Project Acronym: CUMULUS
Project Title: Certification infrastrUcture for MUlti-Layer cloUd Services
Call identifier: FP7-ICT-2011-8
Grant agreement no.: 318580
Starting date: 1st October 2012
Ending date: 30th September 2015

D6.6 Final Evaluation Report

AUTHORS: Matthias Junk (IFX), Vittorio Bagini (FUB), Renato Menicocci (FUB), Alessandro Riccardi (FUB), Antonio Álvarez (ATOS), Lorna Woods (CITY), Jake Newell (CITY), George Spanoudakis (CITY), Maria Krotsiani (CITY), Jesús Luna (CSA), Antonio Maña (UMA), Hristo Koshutanski (UMA), Ignacio Sanchis (WELL)

REVIEWERS: Maria Rosa Viera (ATOS), Claudio Ardagna (UMIL)

Summary

EXECUTIVE SUMMARY **4**
1. INTRODUCTION **5**
2. BUSINESS EVALUATION **7**
2.1. Current practices on certification 9
2.1.1. General considerations *9*
2.1.2. Metaframeworks of certification *10*
2.1.3. Undergoing the process of certification *15*
2.2. Justifying the need of certification 18
2.3. CUMULUS contribution from the point of view of the main stakeholders 19
2.3.1. The Cloud Certification Provider perspective *19*
2.3.2. The Cloud Auditor Perspective *20*
2.3.3. The Cloud Provider Perspective *20*
2.3.4. The insurance companies and their accountability *21*
2.4. Outlook and Next Steps 22
3. EVALUATION OF CERTIFICATION FRAMEWORK **24**
3.1. Introduction 24
3.2. First Session with External Validators 24
3.2.1. Session Design and Execution *24*
3.2.2. Session Results *31*
3.2.3. Outlook and Next Steps *39*
3.3. Second Session with External Validators 40
3.3.1. Session Design and Execution *40*
3.3.2. Session Results *44*
3.3.3. Outlook *47*
4. EVALUATION OF TRUSTED COMPUTING PROJECT RESULTS **48**
4.1. Introduction and recapitulation from D6.2 48
4.2. Overview of CC certification of Infineon TPM 48
4.3. Performed work and achieved results 50
4.3.1. TPM 2.0 Security Evaluation Test Tool *51*
4.3.2. Cryptographic Security Functional Requirements *51*
4.3.3. Measuring and reporting Security Functional Requirements *52*
4.3.4. Security Assurance Requirements *52*
4.3.5. TPM Security Evaluation Documentation *54*
4.4. Conclusions 55
5. CUMULUS ENGINEERING TOOL EVALUATION **56**
5.1. First Focus Group Evaluation 56
5.2. Second Focus Group Evaluation 57
5.3. Conclusions 57
6. LEGAL EVALUATION **59**
6.1. Overview 59
6.2. Contractual Liability 59
6.3. Non contractual liabilitity: Tortious liability and Negligence 61
6.4. Data protection and regulatory matters 61
6.5. Using CUMULUS Evidence in Court 62
6.5.1. Criminal Law *62*
6.5.2. Civil Law *63*
7. ONLINE SURVEY FOR EXTERNAL EVALUATORS **64**
7.1. Introduction 64
7.2. Survey Results 64
7.3. Conclusions and Next Steps 67
8. APPENDIX 1 – EVALUATION OF CERTIFICATION FRAMEWORK: FIRST VALIDATION SESSION **69**

9. APPENDIX 2 – EVALUATION OF CERTIFICATION FRAMEWORK: SECOND VALIDATION SESSION 69
10. APPENDIX 3 – ONLINE SURVEY FOR EXTERNAL EVALUATORS 69
11. APPENDIX 4 – SUMMARY OF CUMULUS PROJECT RESULTS 69
12. APPENDIX 5 – MAPPING ENISA CCSM TO CUMULUS SECURITY PROPERTIES 70
13. APPENDIX 6 – CUMULUS ENGINEERING TOOL EVALUATION QUESTIONNAIRE 86
REFERENCES 88

List of Figures

Figure 1. Framework structure 10
Figure 2. Open Certification Framework 11
Figure 3. CUMULUS in the context of ENISA CCM 15
Figure 4. Cloud-Based Security Market Size Forecast (Source Gartner) 18
Figure 5. Common Criteria Certification Process 48
Figure 6. Common Criteria Evaluation Assurance Levels 49
Figure 7. Evaluation Assurance Level Notation 50

