white paper	Adopted	Public	Published	August 2011

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[ISO01]	ISO	Information technology – Security techniques – Privacy framework	ISO/IEC 29100:2011	Standards	Adopted	Public	Published	5 Dec 2011
[ISO02]	ISO	Information security incident management	ISO 27035	Standards	Adopted	Public at cost	Published	8 Nov 2011
[ISO03]	ISO	Information technology -- Open Distributed Processing -- Reference Model: Foundations, 11.2.4, 11.2.5, 11.2.6, 11.2.7	ISO/IEC 10746-2:2009	Standards	Adopted	Public at cost	Published	15 Dec 2009
[ISO04]	ISO	Information technology -- Open distributed processing -- Reference model -- Enterprise language, 6.4.1, 6.4.2, 6.5.6	ISO/IEC 15414:2006	Standards	Adopted	Public at cost	Published	18 Sep 2013
[ISO05]	ISO	Systems and software engineering – Measurement process. 2007	ISO/IEC 15939:2007	Specification	Adopted	Public at cost	Published	19 Dec 2012
[ISO06]	ISO	Information technology - Security techniques - Information security management systems - Overview and vocabulary	ISO/IEC 27000:2014	Standards	Adopted	Public	Published	15 Jan 2014
[ISO07]	ISO	Information Technology – Security techniques – Information Security Management – Measurement. 2009	ISO/IEC 27004:2009 (E)	Standards	Adopted	Public at cost	Published	11 June 2013
[ISO08]	ISO	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models	ISO/IEC 25010:2011	Standards	Adopted	Public at cost	Published	1 March 2011
[ISO09]	ISO	Common Criteria	ISO 15408-1:2009, -2:2008, -3:2008	Standards	Adopted	Public	Published	
[ISO10]	ISO	Guidelines for identification, collection, acquisition, and preservation of digital evidence	ISO 27037:2012	Standards	Adopted	Public at cost	Published	15 October 2012
[ISO11]	ISO	ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements	ISO 27001:2013	Standards	Adopted	Public at cost	Published	25 September 2013
[ISO12]	ISO	ISO/IEC 27002:2013 -Information technology - Security techniques - Code of practice for information security controls	ISO 27002:2013	Standards	Adopted	Public at cost	Published	September 2013

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[ISO13]	ISO	Information security for supplier relationships	ISO 27036-1:2014	Standards	Adopted	Public	Published	1 Apr 2014
[ISO14]	ISO	Generic Standard for Risk Management - Risk assessment techniques	ISO 31010	Standards	Adopted	Public at cost	Published	1 Dec 2009
[ISO15]	ISO	Generic Standard for Risk Management - Principles and guidelines	ISO 31000	Standards	Adopted	Public at cost	Published	13 Nov 2009
[ISO16]	ISO	Information Security Glossary	ISO ISG	Standards	Adopted	Public	Published	2nd version - 2012
[ISO17]	ISO	Unified Modeling Language	ISO 19501	Standards	Adopted	Public	Published	6 May 2012
[ISO18]	ISO	ISO/IEC 38500:2008 - Corporate governance of information technology	ISO/IEC 38500:2008	Standards	Adopted	Public at cost	Published	2008
[ISO19]	ISO	Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology	ISO/IEC 19086-1, -2, -3	Standards	In Development	Non Public	Draft/Incubator	n/a
[ITU01]	ITU	Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements	FG-Cloud-TR-1	Standards	Adopted	Public	Published	Version 1.0 - February 2012
[ITU02]	ITU-T	X.509 : Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	X.509	Standards	Adopted	Non Public	Published	October 2012
[JF01]	Jericho Forum	Cloud Cube Model: Selecting Cloud Formations for Secure Colaboration, Version 1.0	n/a	report/white paper	Not adopted	Public	Published	version 1.0 - April 2009
[JLC01]	Justice Laws Website Canada	Personal Information Protection and Electronic Documents Act	n/a	report/white paper	Adopted	Public	Published	9 Dec 2013
[NIST01]	NIST	Assessment of Access Control Systems	Interagency Report 7316	report/white paper	Adopted	Public	Published	September 2006
[NIST02]	NIST	Glossary of Key Information Security Terms	NIST IR 7298: Revsion 1	Specification	Adopted	Public	Published	Revision 2 - 31 May 2013
[NIST03]	NIST	NIST Cloud Computing Standards Roadmap	NIST SP 500-291	Specification	Adopted	Public	Published	July 2011

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[NIST04]	NIST	NIST Cloud Computing Reference Architecture	NIST SP 500-292	Specification	Adopted	Public	Published	September 2011
[NIST05]	NIST	NIST Guidelines for Security and Privacy in Cloud Computing	NIST SP-800-144	report/white paper	Adopted	Public	Published	December 2011
[NIST06]	NIST	The NIST Definition of Cloud Computing	NIST SP 800-145	report/white paper	Adopted	Public	Published	September 2011
[NIST07]	NIST	Security Metrics Guide for Information Technology System (July 2003)	SP 800-55 Rev	Specification	Adopted	Public	Published	July 2008
[NIST08]	NIST	Recommended Security Controls for Federal Information Systems and Organizations	NIST SP-800-53	Specification	Adopted	Public	Published	Revision 4 - July 2013
[NIST09]	NIST	Secure Hash Algorithm Series	SHA-*	Standards	Widely adopted.	Public	Published	2012
[NIST09b]	NIST	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions	SHA-3	Standards	Draft	Public	Draft/Incubator	May 2014
[NIST10]	NIST	Advanced Encryption Standard	AES	Standards	Widely adopted.	Public	Published	26 November 2011
[NIST11]	NIST	Guidelines for Improving Security and Privacy in Public Cloud Computing (ITL BULLETIN FOR MARCH 2012)	n/a	report/white paper	Adopted	Public	Published	March 2012
[NIST12]	NIST	Cloud Computing Synopsis and Recommendations	SP 800-146	report/white paper	Adopted	Public	Published	May 2012
[NIST14]	NIST	Recommendation for Key Management – Parts 1-3	SP 800-57 1-3	report/white paper	Adopted	Public	Published	July 2012
[NIST15]	NIST	Security Content Automation Protocol	SCAP SP-800-126	Specification	Adopted	Public	Published	version 1 - Nov 2009
[NIST16]	NIST	Media Sanitization	SP 800-88 Rev	Specification	Draft	Public	Draft/Incubator	September 2012
[NIST17]	NIST	Trusted computer system evaluation criteria	NIST DOD85	Specification	Adopted	Public	Published	26 Dec 1985
[NIST18]	NIST	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	SP 800-27 rev A (EP-ITS)	Specification	Adopted	Public	Published	June 2004
[OASIS01]	OASIS	Extensible Access Control Markup Language	XACML	Standards	Adopted	Public	Published	22 January 2013

