Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
OFE	All	All	Ge	There are two central parts to this document. One part goes through a series of scenarios/use cases. These are of such a high level that they do nothing to identify anything more specific than secure, interoperable and portable solutions are needed for successful cloud adoption! These scenrios need to be more narrowly focused so as to tease out more concrete issue and gaps that need to be worked on. A focus on key enabling scenarios would help focus the dialogue The second part goes through “core concepts”, and all it does is provide very high level definitions of interoperability, portability, security and SLAs. This it does in less detail than can be found in ISO/IEC 17788 and 17789 and therefore does not add to the subject. This document needs a major refocus and re-write in order for it to offer a vehicle for future work and study. It is hard to suggest what this should be since it is not clear what the goal of this document is. Specifically the paragraph starting on line 1243 talks about outstanding gaps, yet the report itself has done very little to identify where the gaps are.	Decide the purpose of this document (e.g. enumerating gaps and issues) and refocus accordingly.
OFE		All	Ge	There is much reference made to CSLA's and ISO 19086/27001. ISO 19086 has a focus on security and is only in draft stage at the moment. The title of WP3 includes the phrase 'interoperability' which extends significantly beyond the scope of 19086.	Therefore further work is needed to expand the remit of standards under the heading of CSLA to cover interoperability.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
H2020 CLARUS project	Several sections	Several pages	Editorial	"must most likely have to be supported"	"must most likely be supported"
OFE		72	Ge	It is not clear what "accessibility" means in this context. Is it related to availability, or disability? Accessibility related to disabled people is of a crucial concern, though it is not address further in this document.	If accessibility in the disabled sense, add a footnote to say that while important it is not covered in this document. If it is not related to disabled people, change to availability.
MS 1	Introduction	72	Ed	I assume this refers to the ability to access data, not to the general subject of accessibility.	Change "accessibility" to "data accessibility" (as used elsewhere in the document).
SICS Swedish ICT/PaaSword	1		General	Although the report according to the scope section aims to handle interoperability and security in cloud computing, it provides just a list (very nice and important though) use cases and discusses general security problems. But, the report does not really address what one would expect considering the scope statement, i.e. specific security interoperability issues for cloud environments and in depth analysis of the current status?	In next version, it would be nice if each of the defined different use cases could be analysed with respect to the current situation regarding security standards support and identification of potential gaps.
OFE		98-99	Ge	It is not clear how a global approach to interoperability increases levels of trust in cloud computing.	Clarify what is meant by trust here, esp wrt interoperability
Cloud Security Alliance	1	99	Technical	The following text: "…increase the level of trust in Cloud Computing" does not consider that also the level of transparency can increase thanks to both interoperability and security assurance.	Please change the following text: "…increase the level of trust in Cloud Computing" to: "…increase the level of trust and transparency in Cloud Computing"
MS 2	3.1	140	Te	Contradicts line 138.	Review and correct definitions (see comments on WI2).
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	3.2	148 all	General	SLA IS MORE POPULAR TERM THAN CSLA	CSLA => Cloud SLA

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	3.2	151, 152 all	General	CONFUSING ABOUT SAME ABBREVIATIONS FOR CLOUD SERVICE CUSTOMER AND CLOUD STANDARD COORDINATION	PLEASE DO NOT USE CSC TO ABBREVIATE CLOUD STANDARDS COORDINATION OR CLOUD SERVICE CUSTOMER
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	3.2	188, 189 all	General	CONFUSING ABOUT SAME ABBREVIATIONS FOR SINGLE SIGN-ON AND STANDARDS SETTING ORGANIZATION	PLEASE DO NOT USE SSO TO ABBREVIATE STANDARD SETTING ORGANIZATION OR SINGLE SIGN-ON
TECNALIA	5	269	Technical	in all design phases	in all engineering phases
TECNALIA	5	270	Technical	required capabilities and their implementation and deployment	required capabilities and their design, implementation and deployment
CAS Software AG/PaaSword	5		General	The use scenarios deal with the data protection and the application of a suitable encryption algorithm is recommended. The document miss the discussion about which encryption algorithms are currently recommended and included in different standards.	Please expand the data protection section corresponding to the use scenario with respect to recommended encryption mechanism. Also, attackers gain information about encrypted data by intelligent queries and searches. This scenario could also be part of the data protection sections.
SixSq/PaaSword	5		General	Perhaps intentionally the document relies heavily on certification of CSPs and neglects techniques that could be employed by the developers of cloud applications (either with a CSC's organization or outside of it) to secure data even in the face of poor or negligent information handling by the CSPs. Certifications will reduce the financial exposure of CSCs using cloud service, but will not protect them from harm to their reputations in light of a data breach.	Provide technical recommendations that CSC can use within their applications to reduce their risks of data exposure irrespective of the security performance of a particular CSP.
CAS Software AG/PaaSword	5.2		General	The document defines requirements and capabilities for every use scenario. Data protection is one part of the requirements, but only the actual used data set is considered in the current version of the paper. Data protection	The authors could also include backup data into the data protection requirements in every use scenario.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				includes also the protection of backups.	
CAS Software AG/PaaSword	5.2		General	In the current version of the document the authors only consider data security with respect to external adversaries, internal adversaries are not included at the moment.	Consider also including possible internal adversaries in the analysis of the use scenarios with respect to data security and access control.
CAS Software AG/PaaSword	5.2		General	Data classification is mentioned as a necessary precondition for data protection. The document is missing a specific recommendation which taxonomy should be used for data classification.	Please add a recommended taxonomy or standard for data classification.
ICCS/PaaSword	5.2	281,443,535,737	General	In the discussion about the scenarios 1, 3, 4, 6 it would be valuable to consider more advanced and detailed requirements that are related to access control and security policy management.	Please consider mentioning contextual elements (e.g. IP, time, patterns of access etc.) that may be taken into account for applying advanced security policy management.
TECNALIA	5.2.1	292	Editorial	an designated	a designated
TECNALIA	5.2.1	298	Editorial	in order meet	in order to meet
H2020 CLARUS project	5.2.1	298	Editorial	“In order meet”	“In order to meet”
Kyung Hee University	5.2.1	298	Editorial	wrong typing “in order meet”	in order to meet
TECNALIA	5.2.1	300	Editorial	It’s	It is
MS 3	5.2.1	305	Ed	Typo	Change "CSP" to "CSC"
Kyung Hee University	5.2.1	305	Editorial	wrong typing “on the CSP’s request”	on the CSC’s request
TECNALIA	5.2.1	309	Technical	The contract between	The CSLA (and / or contract4) - Include footnote 4 in this line.
TECNALIA	5.2.1	311	Technical	possible removal of audit trail (log) data	Explain in the Conclusions why it is only “possible” – are you referring to those cases of Law Enforcement when it is not possible?
H2020 CLARUS project	5.2.1	311	Technical	Specifying the security policies the CSC wants to apply to data is something relevant.	Add “… the level of security the CSC requires for the data”