List of Tables

Table 1. Scoring of controls 12
Table 2. Control areas considered in CCM to apply to CSA OCF 12
Table 3. Security Rating Guide: process example 14
Table 4. Synthesis of the cost effectiveness analysis presented to the session with external validators 28
Table 5. Questions proposed for the session with external validators 31
Table 6. Raw results of the responders to the questionnaire. 32
Table 7. Questions proposed for the session with external validators 43
Table 8. Raw results of the responders to the questionnaire. 44
Table 9. Overview of CUMULUS relevant tests 51
Table 10. TPM V2.0 Cryptographic SFR 52
Table 11. TPM V2.0 Measurement and reporting SFR 52
Table 12. Security Assurance Requirements for the TOE 54
Table 13. TPM Security Evaluation Documentation 54
Table 14. Documentation after evaluation 55
Table 15. Documentation after CC certification 55
Table 16. Online Survey Responses 66
Table 17. Online Survey – Participants' Background 67

Executive Summary

Deliverable D6.6 provides the final report on the evaluation of CUMULUS project results. This report covers the following aspects: Business evaluation, evaluation of the certification framework, evaluation of Trusted Computing project results, evaluation of the CUMULUS Engineering Tool, legal Evaluation and the CUMULUS online survey for external evaluators.

The following new topics have been added to the final version of this report: Legal evaluation, CUMULUS online survey for external evaluators, evaluation of Certification Framework (second session with external evaluators), evaluation of the CUMULUS Engineering Tool, mapping ENISA CCSM to CUMULUS Security Properties.

1. Introduction

Deliverable D6.6 describes the evaluation of CUMULUS project results and provides the according evaluation results. The goal was to reassess that what has been made and accomplished in CUMULUS can do the following:

1) Contribute to and enhance the state of the art in the field of certification of cloud services

2) Entail a big leap forward which can be leveraged in the future.

Evaluation is accomplished from different perspectives, which are covered in sections 2 - 7 of this document.

This report builds on the results of previous deliverables as follows:

- The Specification of CUMULUS Evaluation Criteria (D6.2) presented the criteria that would be followed to perform the evaluation. These criteria come from the scenarios and the requirements presented as a result of Task 6.1 and covered in D6.1. When it came to applying these criteria, some of them were applied as they were designed. Others suffered some modifications, whereas some new criteria arose, as a result of putting evaluation into practice. This is not surprising, since what is descripted in D6.2 is a first approach to such criteria.
- The Initial Evaluation Report (D6.5) explained the general approach of both business related and technical evaluation, and provided the first set of results, e.g. concerning the CUMULUS Certification Framework, and concerning Trusted Computing project results.

This deliverable (D6.6) adds legal evaluation aspects and describes how in year 3 external evaluators were even more involved in the evaluation of CUMULUS project results (e.g. via the online survey for external evaluators, the second Certification Framework evaluation session with external evaluators, and the evaluation of the CUMULUS Engineering Tool).

The rest of this document is structured as follows:

- Section 2 deals with the evaluation from the business point of view. This section and all the work related is envisaged to gather evidence of the benefits that all the stakeholders involved in the cloud business might obtain from the innovation brought by CUMULUS. It aims to gather evidence of the need of security placed by the market in general, for example what makes appealing the adopting of a product like CUMULUS in order to provide the required assurance. Another way to evaluate the soundness of the concept of CUMULUS is by analysing the contribution that it may make to the current landscape of certification meta-frameworks. Companies that adopt CUMULUS must also consider the related costs and find out whether it makes sense to introduce CUMULUS as a way to improve security. This evaluation is, in consequence, mostly based on an ongoing analysis as reported in this deliverable.
- Section 3 deals with the evaluation of the certification framework itself. Aspects like usability, representation capability, perceived security, assurance and cost effectiveness are assessed. In order to do so, people outside the consortium were involved and two sessions took place to collect feedback. All the material produced for these evaluation sessions including raw results from validators are referenced (see appendices 1 and 2).
- Section 4 deals with the validation of Trusted Computing project results. Since the TPM serves as a root of trust in CUMULUS, it must be properly certified so that one can rely on the TPM fulfilling all necessary security requirements. To ensure this, the Common Criteria certification is undertaken and applied to the new TPM 2.0 chip. The corresponding security evaluation of the TPM properties related to CUMULUS requirements is done within CUMULUS.
- Section 5 describes how external experts were involved in the evaluation of the CUMULUS Engineering Tool. Evaluation results are summarized and conclusions presented. Two evaluation sessions with defined focus groups were conducted. The evaluators' feedback was considered in the design of the second version of the engineering tool, which resulted in GUI improvements.