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[OASIS02]	OASIS	A brief Introduction to XACML	n/a	report/white paper		Public	Published	
[OASIS03]	OASIS	Cloud Application Management for Platforms	CAMP	Specification	Adopted	Public	Published	Version 1.1, 31 July 2013
[OASIS04]	OASIS	Topology and Orchestration Specification for Cloud Applications	TOSCA	Specification	Adopted	Public	Published	Version 1.0, 18 March 2013
[OECD01]	OECD	Guidelines for the protection of personal data and transborder data flows	n/a	report/white paper		Public	Published	11 July 2013
[OGF01]	OGF	Web-Service Agreement	WS-Agreement	Standards	Adopted	Public	Published	October 2011
[OMG01]	OMG	Business Process Definition Metamodel	BPDM	Specification	Adopted	Public	Published	Version 1.0, Nov 2008
[OPC01]	OPC	Privacy Impact Assessments	PIA	report/white paper		Public	Published	
[OPC02]	OPC	Getting Accountability Right with a Privacy Management Program	n/a	report/white paper	Adopted	Public	Published	April 2012
[PON01]	PONEMON Institute	Security of Cloud Computing Users 2013 Study	n/a	report/white paper	Adopted	Public	Published	March 2013
[SEI01]	SEI (Software Engineering Institute)	CMMI for development: Improving processes for developing products and services	CMMI-DEV, V1.3	report/white paper	Adopted	Public	Published	Version 1.3, November 2012
[UCL01]	UCL (University College London)	SLA Language Spec	SLANG	Specification	Adopted	Public	Published	Revision 1.1
[UKICO01]	UK ICO	Privacy Impact Assessment Handbook	PIA	report/white paper	Adopted	Public	Published	Version 2
[VER01]	Verizon	Vocabulary for Event Recording and Incident Sharing	VERIS	report/white paper	Adopted	Public	Published	Version 1.2.1
[W3C01]	W3C	HTML5 Device APIs	HTML5	Specification	Adopted	Public	Draft/Incubator	Version 5.1, January 2014
[W3C02]	W3C	Hypertext Markup Language	HTML	Specification	Widely adopted	Public	Published	Version 4.01, 24 December 1999
[W3C03]	W3C	Extensible Markup Language	XML	Specification	Adopted	Public	Published	XML1.1 (second edition), Spetember 2006

Unique ID	Organisation	Full title	Acronym	Type	Adoption	Availability	Status	Version
[W3C04]	W3C	Content Security Policy	CSP	Specification	Adopted	Public	Published	v1.0, 15 November 2012
[W3C05]	W3C	Web Service Description Language	WSDL	Specification	Adopted	Public	Published	V1.1, 15 March 2001
[XARF01]	X-ARF community	Extensible abuse reporting format	X-ARF	report/white paper	Adopted	Public	Published	v0.2, February 2013

Appendix B. Compliance with standards (per WP)

Table 4. Compliance with standards

Unique ID	Type	Full title	Acronym	B3	C2	C3	C4	C5	C6	C7	C8	D2	D3	D4	D5	D6	D7
[CIS01]	Specification	The CIS Security Metrics	CIS Security Metrics					x									
[CSA02]	Specification	Privacy Level Agreements	PLA		x												
[CSA06]	Specification	Cloud Controls Matrix	CCM		x			x									
[CSA07]	Specification	Consensus Assessments Initiative Questionnaire	CAIQ		x			x									
[CSA08]	Specification	Open Certification Framework	OCF		x												
[EC02]	Specification	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'	n/a	x													
[EC03]	Specification	Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'	n/a	x													
[IIA01]	Specification	Managing and Auditing Privacy Risks - replaced by Practice Guide: Auditing Privacy Risks, 2nd Edition	n/a								x						
[NIST02]	Specification	Glossary of Key Information Security Terms	NIST IR 7298: Revsion 1		x												
[NIST04]	Specification	NIST Cloud Computing Reference Architecture	NIST SP 500-292	x													
[NIST08]	Specification	Recommended Security Controls for Federal Information Systems and Organizations	NIST SP-800-53		x			x									
[ISO01]	Standards	Information technology – Security techniques – Privacy framework	ISO/IEC 29100:2011		x												
[ISO02]	Standards	Information security incident management	ISO 27035														