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
TECNALIA	5.2.1	312	Editorial	It should	it should
TECNALIA	5.2.1	318	Technical	without any significant extra work.	without any significant extra work for CSC.
TECNALIA	5.2.1	319	Technical	data classification & taxonomy principles	There is a mixture of data classification, data categorization and taxonomy words employed in the Scenario 1 and 2 (line 417). Please clarify the differences or keep always the same concepts.
TECNALIA	5.2.1	320	Editorial	what data ("type of data") that belongs	what data ("type of data") belongs
TECNALIA	5.2.1	321	Technical	(according to criticality)	(e.g. according to criticality)
Consortium of Cloud Computing Research	5.2.1	329	Technical	It is too general description of data protection, even though the scenario and use case describe moving data from and between CSPs.	It is better to explain importance of data protection and responsibilities in the point of view of data movement, e.g., how to protect exchanging data between CSPs.
TECNALIA	5.2.1	330	Technical	is well protected is yet another	is well protected by the Cloud Service is yet another
H2020 CLARUS project	5.2.1	334	Technical	Key Management is important for data protection when encrypting data	Add "… and the implementation of key management scheme"
H2020 CLARUS project	5.2.1	334	Technical	Data encryption is not sufficient if the securisation workflow is not properly enforced.	Add "At any moment in the data securisation workflow, the CSP must not apply some unprotection mechanism that may lead to disclosure or leakage of sensitive or confidential data to unauthorised third parties during data migration."
H2020 CLARUS project	5.2.1	334	Technical	The CSC should be able to monitor the security and privacy enhanced mechanisms used for data protection	Add " The CSP should offer security and privacy enhanced mechanisms for data protection whose usage the CSC can monitor"
TECNALIA	5.2.1	335	Editorial	it's	it is
Korea Association of Cloud Industry(KACI) Cloud Computing	4 1, 3 5	338 annotation , 496	Editorial	DO NOT ENCLOSE A STANDARD NUMBER IN BRACKETS	ISO/IEC (17789) => ISO/IEC 17789 ITU-T (Y.3502) => ITU-T Y.3502

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Standard Forum(CCF)		annoation			
TECNALIA	5.2.1	343	Technical	standard.	Add a new sentence following: ….standard. These aspects need to be regulated by the CSLA or contract.
TECNALIA	5.2.1	347	Editorial	CC’s users	CSC’s users
TECNALIA	5.2.1	351-362	Editorial		I suggest that Certification is the last requirement mentioned in all scenarios. At least in Scenario 1 it makes more sense to place the Access control req just after Authentication and identity management.
OFE		352-353	Ed	Not sure why certification per see is important in this scenario. Rephrasing might help in this regard.	Change to: “Certification allows CSPs to provide commitments on aspects such as security, and privacy, portability and interoperability enabling a CSP to pick a suitable CSP.”
OFE		355	Te	Access control is part of Identity management (identity, authentication, authorization). However throughout this report they are treated inconsistently – sometimes the same sometimes different topics.	Place this text under bullet five on line 345, and make sure throughout the document that identity/access/authentication and authorization are not described separately from one another
H2020 CLARUS project	5.2.1	355	Technical	Confusion between the Access control layer and access control multilayer	Change Access control to Access control management, or put 4 5 7 together (as belong to the access control multilayer)
TECNALIA	5.2.1	356	Technical	access of Cloud services.	access of users to Cloud services.
TECNALIA	5.2.1	361	Technical	capabilities of the multi-layer	capabilities of the Access Control multi-layer
TECNALIA	5.2.1	362	Editorial	point 3 and 4).	point 4 and 5).
TECNALIA	5.2.1	365	Technical	more attention and work	more attention and most likely more work
TECNALIA	5.2.1	371	Technical	Conformance	The core concept Conformance is listed in Scenario 1 but is explained in Scenario 5 and not mentioned in the text of Scenario 1, what is a bit

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
					confusing.
Kyung Hee University	5.2.1 5.2.3	371 517	Technical	The “conformance” in the each core concepts needs explanation in section 6.	Give an explanation of conformance in section 6.
OFE		378	Te	This scenario doesn't demonstrate many facets of interoperability as this is primarily a data portability scenario.	Change “interoperability” to “data portability”
TECNALIA	5.2.2	396	Editorial	the service a reason that	the service for a reason that
TECNALIA	5.2.2	416	Technical	without any significant extra work.	without any significant extra work for CSC.
TECNALIA	5.2.2	417	Technical	data classification	It appears twice in the sentence. Linked to my comment on text line 319.
TECNALIA	5.2.2	417	Technical	data integrity,	data protection, (it is more general)
TECNALIA	5.2.2	430	Editorial	a emergency	an emergency
TECNALIA	5.2.2	433	Technical		Add Contingency Plan to the list of core concepts for this scenario and in 6.1?
OFE		439-441	Te	What is in a CSLA is meaningless unless it enforced. Who will enforce the CSLA for a bankrupt or otherwise closed down CSP? This aspect needs to be explored more.	Enforcement of a CSLA esp, after a CSP has gone out of business - especially overnight and without warning- should be highlighted as an issue.
TECNALIA	5.2.3	447	Technical	identity access solutions	identity management solutions (in fact, Single Sign On is an authentication solution)
OFE		452	ed	Would the type of cloud (private or public) change the scenario/use case, or is this a public cloud scenario?	
TECNALIA	5.2.3	454	Technical	identity access solutions	identity management solutions or authentication solutions