- Section 6 presents legal evaluation aspects. It is a supplemental report to the legal evaluation framework set in deliverable D6.2 [13] and is based on the same factual assumptions and methodological approach. It specifically considers the following aims: 1. Identify significant changes in the law affecting cloud computing certification audits and auditing techniques using England and Wales as a case study. 2. Consider the rules relating to evidence in court proceedings with regard to logs produced by the CUMULUS infrastructure for cloud service certification. 3. Provide an assessment of the legal aspects of the use of the CUMULUS infrastructure by taking into account the latest version of it and the certification approach underpinning it.
- Finally, section 7 describes how the group of external experts evaluating CUMULUS project results was enlarged via an online survey. CUMULUS stakeholders such as developers, providers and users of cloud services, evaluators and certifiers of ICT security and other experts were asked to participate in the survey by filling out an online questionnaire, which can be accessed from the CUMULUS web site. High-level survey results are presented in this section, and the complete results are available in a separate document.

2. Business evaluation

D6.2 suggests some evaluation criteria to take into account to perform the validation of the framework from the business perspective, and it is focused on the application scenarios proposed in the project. Below, the criteria are reviewed and the specific application to the scenarios is discussed:

- Criterion 1: *Study which services and layers are going to be certified by CUMULUS*. This service and layers are specified in deliverables D6.3 and D6.4, related to the pilots. During year 3 new security properties were proposed for certification as a consequence of the development of new hybrid and incremental certification models.
- Criterion 2: *Define the attributes to consider the property as 'verified'*: As it will be discussed in this subsection, some widely accepted criteria need to be taken into consideration to make the certification process reliable. In response to this demand, we will follow the criteria established in *NSA protection profiles* [18][19][20] , which has been proposed within the consortium. .
- Criterion 3: *Update the service in order to interact with CUMULUS mechanisms*: Both Smart Cities and e-Health scenarios have been adapted in order to interact properly with the CUMULUS Framework. Besides, in order to certify security properties chosen in Criteria 1, some security mechanisms must be in place. In D6.3 and D6.4 the improvements in security that both scenarios have experienced are explained carefully.
- Criterion 4: *Evaluate risks of applying the CUMULUS Framework with respect to costs and security*: Throughout the development of WP6 we have quantified the cost of applying CUMULUS to a couple of pilot scenarios and we have considered the risks that the certification process for certain security properties entail. However, regarding the costs, we could only know them *a posteriori*, and, as it is stated in the section, these costs are really uncertain when calculated in advance. The reason is that the disparity among scenarios is so big that it is really difficult to make estimations basing on previous experiences

Apart from these criteria, we propose some new ones to make the validation more complete:

- Criterion 5: *Analyze how CUMULUS can play a role in the context of certification metaframeworks*. As one of the goals of the project is to contribute to the state of the art of certification, one metric to validate the framework is to obtain convincing evidence about the contribution of CUMULUS to these certification metaframeworks [2][3][11][12][18][19].
- Criterion 6: Offer arguments for the need of certification of security in the cloud field (including pilots domains), according to market demands. This is about offering proofs of the market demanding such security and, in consequence, the need of such security being certified to provide assurance.
- Criterion 7: *Offer arguments proofing the benefits different stakeholders can obtain* from the application of the CUMULUS Framework in order to provide assurance about security of cloud services.

This section is structured in the following way:

- Section 2.1 intends to provide an overview about the current practices regarding the certification process, and give a first approach on the role CUMULUS might play in this field.
    - Section 2.1.1 goes through the general considerations of certification. Some key-points about specific requirements a certification process must fulfill are specified. Then, the current approach of certification to the current case of cloud computing is explained, highlighting that cloud-aimed certification can never replace more generic schemes, but rather supplement them.
    - Once a general consideration of what certification is about, and a first approach to how it is applied to cloud computing is provided, section 2.1.2 gives a high-level overview of the

current landscape of metaframeworks of certification, analyzing more deeply how a couple of those metaframeworks are applied (CCM applied to CSA OCF and Security Rating Guide). For those particular metaframeworks, the process of evaluating the different cloud assets applying several criteria, and the way the final evaluation result is calculated, are explained. Once this is done, it is analyzed a first approach on how CUMULUS can play a role in the context of certification metaframeworks. This would correspond to Criterion 5. Deliverable D6.6 covers the work carried out to evaluate CUMULUS from the point of view of this criterion.