Unique ID	Type	Full title	Acronym	B3	C2	C3	C4	C5	C6	C7	C8	D2	D3	D4	D5	D6	D7
[ISO03]	Standards	Information technology -- Open Distributed Processing -- Reference Model: Foundations, 11.2.4, 11.2.5, 11.2.6, 11.2.7	ISO/IEC 10746-2:2009		x												
[ISO07]	Standards	Information Technology – Security techniques – Information Security Management – Measurement. 2009	ISO/IEC 27004:2009 (E)					x									
[ISO08]	Standards	Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models	ISO/IEC 25010:2011		x												
[ISO10]	Standards	Guidelines for identification, collection, acquisition, and preservation of digital evidence	ISO 27037:2012								x						
[ISO11]	Standards	ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements	ISO 27001:2013		x			x									
[ISO12]	Standards	ISO/IEC 27002:2013 -Information technology - Security techniques - Code of practice for information security controls	ISO 27002:2013		x			x									
[ISO13]	Standards	Information security for supplier relationships	ISO 27036-1:2014		x												
[ISO16]	Standards	Information Security Glossary	ISO ISG		x												
[ISO19]	Standards	Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology	ISO/IEC 19086-1, -2, -3		x			x									
[ITU02]	Standards	X.509 : Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks	X.509							x					x		
[OASIS01]	Standards	Extensible Access Control Markup Language	XACML				x						x				

Appendix C. Leveraged standards list

Table 5. Leveraged standards

Unique ID	Acronym	Type	Full title	C2	C4	C5	C6	C8	D3	D4	D5	Comments to SDO	Expected Revision
[AS01]	CEF	Standards	Common Event Format		✔				✔			n/a	n/a
[CSA01]	CTP	Specification	Cloud Trust Protocol	✔			✔					Q2/2014 (data model)	Q3/2014 (API)
[CSA02]	PLA	Specification	Privacy Level Agreements	✔	✔		✔		✔			Q3/2014 (Gap analysis)	n/a
[CSA03]	A6	Specification	CloudAudit				✔					Q4/2014 (Update functionalities)	n/a
[CSA06]	CCM	Specification	Cloud Controls Matrix			✔	✔					Q2/2014 (v3.01 minor)	Q4/2014 (v4)
[CSA07]	CAIQ	Specification	Consensus Assessments Initiative Questionnaire				✔					Q2/2014 (v3.01 minor)	n/a
[CSA08]	OCF	Specification	Open Certification Framework				✔					Q4/2014 (CTP-based)	n/a
[IETF02]	M-ARF	Specification	Messaging abuse reporting format		✔				✔	✔		n/a	n/a
[IETF08]	n/a	Standards	Terminology for Policy-Based Management, RFC 3198, Internet Engineering Task Force (IETF), November 2001.	✔								n/a	n/a
[ISO01]	ISO/IEC 29100:2011	Standards	Information technology – Security techniques – Privacy framework	✔								n/a	n/a
[ISO03]	ISO/IEC 10746-2:2009	Standards	Information technology -- Open Distributed Processing -- Reference Model: Foundations, 11.2.4, 11.2.5, 11.2.6, 11.2.7	✔								n/a	n/a
[ISO04]	ISO/IEC 15414:2006	Standards	Information technology -- Open distributed processing -- Reference model -- Enterprise language, 6.4.1, 6.4.2, 6.5.6	✔								n/a	2014 (extension)
[ISO06]	ISO/IEC 27000:2014	Standards	Information technology - Security techniques - Information security management systems - Overview and vocabulary	✔								n/a	n/a

Unique ID	Acronym	Type	Full title	C2	C4	C5	C6	C8	D3	D4	D5	Comments to SDO	Expected Revision
[ISO07]	ISO/IEC 27004:2009 (E)	Standards	Information security management – Monitoring, measurement, analysis and evaluation	✔								12/09/2014	2016 (3rd WD out for comments)
[ISO10]	ISO 27037:2012	Standards	Guidelines for identification, collection, acquisition, and preservation of digital evidence					✔				n/a	n/a
[ISO16]	ISO ISG	Standards	Information Security Glossary	✔								n/a	2014 (as ISO/IEC 27000:2014)
[ISO18]	ISO/IEC 38500:2008	Standards	ISO/IEC 38500:2008 Corporate governance of information technology.	✔								n/a	2015 (DIS stage)
[ISO19]	ISO/IEC 19086-1, -2, -3	Standards	Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology			✔						01/10/2014	2016-18 (split in 3 parts, -1 as a WD)
[ITU01]	FG-Cloud-TR-1	Standards	Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements	✔								n/a	n/a
[NIST01]	Interagency Report 7316	Standards	Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Assessment of Access Control Systems, NIST Interagency Report 7316, September 2006.	✔								n/a	n/a
[NIST02]	NIST IR 7298: Revsion 1	Specification	Glossary of Key Information Security Terms	✔								n/a	n/a
[NIST04]	NIST SP 500-292	Specification	NIST Cloud Computing Reference Architecture	✔								n/a	n/a
[NIST05]	NIST SP-800-144	Standards	Jansen, W., Grance, T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.	✔								n/a	n/a
[NIST06]	NIST SP 800-145	Standards	Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.	✔								n/a	n/a
[NIST08]	NIST SP-800-53	Specification	Recommended Security Controls for Federal Information Systems and Organizations	✔								n/a	n/a
[NIST17]	NIST DOD85	Specification	Trusted computer system evaluation criteria	✔								n/a	n/a

Unique ID	Acronym	Type	Full title	C2	C4	C5	C6	C8	D3	D4	D5	Comments to SDO	Expected Revision
[NIST18]	SP 800-27 rev A (EP-ITS)	Standards	Stoneburner, G., Hayden, C., Feringa, A., Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev. A, June 2004.	✔								n/a	n/a
[UCL01]	SLANG	Specification	SLA Language Spec		✔				✔			n/a	n/a