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
OFE		462	Te	Isolation and multi-tenancy is a fundamental principle of public cloud computing	Change: "the CSP must provide a secure and trustworthy environment," to: "the CSP must provide a secure and trustworthy multi-tenant environment,"
TECNALIA	5.2.3	466	Technical	during processing	during processing (i.e. while authenticating the users)
OFE		477-483	Te	Since no interoperable language exists why is it being discussed here in the middle of a scenario/set of requirements?	Suggest moving the text about standardized metrics to a more appropriate place that discusses general gaps and issues.
TECNALIA	5.2.3	481	Editorial	project SPECS project	project SPECS
TECNALIA	5.2.3	486	Technical	capability required	capability of Cloud Service required
TECNALIA	5.2.3	492	Technical	identity access solutions	identity management solutions or identity authentication solutions
TECNALIA	5.2.3	493	Technical	Management of keys	Secure management of encryption keys
TECNALIA	5.2.3	494	Technical	Certification and CSLAs are needed	remove or reword sentence, because it is already said in pints 1 and 4. Suggestion of sentence: These data protection requirements need to be included in the CSLA and appropriately audited and /or accredited in Certifications.
TECNALIA	5.2.3	499	Technical	enforcement of the CSP's management and more.	Why is this different from sentence in line 341?
OFE		507	Te	access control is not distinct from on line 496	combine access control with authorization and security policy on line 496
H2020 CLARUS project	5.2.3	507	Technical	Confusion between Access control and Identity management	In section 5.2.1, the requirement Access control does not include identity management, but here it does.
TECNALIA	5.2.3	512	Technical	identity access solutions	identity management solutions or authentication solutions

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
TECNALIA	5.2.3	514	Editorial	certification..	certification.
TECNALIA	5.2.3	517	Technical		Include Trustworthiness of CSP in the list of core concepts.
H2020 CLARUS project	5.2.3	517	Technical	Add "Privacy" to "Data Integrity, Data Protection, Conformance, Interoperability (at several levels), Portability, Certification, CSLA."	Add "Privacy"
TECNALIA	5.2.3	531	Editorial	certification for	Certification for
SixSq/PaaSword	5	535	General	The vulnerability of a dataset depends significantly on how the dataset is stored and exposed. Data in files may be easier to protect than datasets made available via a database or application API. This is an important aspect of the data categorization considerations and should be mentioned. (E.g. in Sec. 5.2.4, high-level requirement 2.)	Add data exposure "footprint" as a consideration for data handling.
TECNALIA	5.2.4	569	Technical	interoperability	exchange
TECNALIA	5.2.4	569	Technical	Public Cloud Service and own operated Private Cloud as well as the own	Public Cloud Service(s) and own operated Private Cloud and /or the own
Cloud Security Alliance	5.2.4	572-578	Editorial	The entire paragraph is not clear. Please clarify and rephrase.	The entire paragraph is not clear. Please clarify and rephrase.
TECNALIA	5.2.4	576	Technical	quality of data	quality (e.g. sensitivity) of data
TECNALIA	5.2.4	583	Technical	on top.	taken into account.
TECNALIA	5.2.4	584-585	Technical	between other Private or Public Cloud.	between the Private and Public Cloud(s).
TECNALIA	5.2.4	597	Technical	become mandatory	becomes mandatory
OFE		601-604	Te	The text here is a describes solutions not	Rephrase in a way that describes Authentication

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				requirements	and identity requirements for this scenario, and don't recommend solutions.
TECNALIA	5.2.4	606-608	Technical	The two sentences are not clear and have typos.	Clarify the two sentences and the recommendation given by them.
Cloud Security Alliance	6	615 Note: either clause or line number incorrect	Technical	You refer to Cloud Customer as owner of the data. What do you mean? The owner of the personal data is normally the "data subject" which is normally the end-user of a cloud customer.	Please correct the reference to the data owner.
Cloud Security Alliance	5.2.4	623	Technical	The statement: "The well-.-known IT certifications such as ISO 27001, SSAE16 are not that helpful, as they do not cover the cloud specific requirements in all aspects.." is not correct and it contradicts with the result of your survey.	Please amend the statement taking into account the results of the your survey
OFE		624	Te	The statement here, that ISO 27001 is not very useful, contradicts lines 631-632 since ISO 27001 is a recommended cloud certification scheme according to the CCSL.	Rephrase so as to avoid this apparent contradiction.
Cloud Security Alliance	5.2.5	ALL	Technical	The scenario 5 doesn't mention at all the concept of "containers".	Please update the scenario including the concept of containers
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	6	624	Editorial	EXACT STANDARD CODING RECOMMENDED	ISO 27001 => ISO/IEC 27001
TECNALIA	5.2.4	627-629	Technical	data centers are not mentioned before in the Certifications.	The sentence is valid for all Certification req in all Scenarios. Nevertheless, the wording can be improved.
TECNALIA	5.2.4	635	Technical	Trust	Trustworthiness of CSP (better talk of trustworthiness as it is a

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
					characteristic of the CSP)
OFE		647-651	Te	This conclusion/remark demonstrates that this scenario is too high a level and far too generic to be able to derive actionable requirements that can be used to identify gaps.	Narroe the scenario to look at key enablers
TECNALIA	5.2.4	647	Technical	documented so far, are the impacts to the CSP's organization, where	documented so far is the impacts to the organisation providing the combined service, where
TECNALIA	5.2.4	649	Technical	need to	needs to
H2020 CLARUS project	5.2.5		Technical	When discussing PaaS Clouds Services, the cloud may inadvertently run malware on behalf of the user. The legal responsibilities for any harm caused by user malware running on PaaS ought to be clarified in the service agreements	Please discuss this in scenario description and high-level requirements.
TECNALIA	5.2.5	667	Editorial	leading potentially	potentially leading
TECNALIA	5.2.5	671	Editorial	applications	application
TECNALIA	5.2.5	672	Editorial	to port to other	to port it to other
TECNALIA	5.2.5	674	Technical	application environment	application execution environment Is this what you mean?
TECNALIA	5.2.5	687	Technical	used runtimes	used runtime execution environments
TECNALIA	5.2.5	691	Technical	"origin CSP" and the "target CSP"	"origin PaaS CSP" and the "target PaaS CSP"
TECNALIA	5.2.5	693	Technical	"data portability"	Data portability
TECNALIA	5.2.5	694	Technical	"data".	data managed by the application.
TECNALIA	5.2.5	697-698	Editorial	Very complex sentence with support twice	Rewrite the sentence