  - Finally, once the current certification environment is explained and the likely role CUMULUS could play on it, section 2.1.3 deals with the materialization of the certification process. First, the motivations both public and private organizations may have to undergo a certification process, and the benefits it can bring to them are addressed. These motivations are good reasons clearly supporting the use of CUMULUS, moreover given the fact that can provide automation to such process. Then, some aspects like the time it takes; how the size of the organization, the scope of the certification or the previous experience shape the process; or the typical cost are discussed. Finally, the requirements a person must fulfill to offer certification services playing the role of auditor are also enumerated.

- Section 2.2 provides a set of references demonstrating first the growing demand of security services in the cloud domain and secondly, the need of certification as a way to increase the trust on cloud platform. This includes the contexts of Smart Cities and Health applications, which are particularly relevant, since those two contexts are the ones the pilots are based on. In the particular case of Smart Cities, the possibility of cyber attacks against cloud assets controlling, for instance, public lighting, could provoke blackouts in a whole city with dramatic consequences. This possibility is higher as the Internet of Things paradigm becomes more and more real. Such need of enforcing security requirements will be accompanied by the need of certification providing assurance. This could be a clear business case for CUMULUS, where the framework and infrastructure created within the project can play an important role to develop this new business model and fulfill the need of security against these likely attacks. This corresponds to Criterion 6. In the case of the eHealth, this is also a domain vulnerable to cyber attacks, and due to the critical data managed, requires the highest level of security, however, the main driver for certification in this context would be checking compliance with the legal framework. Consequently, thanks to CUMULUS we can demonstrate, first of all, that the security mechanisms required by law are in place, and secondly, that they are operating as expected.

- Section 2.3 offers a first approach to the analysis of the contribution made by CUMULUS from the point of view of the different stakeholders. Deliverable D6.6 covers the whole analysis, corresponding to Criterion 7.
  - Section 2.3.1 deals with the business benefits CUMULUS brings to cloud certification providers
  - Section 2.3.2 discusses the impact CUMULUS might have in the activities carried out by cloud auditors.
  - Section 2.3.3 discusses the benefits CUMULUS can bring to cloud providers, along with the problems the adoption of the framework can entail.
  - Finally, section 2.3.4 discusses the vision of the insurances companies protecting the cloud service providers in case of cloud-related incidents originating damages to cloud assets.

2.1. Current practices on certification

2.1.1. General considerations

In an ENISA (European Union Agency for Network and Information Security) [1] study published in 2007 the authors define certification as the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements [5]. The main objective of certification is to inspire trust. A certification scheme can be defined as the collection of requirements, procedures and means available for obtaining a certificate.

Certification often means compliance with a standard. ISO defines an official standard as follows: document established by consensus and approved by a recognized body that provides, for common and repeated use, rules guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context [6]. However, standards can also be set de facto, by private actors. By way of illustration, the so-called 'Common Criteria' is a certification scheme where the security level of a product is evaluated according to a set of criteria defined in the international standard ISO/IEC 15408.

Certification as defined in the aforementioned ENISA study, is the final stage of a longer process. This process is usually designated with the term conformity assessment. During a conformity assessment a person or a body will evaluate compliance of persons, products and or processes with a given set of requirements. It is important to emphasize that (i) the evaluation and (ii) the certification, are not necessarily performed by the same body [4].

Cloud computing is such a new discipline that its standardization and everything related is a tall order in progress nowadays. Included in the aforementioned standardization would be the processes aimed at the certification of the security of cloud services. Europe, in this sense, needs to catch up with other countries where certification is already a part of the cloud strategy [43] such as USA, Singapore, Thailand, China, Hong Kong or Taiwan. These countries are starting to discern and pave the way to follow. The goal is to implement a reliable ISMS (Information Security Management System). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems [4]. The cloud-focused schemes tend to draw upon six existing established standards "families", namely: NIST, ISO, PCI-DSS, COBIT, ITIL and accounting-based standards. None of these six ones provides a general purpose standard for cloud computing, although the ITU-T has developed a set of high level recommendations for cloud computing [8]. Most certification schemes are privately run. Industry bodies have had an influential role in their development [9].

As a first step, the work previously accomplished in the field of the certification of information security certification schemes can be leveraged. This work has been developed during previous years much before the emergence of cloud computing. By means of rigorous analysis, organizations like ENISA and related work groups such as CERT-SIG, have found out some of the requirements a certification scheme must fulfill when applied to cloud providers. Among others, it could be highlighted that the certification should be voluntary, never imposed, and driven by industry; should provide the possibility of self-attestation, regardless of the issuing of certificates by an external authority; be technology neutral, be lean and affordable (nevertheless, this criterion is rather subjective) and leverage global standards as much as possible [2]. With this input, some of the current standards are likely to be applied to the particular case of cloud computing.