Appendix D. Opportunity to contribute

Table 6. Opportunity to contribute

Standardisation Group	Areas of interest	Topics for contribution	Deadline
CSA-ISC	All	Annual revisions to: ▪ Cloud Controls Matrix (CCM) v3.0.1 ▪ Consensus Assessments Initiative Questionnaire (CAIQ) v.3.0.1	-
ITU-T SG13	AoI-1, AoI-3, AoI-4, AoI-6, AoI-7	Contribution to work items: ▪ Y.cloudSECasaservice ▪ Y.cloudtrustmodels ▪ Y.clouduse&req ▪ Y.inter-cloud-sec ▪ Revisions to Y.NGN IdM Use-cases (Technical Report)	-
ITU-T SG17	AoI-1, AoI-2, AoI-3, AoI-4, AoI-6, AoI-7	For Q4/17, contribution to X. work items. For Q8/17, contribution to work items: ▪ X.ccsec ▪ X.fsspvn ▪ X.goscc ▪ X.sfcse	-
ISO/IEC DIS	All	Contribution to ▪ Document ISO/IEC 17788/17789 with respect to information security: preservation of confidentiality, integrity and availability of information [ISO/IEC 27000:2014] ▪ ISO/IEC 19086 Including CSIG SLA	Expired
ISO/IEC-JTC 1/SC 27- WG1 AoI-1, AoI-2, AoI-3, AoI-4, AoI-6, AoI-7		ISO/IEC 3rdWD 27003 – Information Security Management System – Guidance	12/9/2014
		ISO/IEC 3rdWD 27004 – Information security management – Monitoring, measurement, analysis and evaluation	12/9/2014
		"ISO/IEC 2ndCD 27006 – Requirements for bodies providing audit and certification of information security management systems"	6/9/2014
		ISO/IEC CD 27009 – Sector-specific application of ISO/IEC 27001 – Requirements	12/9/2014
		"ISO/IEC CD 27013 – Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1"	28/8/2014
		ISO/IEC 2ndWD 27005 – Information security – Risk management	12/9/2014
		Future Version Development of ISO/IEC 27000	19/8/2014
ISO/IEC-JTC 1/SC 27- WG4 AoI-1, AoI-2, AoI-3, AoI-4, AoI-6, AoI-7		Selection, deployment and operation of intrusion detection and prevention systems (IDPS)	15/9/2014
		Storage security	15/9/2014
		Guidance on assuring suitability and adequacy of incident investigation methods	-
		Guidelines for the analysis and interpretation of digital evidence	-
		Incident investigation principles and processes	15/9/2014
		"Guidelines for security information and event management	15/9/2014
		Application security – Part 5: Protocols and application security control data structure	15/9/2014

Standardisation Group	Areas of interest	Topics for contribution	Deadline
		Application security – Part 5-1: Protocols and application security control data structure – XML Schemas	15/9/2014
		Information security incident management – Part 1: Principles of incident management	15/9/2014
		Information security incident management – Part 2: Guidelines to plan and prepare for incident response	15/9/2014
		Information security incident management – Part 3: Guidelines for incident response operations	15/9/2014
		Information security for supplier relationships – Part 2: Requirements	20/5/2014 - expired
		Information security for supplier relationships – Part 4: Guidelines for security of cloud service	15/9/2014
		CfC on the Cloud Security Assessment and Audit Study Period	15/9/2014
		CfC on the Cloud Adapted Risk Management Framework Study Period	19/8/2014
ISO/IEC-JTC 1/SC 27- WG5 AoI-1, AoI-2, AoI-3, AoI-4, AoI-6, AoI-7		ISO/IEC 4thWD 29134 Privacy impact assessment – Methodology	24/9/2014
		ISO/IEC DIS 29190 Privacy capability assessment model (Revised)	-
ISO/IEC-JTC 1/SC 38 AoI-1, AoI-2, AoI-3, AoI-4, AoI-6, AoI-7		Cloud computing – Overview and vocabulary	-
		Cloud computing – Reference architecture	-
		Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 1: Overview and concepts	-
		Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 2: Metrics	-
		Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 3: Core requirements	-
NCC-SWG	All	▪ Contribution to the work of the Reference Architecture and Taxonomy (RATAX) working group ▪ Contribution to the work for cloud metrics	Expired
ETSI-CSC	All	Leverage the accountability work in the reports of the CSC to support further research in Europe	-

Appendix E. Feedback provided to ISO/IEC DIS 17788 and ISO/IEC DIS 17789

This section has been removed due to confidentiality issues.

Appendix F. Feedback provided to "NIST Cloud Computing Cloud Service Metrics Description"

General comments to draft "NIST Cloud Computing Cloud Service Metrics Description"
Rev 2.3d9 (January 12th, 2014)

The methodology followed in this draft shares commonalities with the one used by both EC funded A4Cloud (cloud accountability metrics) and SPECS (security metrics in Cloud SLA) projects. Actually, as part of the on-going work in A4Cloud, we are developing techniques for eliciting and defining metrics for properties that influence accountability of cloud services. To this end, we defined in a metamodel[12] for metrics for accountability properties, which is intended to be used during the elicitation of metrics for these kinds of properties. We think that the work presented in this draft is very promising, as there is a need for harmonization of concepts and terminology when facing the definition of metrics for cloud services. We have identified synergies that can to enrich our EU/NIST activities in this area.