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
TECNALIA	5.2.5	702	Editorial	then the tools	the tools
TECNALIA	5.2.5	703	Editorial	needs	need
TECNALIA	5.2.5	704	Editorial	CSP" when migrating between CSPs.	CSP".
TECNALIA	5.2.5	706	Editorial	CSC	CSC's
OFE		709-711	Te	Some Clarification as to what type of certification and how it helps in app portability would be helpful.	Add examples of certification of app portability.
TECNALIA	5.2.5	720	Editorial	when a moving	when moving
TECNALIA	5.2.5	729	Editorial	process [space]	process.
TECNALIA	5.2.5	730	Technical	This partial influence cannot be accepted in this scenario.	Add such explanations at the end.
TECNALIA	5.2.5	732	Editorial	eg technical	e.g. technical
TECNALIA	5.2.6	744	Technical	Development.	Development environments.
TECNALIA	5.2.6	758	Technical	safely processed	securely processed ??
TECNALIA	5.2.6	764	Technical	metrics.	metrics in those aspects.
TECNALIA	5.2.6	767	Technical	need to	need for the CSP to
TECNALIA	5.2.6	769	Technical	may require additional R&D efforts	What do you mean with this?
TECNALIA	5.2.6	772	Technical	capability to ensure	capability that needs to be regulated in order to ensure
TECNALIA	5.2.6	773	Technical	the technical support	the CSP's technical support

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
TECNALIA	5.2.6	780	Editorial	support of	support
TECNALIA	5.2.6	790	Editorial	high-level of trust	high level trust
TECNALIA	5.2.6	790	Technical	in the CSP, the	in the CSP, the CSP's measures for
TECNALIA	5.2.6	796	Technical	support of	schema supporting
OFE		798-854	Te	This is not really a scenario, more of an analysis against the new GDPR. The content is relevant to this document, but suggest it is moved out of the scenarios section and into an analysis section.	Repurpose this text from a scenario to an analysis.
H2020 CLARUS project	5.2.7	804, 807, 811, 816, 838	General	New EU Data Protection Directive	Should be changed to "New EU Data Protection Regulation"
MS4	5.2.7	804	Te	The new EU data protection instrument is a Regulation, not a Directive	Change "between … directive" to "between the existing Data Protection Directive and the proposed Data Protection Regulation,"
H2020 CLARUS project	5.2.7	805, 813, 820, 842, 852	General	Use of Personal Identifiable Information (PII)	Strange to only refer to PII (more US term) when talking about the new General Data Protection Regulation. Nuance between PII and Personal Data should be (somewhere) highlighted. Personal Data is more broad.
MS5	5.2.7	807	Te	The new EU data protection instrument is a Regulation, not a Directive	Change "directive" to "Regulation"
H2020 CLARUS project	5.2.7	810	Technical	Accountability and audit of the CSP	Add another item "The CSP should adopt internal policies and mechanisms that ensure compliance with the data protection rules. The controller must also be able to demonstrate this compliance with evidence."
H2020 CLARUS project	5.2.7	810	Technical	Security and Notification	Add another item "The CSP should implement appropriate technical and organisational measures to protect data processing activities."

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
H2020 CLARUS project	5.2.7	810	Technical	Transparency of processing data	Add another item " The CSP should implement easily accessible and transparent policies for data processing"
Cloud Security Alliance	5.2.7	810	Editorial	The "High-Level Requirements" in this scenario are not presented as in previous scenarios i.e., organized by core concepts.	Please present these requirements organized in core concepts.
Cloud Security Alliance	5.2.7	811	Technical	The reference to the "new data protection directive" is misleading. What are you referring to? The new PROPOSED draft of the General Data Protection Regulation (GDPR)? If that correct and you are referring to the GDPR then please note that is not finalised yet and you cannot refer to imaginary requirements.	There's no proposed change. Please clarify and fix the mistake.
TECNALIA	5.2.7	820	Technical	European Economic Area	Add a footnote on which countries are included in this definition.
MS 6	5.2.7	824	Te	No certification based on standards can ever be definitive that a CSP is in compliance with its legal obligations.	Replace "as being compliant" with ", to provide evidence supporting their compliance"
H2020 CLARUS project	5.2.7	824	General	Data transfer outside the EEA	Add "Any transfer of data outside the EEA must respect the specific provisions related to data transfer"
MS 7	5.2.7	825	Ed	Typo	Change "PID" to "PII"
TECNALIA	5.2.7	825	Technical	PID	PII
MS 8	5.2.7	826	Te	There can never be a situation "without … risk of legal breaches"	Replace "without the risk" with "with minimized risk"
TECNALIA	5.2.7	828	Editorial	subcontractors are also	subcontractors also
TECNALIA	5.2.7	832	Technical		Add Conformance to the list of core concepts. And can PII be added?
Cloud Security Alliance	5.2.7	837-853	Technical	The conclusion and remarks of this scenario do not provide any guidance on standard. It just	We suggest to focus on existing national laws and directive and provide guidance about those