The agreement on the need of certification as a key requirement to trust cloud services is clear. Nevertheless so far the work is made separately and there are different approaches depending on the countries, even regions within the countries, the kind of sector (public or private) or the working groups. Furthermore, some companies are represented in more than one group and the fact that there many different approaches with a far from negligible overlap is quite clear. Given the clear borderless character of cloud computing, it is necessary to converge step by step on a universal certification view which is compliant with different legislations around the world and is inclusive, counting on both big and small companies, as it was highlighted previously. This view cannot be composed of a single scheme covering everything. The different security requirements have to be grouped properly in different

certification schemes. This will simplify the certification process for any company, since they will be able to focus on what is really crucial for them. In [2] ENISA highlights that it should be very positive to get (i) a list of existing certification schemes and (ii) a meta framework of existing certification schemes detailing the requirements covered by each scheme. This would provide more transparency to costumers and would allow them to map their detailed security requirements to the certification of a provider.

The case of public sector is quite striking. In some cases, a list of requirements is elaborated basing on the input obtained by prospective contestants in those tenders. By doing this, the alignment between what providers actually offer and the expectation of the public sector representatives is much more accurate.

It is interesting to highlight ENISA point as for self-attestation. CERT-SIG lists the possibility of self-attestation as a key principle. Companies should have this possibility in order to make a certification scheme affordable for smaller companies, as no third-party audits would be necessary. In fact, smaller provider´s circumstances seem not to be taken into account when certification processes are addressed.

Finally, it is important to stress that cloud specific assessment should never be seen as replacements for certification processes, but a supplement. For instance, CSA STAR certification assessment (which will be addressed on section 2.1.2) should be seen as part of an ISO 27001 assessment [11] and, in consequence, the scope of ISO 27001 certification must not be less than that of the scope of the STAR Certification.

2.1.2. Metaframeworks of certification

During year 2014, ENISA was working on the creation of a metaframework of security measures for cloud providers [2]. The framework has a tree structure shown in the figure, where there are several domains each of them containing a set of high level security objectives and, in turn, there will be a detailed set of detailed security measures, grouped in sophistication levels. These sophistication levels are necessary so as to be flexible enough to deal with different types of services and different types of customers. ENISA also highlights the importance of not considering a one-dimension rating of security. This is because security can be considered from several points of views: physical security of the infrastructure (especially at IaaS level), security from the point of view of software development or security from the point of view of human resources, to name but a few. Thus, if a one-dimension rating is employed, all these aspects are grouped when they actually need a separate treatment. This need is exactly the same for both providers and customers.