We very much like and support the metrology intent of the document, and we just add the following high level comments:

- Elaborate upfront the cloud systems model where the metrics are targeted. That would quite help put the metrics in context. In particular, in our own contexts (cloud security and accountability) we have found that organizational/business objectives should be also part of such cloud system model. This was reference also by NIST in report NISTIR 7564 (and more recently in the SLA mind map) and, is also part of CSA's Cloud Control Matrix.
- Clarify the metrics issues w.r.t the Cloud – why are they needed (monitoring, SLA compliance, benchmarking & economic value comparisons), what are the property dimensions that are meaningful for metrics (performance, resiliency, …security???), why is it hard in the Cloud (a common question we have received in several forums), and then the focus on how to conduct metrology – the last being the aspect most covered in the report but the lesser focus on the earlier issues makes it hard to grasp.
- The text around Fig 1/2 needs more careful thought. It raises a number of key issues that are not covered in the text. See Neeraj's notes in attached document.
- The report would benefit by adding some content on how aggregation/composition of quantitative & qualitative metrics (an aspect also raised in NISTIR 7564). These are BIG open questions in the community that will also help to clarify how to reason about sets of elicited metrics. We don't expect answers here though a discussion of the issues would help the value of the document. See Neeraj's comments on page 8 of attached document.
- Emphasize the SMART aspects of metrics (i.e., specific, measurable, attainable, repeatable, and time-dependent), in particular reproducibility of measurements!
- More SLA basis (if this is the document that should take that aspect into account). As the use of SLA's is well established in the Cloud(y) world, a discussion section explicitly related to (a) the use and (b) the limitations of SLA usage w.r.t metrology would be nice.
- What is the actual relationship between security metrics and security controls, like those in CSA's Cloud Control Matrix. We have found that in the (cloud) security community this is becoming a source of confusion.
- Sections 2 and 3 could be actually used to provide more arguments about the use of cloud metrics and measurements. While the current examples are a good starting point, it's necessary to provide more advanced scenarios (e.g., negotiation, accounting).
- Our main concern wrt Section 2 and 3, is that further/detailed analysis seems to be required in order to justify that elicited requirements cover all the possible uses of metrics in the cloud context.
- Maybe in section "Other Considerations", should be discussed issues like trust and privacy assumptions related with the use of metrics, the need of common vocabularies (SLA's?).
- If metrics are "user-centric", then the actual notion of user requirements seems to be missing. What if some metrics are more important than others? This previous fact makes more complex the actual scenario depicted

[12] Nunez, D., Fernandez-Gago, C., Pearson, S., & Felici, M. A Metamodel for Measuring Accountability Attributes in the Cloud. In 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013).

in Fig. 1. Our previous research, considers user-assigned weights associated with metrics or groups of metrics[13].

- The concept of Logical Group (LG) is never clearly defined or introduced.
- Is the contextCondition in Fig. 4 related with the notion of "scenario" shown in Fig. 3? We suggest using also UML for Fig. 3 and then, clarify the relationship with the model in Fig. 4.
- The concept of Primary Measure if not clear. It gives the impression, that a Primary Measure can also aggregate other measurements, therefore this is confusing. Maybe should be related to the metric (i.e., Primary Metric) and not the measure? The notion of Basic Measurable Component has been adopted in our research.
- We would like to comment on the notion of "Observation", related to the measurement process. This concept is not clearly defined and identified. Additionally, not all metrics could be based on observing a system from outside, as in the case of Availability. For example, how can one measure "Transparency" (as understood by the data protection community) of a cloud service provider? Measures of this kind of properties should be based on a different type of evidence.
- From our point of view, any assessment or evaluation (i.e, a metric) can only be made using as input some tangible and empirical evidence, such as an experimental observation (as in the case of the metrics described in the Cloud Service Metrics Description draft), a system log, a certification asserted by a trusted party, a textual description of a procedure, etc. Thus, a metric does not directly measure a property of a process, a service, or a system, but uses the evidence associated with them in order to derive a meaningful measure. That is, evidence is the fundamental support of any evaluation method and is what gives an objective dimension to assessments. We think that the Evidence used by a Metric should be clearly identified and characterized when defining a Metric. The Cloud Service Metrics Description could benefit from the identification of such element, and its inclusion in the Cloud Service Measures and Metrics model.
- In the A4Cloud's metamodel, evidence may come from sources with different levels of certainty and validity, depending on the method of collection or generation. For example, evidence may be publicly verifiable, asserted by a trusted third-party, self-asserted by the cloud service providers, etc. This "quality of evidence" may also affect the results of the metric, and could be explored in the CSMD, perhaps related to the concept of "Measurement uncertainty".
- Finally, we have also identified some grammar issues that are mentioned in the attached document.

[13] Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees
Jesus Luna, Robert Langenberg, Neeraj Suri Proc. of CCSW (ACM Cloud Computing Security Workshop), 2012.

Appendix G. Feedback provided to "CSA Cloud Controls Matrix"