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				highlights a eventual risk that might surface IF/WHEN the new GDPR will enter into force. Since the scenario is about the rather well know issue of privacy compliance in the cloud.	e.g. by referring to what exist both in terms of rules and in term of solutions (EC C-SIG Code of Conduct, CSA Privacy Level Agreement v2.)
MS 9	5.2.7	839	Te	It is not likely that transparency requirements will demand all aspects of sub-structure to be revealed.	Change the second "of" to "about the legally-significant elements of"
OFE		845- 848	Te	This report should not contain editorial opinions like this. Not the time nor the place for this.	Delete
Cloud Security Alliance	5.2.7	845	Editorial	The text “Some of the major players in Cloud Computing (…) have already warned that the new EU Data Protection regulation will “kill Cloud Computing” within Europe.” is unreferenced, vague (i.e. “some major players”) and unverifiable claims. The EU position that follows in the next sentence would also benefit from a reference.	Provide a citation/reference.
TECNALIA	5.2.7	851	Technical	necessary security	necessary confidence
H2020 CLARUS project	5.2.7	852	General	Personal Identifiable Information (PII)	For example in this context it would be better to change PII to ‘Personal Data’, since it is related to the Data Protection Regulation and you should use the Regulation’s terminology.
OFE		855	Te	This Scenario isn't any different than the hybrid scenario starting on 737 as a broker and a csp have essentially the same requirements .	Merge with hybrid or at least derive more distinct requirements.
SixSq/PaaSword	5	855	General	These scenarios in my opinion neglect the case where PaaS providers or brokers provide hybrid cloud features, notably abstractions to provide interoperability between underlying CSPs, data migration, or automation facilities. In this case, these are not simple brokers as defined in	Please consider adding information about delegation and certification of intermediary services in hybrid cloud scenarios.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				Section 5.2.8 and play a direct role in the consumption of IaaS services. Having an intermediary between the CSC and CSPs brings along additional requirements around the management of user credentials, like delegation, and potentially certification issues around these services.	
FP7 EUBrazil Cloud Connect project	5.2	855	Technical	The scenario of “Federation of CSPs, security in distributed applications deployment” does not fit in the other scenarios. The main difference is that the Federation acts as CSP:inter-cloud provider (as described in ITU-T Y.3502 section 8.3.1.6), in contrast with the brokering scenario presented in Section 5.2.8. The Federation is the only entry point for CSCs: signs contractual agreements with the CSCs, manages the user identities and data, barters resources with third party CSPs, deploys the distributed applications on third party CSPs, and it is responsible for the service in accordance with the contractual agreement.	Add a new section for the Federation of CSP. Below there are some initial insights about this scenario. Scenario description: The CSC procures cloud services via a Federation of CSPs. The CSC negotiates cloud services only with the Federation. The Federation has agreements with the CSPs and determines whether the service can be provided by a single CSP or as an aggregation from multiple CSPs, members of the Federation. The CSC does not need to access or be registered with each single CSP. High-level requirements: The Federation acts as CSP:inter-cloud provider. It negotiates the service with the CSC and it is involved during the consumption of the service. The CSCs set up contractual agreements only with the Federation. The Federation outsources the cloud service, or part of it, to the CSPs and it is responsible to manage peer services, aggregate them and for the management and processing of CSC data and identities. The Federation is responsible to set up agreements with the CSPs and ensures that the service is provided in accordance to the established

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
					agreements. Cloud Service Level Agreements: Two level of CSLA should be established: 1) between the CSC and the Federation 2) between the Federation and the CSPs. The Federation is responsible to monitor the contractual agreements and give evidence to the CSC. Interoperability & portability: This covers interoperability of IaaS and PaaS APIs and corresponding tools to deploy the distributed application in an IaaS CSP or ensure the connection of PaaS services provided by different CSPs. Interoperability and portability are the key to guarantee migration of application if a CSP is faulty. Security: Identity management can involve delegation mechanisms to permit the Federation to request resources and services on behalf of the CSC transparently. Federated identity management can be used to facilitate the management of the user identities and credentials. Data protection: The Federation needs to specify in advance to CSC where the data will be stored and must ensure that the CSC data is well protected. It must prevent any unauthorized access of the CSC data being stored and processed.
TECNALIA	5.2.8	862	Technical	different services	different Cloud services

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Cloud Security Alliance	5.2.8	865	Editorial	The "High-Level Requirements" in this scenario are not presented as in previous scenarios i.e., organized by core concepts.	Please present these requirements organized in core concepts.
TECNALIA	5.2.8	867	Technical	Cloud SLAs	CSLA(s)
TECNALIA	5.2.8	871	Technical	the SLA in brokered	the "CSLA in brokered
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)		874, 902, 1074, 1204 all	Editorial	UNIFIED PATTERN OF CODING IS NEEDED	1. ISO/IEC 17789 – ITU-T Y.3502 2. ISO/IEC 17789 and ITU-T Y.3502 3. ISO/IEC 17789 / ITU-T Y.3502 4. ISO/IEC 27017 I ITU-T X.1631
TECNALIA	5.2.8	915	Technical	the roles should be followed in order ensure	the role should be followed in order to ensure
TECNALIA	5.2.8	923	Technical	tandem. But	combination. Therefore,
TECNALIA	5.2.8	933	Technical	relationship	relationships
Cloud Security Alliance	6 Note: either clause or line number incorrect	615	Technical	You refer to Cloud Customer as owner of the data. What do you mean? The owner of the personal data is normally the "data subject" which is normally the end-user of a cloud customer.	Please correct the reference to the data owner.
TECNALIA	6.1.1	943	Editorial	to able	to be able
OFE		945	Te	What challenges are outstanding? This should be one of the goals of this document yet few are enumerated.	
TECNALIA	6.1.1	947	Editorial	re	read
TECNALIA	6.1.1	948	Editorial	EIF	Add a footnote with reference to EIF.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
OFE		950	Te	There is no discussion on data portability here. What is required to make data portable and what are the challenges for cloud?	Add a paragraph on data portability- the importance of formats, meta-models and semantics.
OFE		963-968	Te	What significant work is required as this paragraph under values the significant work to date made by the industry on app portability? A high level list should at least be enumerated in this report. Regardless, the market – driven by customers - will decide what languages, middleware and platforms make sense, and if there is a need for further standardization.	Either enumerate a list of potential future work (or issues), or delete.
TECNALIA	6.1.2	964	Editorial	in terms	in terms of
TECNALIA	6.1.2	965	Technical	non standard collaborations	The meaning is not that. They have collaborations for non standard oriented portability solutions.
TECNALIA	6.1.2	967	Editorial	that be ported	that can be ported
TECNALIA	6.1.2	970	Editorial	Finally _	Finally,
Cloud Security Alliance	6.1.3	974-1083	Technical	The terminology used doesn't seem to be consistent with widespread information security literature. Concepts like confidentiality and trust are mixed together as well as privacy and integrity as well as privacy and security. Moreover several import information security domains are not considered at all, e.g. incident management, business continuity / disaster recovery, mobile security.	We suggest the editor to rework this chapter and use appropriate references to existing literature to avoid possible misunderstandings.
OFE		975	ed	"Different flavours" imply some nuances, where really we are talking about different aspects/dimensions of security	Change "flavours" to "dimensions"
A4Cloud project	6.1.3	976	General	Cloud services, starting but not limited to IaaS,	Add a sub-section, for example: "Isolation of