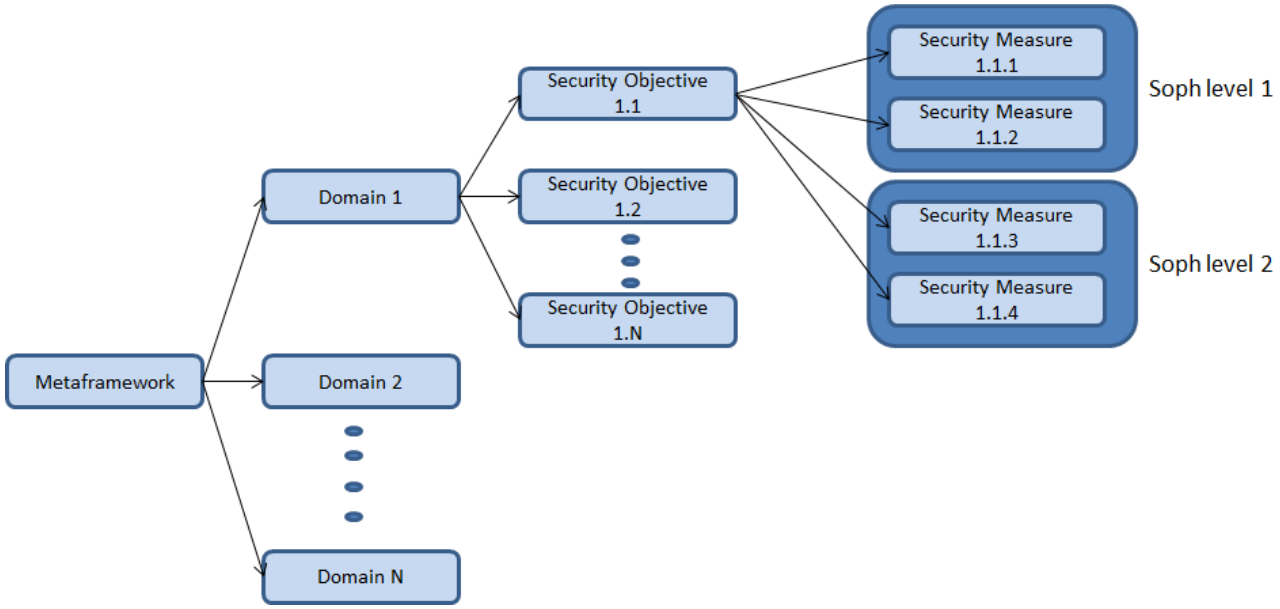

Figure 1. Framework structure

Regardless of how the certification process is set out, it must cover the core Service Level Agreements the organization has with its clients [11].

CCM applied to CSA OCF

A practical example of this kind of frameworks could be CCM (Cloud Control Matrix) [3] which is present at the three levels of the CSA OCF (CSA Open Certification Framework). CCM, in the case of v3.0.1, is a framework structured in 16 domains and composed of 133 controls, which are relevant for cloud [2]. Some of them are to be considered control objectives and others are more detailed technical requirements. The set of controls included in CCM are cloud relevant controls. These controls are also mapped against other rather generic frameworks focused on information security control, and not specifically aimed at cloud, such as ISO 27001:2005 [25], NIST SP 800-53 [26], FedRAMP [27], PCI DSS [28], COBIT v4.1 [29], AICPA Trust Principle, ENISA IAF [30] and the German BSI Cloud Security Catalogue.

Let us see the particular application example of CCM to CSA OCF. The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud provider. It leverages the requirements of the ISO/IEC 27001:2013 and the CSA CCM and is technology-neutral. It measures the capability levels of the cloud service and assigns a 'Management Capability' score to each of the CCM security domains. It is a management systems standard, which outlines the processes and procedures an organization must have in place to manage Information Security Issues in core areas of the business. The standard does not stipulate how a process should operate.

Figure 2. Open Certification Framework

When an organization is audited, a Management Capability Score will be assigned to each of the control areas in the CCM. This will indicate the capability of the management in this area to ensure the control is operating effectively. The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

Score	Descriptor
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement Based Approach
13-15	Optimising Approach

Table 1. Scoring of controls

CSA OCF uses 11 out of 16 control areas of CCM. These areas are specified on the table below. Each of them will be awarded a management capability score on a scale of 1-15

CONTROL AREAS
Application & Interface Security
Audit Assurance & Compliance
Business Continuity Management & Operational Resilience
Change Control & Configuration Management
Data Security & Information Lifecycle Management
Data Center Security
Encryption & Key Management
Governance & Risk Management
Human Resources
Identity & Access Management
Infrastructure & Virtualization Security
Interoperability & Portability
Mobile Security
Security Incident Management, E-Discovery & Cloud Forensics
Supply Chain Management, Transparency & Accountability
Threat & Vulnerability Management

Table 2. Control areas considered in CCM to apply to CSA OCF

When assigning a score to a control area the factors to be considered are, namely: Communication and Stakeholder Engagement; Policies, Plans and Procedures, and a systematic approach, Skills and Expertise; Ownership, Leadership and Management; and Monitoring and Measuring. The lowest score against any one of those 5 factors will be the score awarded for the control area. As mentioned before, the score can range from 1 to 15. If a client has a major Non-Conformance Report (NCR) in an area, the maximum possible score will be 6. Once all control areas are scored, the average score will be used to assign the overall level for the client.

In [12] the assessor´s grid with the criteria to evaluate each factor and ascertain the corresponding mark can be found. Also in [12], an example of how an assessor might audit a control area can be read.

Depending on the result of evaluation (average score), a client will either get: Gold Award (more than 9), Silver Award (between 6 and 9), Bronze Award (between 3 and 6) or No Award (less than 3).