Table 7. Feedback provided on July-2013 for the CSA Cloud Control Matrix 3.0

Control Domain	CCM V.3 Control ID	A4Cloud feedback
Governance and Risk Management	GRM-01	The Information Security Management Program should specifically refer to security awareness trainings to the personnel and provide a connection to the "human resources security" mentioned in GRM-11.
	GRM-02	Should be read "Documented ISMP determine the accountability for the GRC activities"
	GRM-03	The reference to "all impacted personnel and external business relationships" is too general, since they may have different levels of understanding/expertise. What about highlighting the need for policy mapping?
	GRM-05	There is no recommendation on how and why the security strategy should be updated. For instance, monitoring risk levels based on incidents on the provider's own services, but also based on threats to the cloud ecosystem of the provider and the outside world, seem to be relevant criteria. Moreover, this remark is closely related to control DSI-09 (risk assessments) which does not mention many factors that need to be considered in risk assessments e.g. assets, threats, impact, etc.
	GRM-08	Data subject need also to be informed and give consent for third party access to personal data and for the purpose of the processing.
	GRM-09	Also mechanisms allowing data subjects to withdraw access to personal data need to be implemented (for data controllers).
	GRM-10	Access control usually defines roles and access rights but not directly responsibilities and accountability. Accountability needs to be made explicit and documented. Moreover, this control mentions accountability of the user's with respect to the internal organizational policies, not towards external stakeholders: consumers, authorities, partners, etc.
	GRM-11	Might be unrealistic for cloud. The scope need to be constrained to the provider. The provider must then require that partners have performed regular trainings to their personnel/users regularly.
	GRM-13	There should be a connection to LSC-12, in which it is clearer the link to EC recommendation for making this specification explicit in contracts (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf) that all intermediary processors, their location, etc. need to be known by the cloud consumer.
	GRM-14	Even though isolation is covered by control IVS-08, there is an ethical question not addressed here: can a cloud provider support competitors concurrently? This will raise the risk level, including social engineering and corruption risks, if a cloud provider employee maintains data for these competitor customers. Segregation of duty should consider Chinese wall principles to mitigate such risks.
	GRM-15	Shouldn't the users be aware of potential liability measures assigned to their responsibilities?
	GRM-20	A related issue is termination of outsourcing contracts the cloud provider may have, especially those including data storage where costumer data is away. Retrieving the full data, and making sure the outsourcing partners has no more access to the data is fundamental. Same applies in the case of sub-contractor bankrupts.
	GRM-21	Same obligation applies to personal data. The control should be generalized to any kind of confidential data, not only "e-commerce".
	GRM-22	Instead of this control, it would be more meaningful to determine a transparency service should be in place, providing the appropriate and secure monitoring, diagnosing, and accountability tools to cloud costumers. By the way ISV-11 confuses many things with respect to logs, auditability and accountability. This needs to be clarified and more requirements need to be covered concerning logs and accountability.

Control Domain	CCM V.3 Control ID	A4Cloud feedback
	GRM-23	This control is controversial. Does it mean that customers negotiate terms and conditions? Are risks mentioned and how the responsibility to mitigate them distributed among the parties?
	GRM-24	The control mentions “business risks” but these are security risks, in fact. Also, it would be nice to highlight the risks from sharing mobile devices for corporate use – which rules should be applied so that accountability is clearly pointed out for persons (human agents) being assigned roles (i.e. associate accountability metrics with time logs – agent A sharing mobile device x is accountable for performing certain tasks in time period t1-t2)
Legal & Standards Compliance	LSC-01	Measures aiming at the secure storage of data - avoiding data duplication - shall be developed to minimize the risk of business process disruption.
	LSC-02	Organizations shall develop a risk management framework providing for risk assessments to mitigate risk. The risk management framework shall be updated regularly according to the levels of risk presented. Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.
	LSC-03	Does the reference to “information security and confidentiality, service definitions and delivery agreements” include access controls? It is expected that these contracts to provide that (possibly limited to identified) personal data and confidential information should be accessibly only to staff involved directly in providing the service. Risk assessments shall be conducted annually or at regular intervals. The risk assessments will address the likelihood and impact of all identified risks based on qualitative and quantitative methods. The risk assessments shall address separately the possibilities and the impact resulting from inherent and residual risk with respect to all types of risk identified (e.g. audit results, threat and vulnerability analysis).
	LSC-04	This compresses a range of things, and would perhaps be clearer if it were unpacked. It might help to consider the specific example of a bank (cloud customer). Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with the reasonable time response reasonable resolution time frames and executive approval.
	LSC-05	The problem here is that the cost of producing such an inventory increases exponentially with the global reach of the organisation A UK bank, as an example, would probably already do this. A multinational bank might do so comprehensively only for the countries where it has a major presence, and perform much lighter compliance reviews for other countries where it has commercial activity. A global cloud service provider would need to do this for every country in the world, and the cost would be disproportionate to the risks. So this needs to be rethought to find some way of capturing the cost v risk calculation, which organisations actually undertake. Furthermore, audits by external auditors shall be performed on annual basis or at planned intervals to ensure compliance with the obligations provided by law or by contractual arrangements. Audits must be scheduled following a prior agreement between stakeholders
	LSC-06	What kinds of risk? What is “acceptable”? This really says no more than “be careful”, and means nothing in legal terms. There are lots of legal obligations to take reasonable care, and to manage risk, but in each case this means care to avoid particular types of loss, or to manage particular risks. At such a high level, does this add anything useful? Third party service providers shall be subject to audits. Third party service providers shall be requested to keep records and provide reports to demonstrate compliance with the service delivery agreements. Services provided by third parties shall be, also, subject to audits
	LSC-07	See the earlier comment about cost. Most organisations will have a varied set of responses to potential risks – some will be assessed regularly, some infrequently, and some only when the risk actually threatens or materialises (thus no planned schedule). When required to mitigate risks, Third Parties shall have access to the organization’s information systems and data. The cloud service providers will take the necessary measures to minimize the impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.
	LSC-08	The same cost/scope issues arise. As an example, any global cloud service provider is at risk of breaching the law or regulation of Mongolia, if they provide services to Mongolian customers. Most will not even have bothered to identify these risks, unless they have a