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				are often implemented using virtualization technologies. This is associated with a new security property: isolation. This should be addressed as one of the key security functionalities in the list. While the disclaimer in line 976 indicates that the list does not capture all relevant aspects of security, the most important ones should listed.	Virtual Resources: The implementation of Cloud Computing services often relies on the use of virtualization technologies, where a single physical resource is shared to implement multiple instances of a service, each visible to the user as if it were implemented on dedicated physical resources. It is essential that the virtualization technologies implement all required measures and mechanisms to guarantee the isolation of the various service instances, i.e. that there is no possibility for the user of one instance to obtain any information on the data stored or processed in any other instance implemented on the same physical resource.”
A4Cloud project	6.1.3	979	General	While there is an undeniable link between confidentiality and trust, confidentiality alone is far from being the main contributor to trust.	Split section 6.1.3 to separately address Confidentiality and Trust
TECNALIA	6.1.3	979	Technical	Confidentiality and Trust	It is the almost the first time that confidentiality is mentioned in the document, and it is not listed in the core concepts before. It is better to separate it from Trust.
A4Cloud project	6.1.3	980	General	Data encryption is not only important for protecting data during transmission, it is also important for protecting data in storage.	Add “Likewise, encryption can be used to protect data while it is in storage. This is particularly important in the case of multi-tenant clouds, such as Public clouds, where data could be accidently made available to third-parties as a result of storage allocation operations or hardware maintenance.”
H2020 CLARUS project	5.2.7	981	Technical	Encryption	Add "... or even encrypt the data outsourced to the cloud".
H2020 CLARUS project	5.2.7	988	Technical	Verification of computation	Mention that there exist (non-)cryptographic techniques to verify the correctness of the computation on (non-)encrypted data.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
H2020 CLARUS project	5.2.7	988	Technical	Proofs of data storage	In addition, in order to trust on the CSP, the client may need proofs of data storage as an evidence that there are no storage errors.
Cloud Security Alliance	6.1.3	990-991	Technical	The sentence says: "An Initiative that addresses transparency and accountability is the program from Cloud Security Alliance (CSA), "Security, Trust & Assurance Registry (STAR), where CSPs can register and have their offerings ranked." The CSA STAR is the name of the transparency and certification program of CSA, is not a place where cloud offerings are ranked.	Please rephrase as follows: "The Cloud Security Alliance (CSA) maintains the Security, Trust & Assurance Registry (STAR) which is a public repository where CSPs can voluntarily publish the result of their assessment based on CSA CCM/ and ISO27001-2013 or AICPA SOC2. CSPs can submit both the results of their Self Assessment and third party based assessment (i.e. CSA STAR Certification and CSA STAR Attestation) in the registry"
A4Cloud project	6.1.3	990	General	The concept of accountability goes far beyond what is captured by CSA STAR. There are many regulatory references to accountability. Accountability is also highlighted in the opinions expressed by the Article 29 Working Party and the European Data Protection Supervisor (EDPS).	Add a subsection, for example: "Accountability: Accountability is an important but complex notion that encompasses the obligation to act as a responsible steward of the personal information of others; to take responsibility for the protection and appropriate use of that information beyond mere legal requirements; to be transparent (give account) about how this has been done and to provide remediation and redress. This notion is increasingly seen as a key market enabler in global environments and in helping overcome barriers to cloud service adoption. Accountability also has a strong role to play in encouraging appropriate data stewardship by organisations both using the cloud and providing cloud services. An accountability approach mobilizes many of the processes associated with the provisioning of a service, including the identification and acceptance of responsibility by the accountable organisation, the inclusion of an

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
					impact assessment in the risk analysis, the definition and enforcement of clear, complete and relevant policies, the monitoring of practices, the collection and protection of evidence, the deployment of mechanisms and processes to explain and demonstrate compliance to stakeholders and to promptly remedying any failure to act properly."
A4Cloud project	6.1.3	991	General	The CSA STAR program addresses more than the self-assessment scheme that is indirectly referred-to here. CSA STAR also has a Certification / Attestation scheme, and has publicly announced a forthcoming Continuous Compliance scheme	Specifically mention the 3 "grades" of assurance: self-assessment, certification/attestation, and continuous monitoring.
TECNALIA	6.1.3	992	Technical	see i.5	Add reference
TECNALIA	6.1.3	993	Technical	see i.6	Add reference
OFE		995, 1047, 1060	ed	Identity, authentication and authorization should be discussed together and not separately.	Merge under one heading: use sub-sections to structure.
TECNALIA	6.1.3	996	Technical	Identity management	Identity management is only part of IAM, explained in the text. Why not include IAM as core concept and not only Identity Management _
TECNALIA	6.1.3	1007	Technical	the rights allocated to a specific identity.	the rights (over the ICT resources) allocated to a specific identity._
TECNALIA	6.1.3	1010	Technical	No relationship between IAM and Privacy is explained and there are many.	Mention the need of a good IAM system to be able to keep data Privacy.
Cloud Security Alliance	6.1.3	1036	Technical	Presenting "Privacy" as an area under "Security" may be misleading.	Please move "Privacy" (lines 1036 – 1046) to a new subsection 6.1.x
Cloud Security Alliance	6.1.3 and all the doc	1036	Technical	This section and the document in general use "information privacy" and "data protection" as equivalent terms. This is generally incorrect, especially in Europe. Data privacy relates to the	Review definitions of privacy and security, and refer to standard definitions of these terms where appropriate (see Directive 95/46/EC for a description of data protection).