Control Domain	CCM V.3 Control ID	A4Cloud feedback
		significant number of Mongolian customers, let alone plan how to mitigate them. There are around 200 countries in the world, but most global organisations only worry about 20 or so because otherwise the problem is too big to be manageable and the cost disproportionate. Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented and reviewed at planned intervals. However, reviewing confidentiality obligations included, for instance, in contractual clauses may lead to amending contracts at "planned intervals." This is not very efficient in many ways, while it leads to legal uncertainty.
	LSC-9	Contractual agreements between providers of cloud services and customers (tenants) shall include at least clauses relating to: a. The scope of the established relationship b. The characteristics of the offered services (e.g. feature sets and functionalities, personnel and infrastructure network, systems components for service delivery and support) c. The responsibilities of service providers and cloud customers d. The requirements for subcontracting e. The location of the hosting services f. The information security requirements g. The contact details of the parties h. The duration of the contract i. The security measures j. The information to be provided to the cloud customer regarding any changes to the delivery of the cloud service putting at stake his interests k. The deadline for notification of security incidents to customers and other parties with legitimate interests at stake l. Audits by external auditors under certain requirements.
	LSC-10	Policies shall aim to meet customer's requirements for service-to-service application (API), interoperability and portability regarding application development and information exchange, usage and integrity persistence. The policies and the procedures shall be established in relation to the agreements) between cloud providers and cloud customers. The policies will address incidents of non-compliance across the entire chain of service providers.
	LSC-11	Contact information shall be regularly updated to allow competent authorities to address requests.
	LSC-12	The organization shall keep an inventory providing for the location of personal data. The information relating to the organizationally-owned or managed (physical or virtual) infrastructure network and systems components shall be updated regularly. Independent verification of contract compliance (in general) is not common, though it is common to negotiate independent verification for specified (and very limited) obligations. I'm not sure whether a general independent verification service even exists, and if it does it will be extremely expensive! More importantly, there are probably a number of significant omissions from this list, but identifying them will take substantial research. In legal usage these are NOT SLAs! A less confusing term needs to be found (why not Supply Chain Agreements (SCAs)? (Also applies to LSC- 13).
Supply Chain Management, Transperancy and Accountability	STA-01	As a general comment the STA Domain Controls seem to be too generic, hence, they may result ineffective. It would be useful to further specify them. A more specific comment, it seems that they do not capture general governance and privacy principles as defined cloud-related guidelines and standards. These STA Domain Controls seem to have a narrow interpretation of Transparency and Accountability; Transparency is not all information is available; Accountability is not everyone is responsible for everyone else. It would be useful to review such STA Domains Controls by taking into account privacy, transparency and accountability principles and/or elements that support governance of cloud supply chains.

Control Domain	CCM V.3 Control ID	A4Cloud feedback
		For instance, little emphasis is on different aspects transparency and accountability, e.g.: purpose specification and limitation, remediation in case of issues and so on. More specifically, these Domain Controls should capture privacy, transparency and accountability principles as described in relevant guidelines and regulations, e.g., OECD privacy guidelines, Article 29 working party's principle of accountability.
	STA-02	The use of the terms measures/metrics is a bit confusing in this case. Moreover, the generic domain control would require some explanations of what measures/metrics to provide as evidence of “conformance and effectiveness of policies and procedures."
	STA-03	This could be insufficient. Incident information should be timely too. Without prompt information about incidents any counter-measure could be ineffective or too late for customers.
	STA-04	Talking about "risks inherited from other members of that partners cloud supply chain" would just trigger a domino effect of risk. Providers would need to have specific mitigation measures to minimise the effect of risks propagating across the supply chain. Organizational practices may differ without clearly states what are accepted practices supporting transparency and accountability principles. It would be then difficult to assess any consistency and alignment.
	STA-05	It would be necessary not only to "design and implement controls" but also to identify and assess remediation mechanisms in case of data security breaches. We believe that STA-05 should make it clear that refers to sensitive (and probably personal) data. We agree with the comment that “must” is strong to be used for any kind of data quality.
Business Continuity Management & Operational Resilience	BCR-07	A critical requirement for BCP can be the flexibility in accountability tolerance in case of disruptions. During the recovery period, the organization shall be able to gradually return to full operation in order to support the established policies, but this means that the prioritization of responsibilities and operations shall be subject to the accountability obligations deriving from the on-going contracts with customers.
Security Incident Management, E-Discovery & Cloud Forensics	SEF-05	Who is responsible to certify that mechanisms put in place are appropriate for incident handling? (Certification of evidence)?
Datacenter Security	DCS-01	It shall be connected to BCP (probably BCR-07), but responsible for accountability should be appointed.

Appendix H. Analyzing identified standards.

The following table shows the results of the analysis performed by A-5 based on the criteria presented in Section 6.

Table 8. Analysis of identified standards

Acronym	Type	Full title	RELEVANCE	IMPACT	OPPORTUNITY
CEF	Standards	Common Event Format	M	L	L
CTP	Specification	Cloud Trust Protocol	M	H	H
PLA	Specification	Privacy Level Agreements	H	H	H
A6	Specification	CloudAudit	M	M	L
CCM	Specification	Cloud Controls Matrix	H	H	H
CAIQ	Specification	Consensus Assessments Initiative Questionnaire	H	H	H
OCF	Specification	Open Certification Framework	H	H	H
M-ARF	Specification	Messaging abuse reporting format	M	L	L
n/a	Standards	Terminology for Policy-Based Management, RFC 3198, Internet Engineering Task Force (IETF), November 2001.	L	L	L
ISO/IEC 27000:2014	Standards	Information technology - Security techniques - Information security management systems - Overview and vocabulary	H	M	L
ISO/IEC 3rdWD 27003	Standards	ISO/IEC 3rdWD 27003 – Information Security Management System – Guidance	H	M	H
ISO/IEC 3rdWD 27004	Standards	ISO/IEC 3rdWD 27004 – Information security management – Monitoring, measurement, analysis and evaluation	H	H	H
ISO/IEC 2ndWD 27005	Standards	ISO/IEC 2ndWD 27005 – Information security – Risk management	H	M	H
ISO/IEC 2ndCD 27006	Standards	"ISO/IEC 2ndCD 27006 – Requirements for bodies providing audit and certification of information security management systems"	H	M	H
ISO/IEC CD 27009	Standards	ISO/IEC CD 27009 – Sector-specific application of ISO/IEC 27001 – Requirements	L	M	H
ISO/IEC CD 27013	Standards	"ISO/IEC CD 27013 – Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1"	L	M	H
ISO/IEC CD 27017	Standards	ISO/IEC CD 27017 – Code of practice for information security controls	L	M	H
Future Version Development of ISO/IEC 27000	Standards	Future Version Development of ISO/IEC 27000	M	M	H