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				confidentiality of data, or the ability/inability to link information to individuals. Data protection deals with much more than protecting the confidentiality of data, it also encompasses, among other things: - The rights of individuals to access their data / rectify / modify it. - The principle of purpose limitation. - The principle of retention limitation. - Data minimization and anonymization. - International data transfer rules. - Data security (confidentiality, integrity and availability). - Etc. All these elements require specific attention in the cloud.	See also other comments related to privacy and security.
TECNALIA	6.1.3	1047	Technical	Authentication paragraph is better to have it just below the Identity Management part as it is very related, and followed by Authorization paragraph (line 1060)	Reordering of paragraphs.
TECNALIA	6.1.3	1048	Technical	of identifying any user	of verifying the authenticity of the identity of any user
TECNALIA	6.1.3	1051	Technical	full reliability of its users	full reliability of all the parties involved.
TECNALIA	6.1.3	1054	Editorial	e g using	e.g. using
TECNALIA	6.1.3	1057	Technical	OpenID Foundation	Add reference in a footnote.
TECNALIA	6.1.3	1067	Technical	OAuth workgroup	Add reference in a footnote.
Cloud Security Alliance	6.1.3 and all the doc	1075	Technical	The document frequently bundles together the notion of privacy and data integrity (this is also the case in the survey). This is an odd choice that is likely to confuse readers and experts in the field.	Review terminology to make it aligned with common use in information security and data protection.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				In information security, integrity describes the "means to protect the accuracy and completeness of information and the methods that are used to process and manage it" (ISO 27000). Integrity is a distinct notion from privacy altogether. Integrity, confidentiality and availability are usually described as the 3 pillars supporting information security. The frequent association of "integrity" and "privacy" throughout the documents seems unjustified (e.g. why exclude "confidentiality"?)	
A4Cloud project	6.1.3	1076	General	While the section on Privacy does refer to data integrity, associating the two topics as done in the section conveys the wrong message; in particular protecting data integrity is required for all data processed and stored by the Cloud Service Provider, whereas only a privacy-relevant data constitutes only a subset of the data handled by the CSP.	Replace "See Privacy." with "Maintaining data privacy and data integrity is increasingly becoming an important but also problematic and complex issue as the value of data and information increases and the sheer data volumes are becoming enormous in size."
TECNALIA	6.1.3	1076	Technical	Integrity is not Privacy but they are related, you need to explain that because "See Privacy" is confusing.	integrity refers to the accuracy and completeness of information, whether it needs to be kept private or not. Use the definition by ISO.
TECNALIA	6.1.3	1088	Technical	how different aspects of come together	aspects of what? how these different aspects come together
TECNALIA	6.1.4	1100	Editorial	privacy.	privacy,
TECNALIA	6.1.4	1151	Technical	user's availability	user's accessibility
OFE		1182	Te	Do not understand Section 7 and how it relates	Clarify the purpose of this section and add some

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				to the 4th report. Is this a subset of the 4th report, is it different in purpose to the 4th report etc	commentary on its relationship with the 4th CSC report.
SICS Swedish ICT/PaaSword	7		General	This list of standards does not give the reader the expected insights/help as most of them are very generic security standards. Furthermore, the different standards are not categorized with respect to how/if they really support the previous listed use cases.	The section could be complemented with a table and/or analysis of the applicability of the different standards in relation to the previous listed use cases.
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	7.1	1186	Editorial	MISSING BRACKET	ISO/IEC 27014(Governance of information security => ISO/IEC 27014(Governance of information security)
OFE		1243	Te	This report has done very little to identify these gaps.	
TECNALIA	8	1258	Technical	see i.2	Add reference
TECNALIA	8	1267	Editorial	CSCs confidence	CSCs' confidence
INTEL	8	1274	Technical	Presumed typo but changes the meaning: elevate > alleviate	elevate > alleviate
TECNALIA	8	1279	Editorial	SSO needs to be differentiated from Single Sign On just in case.	Standards Setting Organisation (SSO)
ICCS/PaaSword	6.1.3	1018, 1030	Editorial	In the list of example technologies and solutions mentioned as related to identity management the concepts of Access control and Role Based Access Control (RBAC) are mentioned in separate bullets although the second term is a specialization of the first one.	Please consider mentioning Access control in one bullet with its specializations/subcategories in a parenthesis (RBAC, MAC, DAC, ABAC)
CAS Software AG/PaaSword	6.1.3	1060, 1069	General	In section 6.1.3 the authors discussed the core concept of security. In this frame the topic of context awareness is not included in this section. Access control by means of the identity and additional on the context, e.g. geo-location	Consider adding context awareness issues into the presented security concept.

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				or the used device, of the user asking for access increases the security of the application.	
Cloud Security Alliance	7	1178-1232	Technical	It is unclear why the standards have been categorised as described in this chapter. Someone would have expected to find standards categories according for instance to the core concept: Interoperability, portability, security, SLA, instead, Interoperability and portability are listed under Security and Cloud SLA falls into the other standard category. We suggest using a more appropriate way to classify standards.	We suggest using a more appropriate way to classify standards. Since this would need a major rework it has to be the main editor to do it.
Cloud Security Alliance	7	1178	Technical	Very few relevant standards between the relevant ones are mentioned. Several standards used in the cloud security space and also included in the previous ETSI effort are left out of this this list. There are major changes to be made in this chapter: 1) provide a justification of on which ground you have selectively chosen some standards vs others and 2) include those cloud security standards that cannot be left out: e.g. NIST, CSA and BSI standards	There are major changes to be made in this chapter: 1) provide a justification of on which ground you have selectively chosen some standards vs others and 2) include those cloud security standards that cannot be left out: e.g. NIST, CSA and BSI standards. Since this is major change in the context of this document it should be the editorial team / main authors to rework the chapter.
Cloud Security Alliance	7.1	ALL	Technical	Several information security standards missing	Please add at least relevant Standards from NIST and German BSI.
Cloud Security Alliance	7.2	1191	General	Categorizing “Privacy” under “Security” may be misleading.	Please add a new subsection “7.x Privacy” containing all items starting on line 1208.
Cloud Security Alliance	7.2	1191	Editorial /Technical	Do you refer to Cloud Specific Standards or Topic Specific topic or both? It would be worth specifying.	Please clarify
Cloud Security Alliance	7.2	1192-1196	Technical	It is unclear why you are adopting such a granular distinction between Authentication and Authorization standards, especially since you	Please merge Authentication and Authorization under the label: Identify and Access Management