Acronym	Type	Full title	RELEVANCE	IMPACT	OPPORTUNITY
ISO/IEC 17788 - Cloud computing – Overview and vocabulary	Standards	Cloud computing – Overview and vocabulary	H	H	L
ISO/IEC 17789; Cloud computing – Reference architecture	Standards	Cloud computing – Reference architecture	H	M	L
ISO/IEC WD 19086 Part 1	Standards	Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 1: Overview and concepts	H	H	H
ISO/IEC WD 19086 Part 2	Standards	Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 2: Metrics	H	H	H
ISO/IEC WD 19086 Part 3	Standards	Cloud computing – Service Level Agreement (SLA) Framework and Terminology – Part 3: Core requirements	H	H	H
Selection, deployment and operation of intrusion detection and prevention systems (IDPS)	Standards	Selection, deployment and operation of intrusion detection and prevention systems (IDPS)	L	M	H
Storage security	Standards	Storage security	M	M	H
Guidance on assuring suitability and adequacy of incident investigation methods	Standards	Guidance on assuring suitability and adequacy of incident investigation methods	M	L	L
ISO/IEC DIS 27042	Standards	ISO/IEC DIS 27042: Guidelines for the analysis and interpretation of digital evidence	H	H	L
ISO/IEC FDIS 27043	Standards	ISO/IEC FDIS 27043: Incident investigation principles and processes	H	H	L
ISO/IEC WD 27044	Standards	ISO/IEC WD 27044: Guidelines for security information and event management (SIEM)	H	M	H
Application security – Part 5: Protocols and application security control data structure	Standards	Application security – Part 5: Protocols and application security control data structure	M	M	H
Application security – Part 5-1: Protocols and application security control data structure – XML Schemas	Standards	Application security – Part 5-1: Protocols and application security control data structure – XML Schemas	M	M	H
ISO/IEC CD 27035-1:	Standards	ISO/IEC CD 27035-1:Information security incident management – Part 1: Principles of incident management	H	M	H
ISO/IEC CD 27035-2	Standards	ISO/IEC CD 27035-2: Information security incident management – Part 2: Guidelines to plan and prepare for incident response	H	L	H
ISO/IEC CD 27035-3	Standards	ISO/IEC CD 27035-3: Information security incident management – Part 3: Guidelines for incident response operations	H	L	H

Acronym	Type	Full title	RELEVANCE	IMPACT	OPPORTUNITY
ISO/IEC 27036-	Standards	ISO/IEC 27036-2: Information security for supplier relationships – Part 2: Requirements	H	H	L
ISO/IEC 27036-4	Standards	ISO/IEC 27036-4 -- Information security for supplier relationships – Part 4: Guidelines for security of cloud service	H	M	H
ISO/IEC 27037:2012	Standards	Guidelines for identification, collection, acquisition, and preservation of digital evidence	L	H	M
CfC on the Cloud Security Assessment and Audit Study Period	Standards	CfC on the Cloud Security Assessment and Audit Study Period	M	M	H
CfC on the Cloud Adapted Risk Management Framework Study Period	Standards	CfC on the Cloud Adapted Risk Management Framework Study Period	M	L	M
ISO/IEC 4thWD 29134	Standards	ISO/IEC 4thWD 29134 Privacy impact assessment – Methodology	H	M	H
ISO/IEC DIS 29190	Standards	ISO/IEC DIS 29190 Privacy capability assessment model (Revised)	H	L	L
ISO/IEC 29100:2011	Standards	Information technology – Security techniques – Privacy framework	H	L	M
ISO/IEC 10746-2:2009	Standards	ISO/IEC JTC 1/SC 7 - Information technology -- Open Distributed Processing -- Reference Model: Foundations, 11.2.4, 11.2.5, 11.2.6, 11.2.7	M	L	M
ISO/IEC 15414:2006	Standards	ISO/IEC JTC 1/SC 7 - Information technology -- Open distributed processing -- Reference model -- Enterprise language, 6.4.1, 6.4.2, 6.5.6	M	L	M
ISO ISG	Standards	Information Security Glossary	H	M	L
ISO/IEC 38500:2008	Standards	ISO/IEC 38500:2008 Corporate governance of information technology.	M	M	L
FG-Cloud-TR-1	Standards	Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements	M	M	M
Interagency Report 7316	Specification	Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Assessment of Access Control Systems, NIST Interagency Report 7316, September 2006.	L	L	L
NIST IR 7298: Revsion 1	Specification	Glossary of Key Information Security Terms	M	M	L
NIST SP 500-292	Specification	NIST Cloud Computing Reference Architecture	H	H	L

Acronym	Type	Full title	RELEVANCE	IMPACT	OPPORTUNITY
NIST SP-800-144	Standards	Jansen, W., Grance, T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.	H	H	L
NIST SP 800-145	Standards	Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.	H	H	L
NIST SP-800-53	Specification	Recommended Security Controls for Federal Information Systems and Organizations	H	H	L
NIST DOD85	Specification	Trusted computer system evaluation criteria	M	L	L
SP 800-27 rev A (EP-ITS)	Standards	Stoneburner, G., Hayden, C., Feringa, A., Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev. A, June 2004.	M	L	L
SLANG	Specification	SLA Language Spec	M	M	L