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				are mentioning only 1 standard / category	
Cloud Security Alliance	7.2	1192-1196	Technical	Missing standards	Please add other relevant standards, e.g. • ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts • ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements, ISO/IEC WD 24760-3 A Framework for Identity Management—Part 2: Practice • ISO/IEC 29115 Entity Authentication Assurance • ISO/IEC WD 29146 A framework for access management • ISO/IEC WD 29003 Identity Proofing and Verification • etc.
Korea Association of Cloud Industry(KACI) Cloud Computing Standard Forum(CCF)	7.2	1199 ~ 1213	Editorial	PUT UNDER---, OR DO NOT PUT UNDER--- UNIFIED PATTERN OF CODING IS NEEDED	1. Final Draft ISO/IEC 2910 *(Privacy capability assessment model), under FDIS => Final Draft ISO/IEC 2910 *(Privacy capability assessment model) 2. Draft ITU-T X.gpim I ISO/IEC 2915 *(Code of practice for PII protection) => Draft ITU-T X.gpim I ISO/IEC 2915 *(Code of practice for PII protection), under CD
Cloud Security Alliance	7.2	1205	Technical	Missing several standards from CSA and NIST	Please add CSA CCM, CSA CAIQ, CSA CTP, CSA Cloud Audit, CSA Enterprise Architecture, and NIST standards / special publications (http://csrc.nist.gov/publications/PubsSPs.html)
Cloud Security Alliance	7.2	1207	Technical	On the list of references standards is missing the published CSA “Privacy Level Agreement – version 2” (https://cloudsecurityalliance.org/download/privacy-level-agreement-version-2/)	Please add the following to the list (after line 1213): “CSA PLA (Privacy Level Agreement)”
Cloud Security Alliance	7.2	1207	Technical	Missing standards	Please add CSA Privacy Level Agreement v2

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Cloud Security Alliance	7.3	1216-1220	Technical	Very relevant security and cloud certification standards are missing. For instance: FedRAMP (especially important for the Public Sector audience), AICPA SOC 1-2-3	Please add FedRAMP AICPA SOC 1-2-3
Cloud Security Alliance	7.3	1218	Editorial	The following entry has an error: “CSA OSF Level 2”	Please correct to: “CSA STAR Certification Level 2”
Cloud Security Alliance	7.3	1218	Technical	This section only lists one of the applicable certification schemes related to CSA STAR.	Please add the full list of CSA STAR certifications: “CSA STAR Self Assessment - Level 1 CSA STAR Certification - Level 2 CSA STAR Attestation - Level 2”
Cloud Security Alliance	7.3	1218	Technical	The reference to CSA certification standards is completely wrong. The Open Certification Framework (OCF) Working Group (not OSF) is the technical WG that oversees the CSA certification effort (a parallel would OCF WG vs ISO SC27). The CSA STAR is the name of the overall certification program. The names of the CSA certification standards are: • CSA STAR Certification (ISO27001+CCM) • CSA STAR Attestation (SOC2+CCM) • CSA C-STAR (Chinese equivalent of ISO27001+CCM) • CSA Self Assessment We would recommend you consult the ENISA or CSA web sites: https://resilience.enisa.europa.eu/cloud-computing-certification https://cloudsecurityalliance.org/star/	Please replace CSA OSF level 2 with: • CSA STAR Certification (ISO27001+CCM) • CSA STAR Attestation (SOC2+CCM) • CSA C-STAR (Chinese equivalent of ISO27001+CCM) • CSA Self Assessment

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Cloud Security Alliance	7.4	1222-1232	Technical	Several reference to standards are not accurate: COBIT? Which version ITIL ditto, ISO 19086, which part? 1-2-3-4	Please add appropriate references to standards
Cloud Security Alliance	8	1234-1283	Technical	There is no analysis result in this document to support the conclusion and recommendations.	Please substantiate the statements in the conclusion with facts/ results of the analysis
Cloud Security Alliance	8	1243	Technical	The current text seems to imply that identified interoperability and security gaps will be covered with an "enough" number of standards and certifications. This may be misleading, taking into account that the CSC may be unaware of which standards and certification are really needed to fulfil his security and privacy requirements.	Please add the following text at line 1249: "Despite the undisputed advantages of Cloud computing, customers (in particular small and medium enterprises – SMEs) are still in need of "meaningful" understanding of the security and privacy changes that the Cloud entails, in order to assess if this new computing paradigm is "good enough" for their security requirements. Cloud-specific risk management frameworks are conspicuously missing at the state of the art, and are needed to empower CSC with information related to the levels of security and privacy that are required in their own contexts."
Cloud Security Alliance	8	1243	Technical	Despite being identified in the first ETSI CSC report, there is no mention to the existing gap in standards related to machine-readable specifications, for example in the area of CSLA.	Please add the following text at the end of the "Outstanding gaps" subsection: "Standardised machine-readable specifications are required to improve both interoperability and security in Cloud computing, in particular related to the adoption of realistic levels of automation in areas like CSLA management."
Cloud Security Alliance	8	1266	Technical	The following text: "The same need can be applied to certifications; well-structured and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the	Please change the following text: "The same need can be applied to certifications; well-structured and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
				CSCs confidence in the Cloud. ” Misses the fact that the (security) assurance provided by certification schemes strongly depends on the periodicity of the assessment, where continuous (security) certification for the Cloud is a topic that appears on novel schemes like CSA STAR Level 3 Continuous.	CSCs confidence in the Cloud. ” To: “The same need can be applied to certifications; well-structured, continuous and relevant profile based certification schemes will probably increase the uptake of Cloud Computing, by increasing the CSCs confidence in the Cloud. ”
Cloud Security Alliance	8	1272	Editorial	The following text: “The relevance and potential high-value use of the upcoming framework for Cloud SLA must also be mentioned as part…” Does not clarify to which “upcoming framework for Cloud SLA” it refers.	Specify the referenced framework (supposedly ISO/IEC 19086?).
Cloud Security Alliance	8	1275	Technical	The following text: “Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report.” Does not highlight the relevance of Cloud SLA metrics, in particular for security and privacy (as highlighted in ISO/IEC 19086-P4).	Please change the text: “Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report.” To: “Using existing standards for Cloud Computing terminology and the roles, sub-roles and activities defined in the Cloud Computing Reference Architecture along with the definition of security/privacy metrics, will additionally simplify the creation of Cloud SLAs that can encompass and address the core concepts discussed in this report.”

Organization	Section	Line Number	Comment Type General, Technical, Editorial	Comments	Proposed change
Cloud Security Alliance	ANNEX A	1299	Technical	Several references are missing from the Bibliography	Please add missing references