Security Rating Guide

Another example of framework will be leveraged to explain on detail the rating process. Security Rating Guide [18] is a framework provided by Leet Security, SL [19] which considers a set of security measurements, classified in 14 areas, namely: Information Security Management Program, Systems Operation, Personnel Security, Facilities Security, Third-party processing, resilience, compliance, malware protection, network controls, monitoring access control, secure development, incident handling and cryptography. These areas will be named as chapters. Every chapter is in turn divided in a number of variable different elements (so-called dimensions, hence the fact of being a multi-dimensional rating system) that should be considered to evaluate the rating of each chapter, namely: common security measures, security measures regarding confidentiality, security measures regarding integrity and security measures regarding availability. For each element, the conditions needed to achieve each rating level are defined. Five rating levels: A, B, C, D, and E are defined. They are cumulative, so achieving B implies achieving C, D and E. In order to aggregate the rating levels obtained, the formula is the minimum one. This is, when aggregating rating levels the result is the minimum of the levels achieved in each element of the chapter. In turn, the overall rating level is the minimum one obtained among all the chapters (instead of the average as with CCM). Thus, the overall evaluation of the service is based on the weakest component. This rating system has the peculiarity of being applied by the provider itself, who is doing self-assessment, but with the surveillance of Leet Security. This is applied to both the first time the self-assessment is carried out and subsequent modifications. The process is summarized in the table below, where an example is provided.

	DIMENSIONS						
		Common Security Measures	Security Measures regarding Confidentiality	Security Measures regarding Integrity	Security Measures regarding availability	RATING	
CHAPTERS	Information Security Management Program	B	A	A	B	B	C
	Systems operation	A	A	A	A	A	
	Personnel Security	A	A	A	C	C	
	Facilities Security	B	B	A	B	B	
	Third-Party Processing	A	A	A	A	B	
	Resilience	B	A	B	A	B	
	Compliance	A	A	B	A	B	
	Malware protection	B	B	B	B	B	

	Network Controls	A	A	A	A	A	
	Monitoring Access Control	B	B	B	B	B	
	Secure Development	B	A	B	B	B	
	Incident Handling	A	B	A	A	B	
	Cryptography	B	B	B	A	B	

Table 3. Security Rating Guide: process example

CUMULUS in the context of certification metaframeworks

In a recent report from ENISA [22] is introduced the Cloud Certification Schemes Metaframework (CCSM), which maps common security requirements from the European public sector to a set of "security objectives" that should be achieved by suitable Cloud certifications. The CCSM comprises 27 security objectives, derived from the analysis of 29 relevant documents with NIS (Network and Information Security) requirements from 11 countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece, Denmark). As mentioned by ENISA's report "…the goal of CCSM is to provide more transparency and help customers in the public sector with their procurement of cloud computing services." [22].

In order to achieve CCSM's main objective, ENISA is in the process of mapping security controls from well-known frameworks1 (e.g., CSA CCM, and ISO/IEC 27001) to CCSM's security objectives. Given this context, how can Cumulus play a relevant role? A high-level representation of our proposal (to be explained in the rest of this subsection) can be seen in the figure below, where:

1. A set of certification schemes is previously mapped to ENISA CCSM (e.g., CSA OCF and ISO/IEC 27001 as seen in the figure below). This mapping relates security controls from existing certification schemes, to the security objectives defined by ENISA CCSM. The final result shows how well the former are able to cover the requirements for security certifications suggested by ENISA[2].
2. A Cloud Customer from European public sector is trying to select the CSP(s) that better suits its security requirements, by looking at the information published on ENISA's "Cloud Certification Schemes List".
3. Finally, the selected CSP(s) implements Cumulus' certification technology and processes in order to allow the Cloud Customer get assured by continuous/automatic certification of some of ENISA's security objectives from CCSM.

[1] The whole list can be found on ENISA's Cloud Computing Certification website https://resilience.enisa.europa.eu/cloud-computing-certification

[2] At the time of writing this document, ENISA has published a tool that shows the result of the discussed mapping https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework

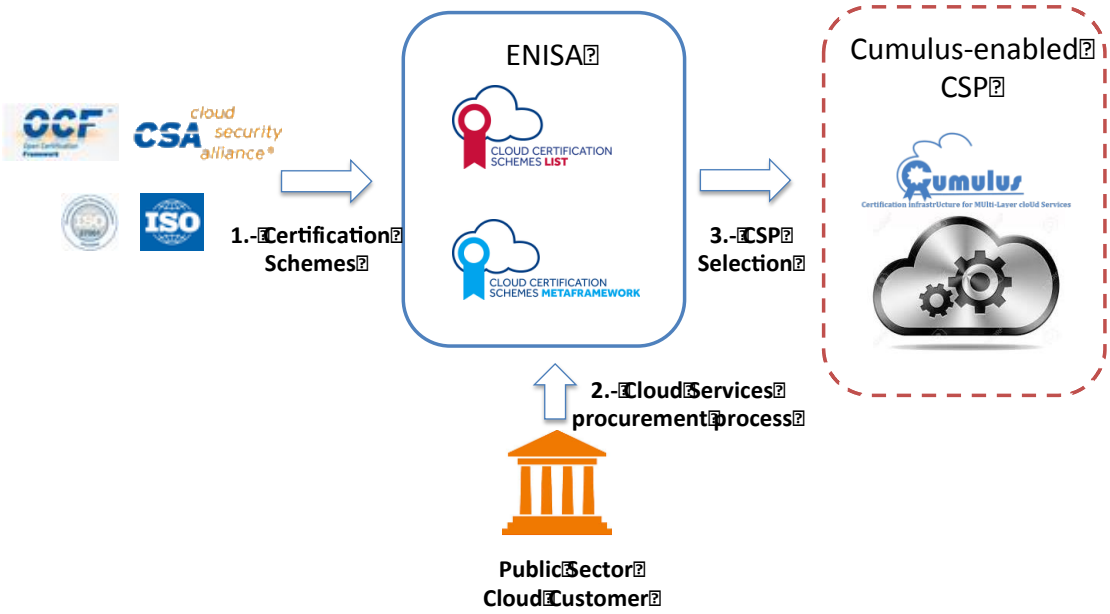

Figure 3. CUMULUS in the context of ENISA CCM

Given the scenario described above, a validation activity for Cumulus performed the gap analysis between Cumulus' security properties and ENISA CCSM's security objectives. The full results of this mapping are reported in Appendix 5, where for completeness reasons the mapping was also done with respect to CSA CCM. All 27 security objectives from ENISA CCSM could be mapped to a corresponding CSA CCM control, however the following objectives did not have a corresponding Cumulus security property associated to it:

- SO 05 - Background checks
- SO 07 - Personnel changes

This was partially expected, because as discussed in this Deliverable some security objectives/controls need human intervention for their assessment. Certification schemes planning to leverage Cumulus should take this fact into consideration.

There are also security objectives that are partially covered by Cumulus, which is the case of "SO 08 - Physical and environmental security" and "SO 04 - Security in Supplier relationships". The automation features contributed by Cumulus are expected to provide some benefit even to the assessment of these objectives.

Future activities related to Cumulus should target the elicitation of new properties in order to provide more/full coverage of the ENISA CCSM security objectives. Some of these activities (expected to continue after the duration of Cumulus) will be driven by CSA3, just as presented in the final Cumulus Exploitation report.

2.1.3. Undergoing the process of certification

Certification focused on cloud was born in a more general context, aimed at information systems in general. Because of that, it is necessary to bear in mind that there are not only cloud focused certification schemes but also more general certification schemes that are at least partly relevant to the delivery of cloud computing services. That is, the field of cloud computing certification contains both cloud-focused

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

certification schemes and schemes with a wider applicability (for instance, security, service management or data protection), which can be adopted to cloud computing.

Successful cloud certification schemes appear to include the provision of real benefits; relevance; recognition and reputation; transferability and adaptability; transparency. On the other hand, potential shortcomings are: issues related to the adequacy; focus; purpose and complexity of standards; process and administration issues; problems with transparency and public communication, including a lack of awareness; and limitations in the assessment process.

Having said this, it is convenient to think about the motivations leading a company to decide to obtain certification of their cloud systems and in general, to obtain ISMS certification. The reasons can be both internal and external. Undergoing a certification process means to check all the services of the company during the preparation for the certification. This will lead to an improvement of the quality (this is also mentioned in section 2.3.3, on the benefits of CUMULUS from the point of view of the cloud provider). Besides, making the system formal (by means of certification) greatly improves the ordinary management of security and, in addition, raises the security awareness of the employees. From the external point of view, the acquisition of a certificate is a marketing and competitive advantage with a good impact both in current and prospective customers (also mentioned in 2.3.3). Moreover, it is more and more common customers driving certification by placing it as a requirement to be fulfilled by a company. Therefore, meeting customer expectations is another motivation to undergo a certification process. Finally, another motivation would be certification being a requirement for procurement procedures [4].

In the case of public organizations their motivations have to do with their awareness of the importance of security and their desire to strengthen the confidence of citizens, or of companies collaborating with them, in the security of IT and data management process. The desire for security to be integrated throughout their business process rather than be a separate process is another key factor. In the specific case of health area, some countries remark the requirement of certification of the involved ISMS.

Regarding the time period needed to prepare the company for certification, it is really variable, ranging from 3 to 18 months for private companies and up to 2 years in the case of public organizations. Most companies take between 6 and 12 months. Basically having previous experience in certification speeds up the process since some controls and mechanisms are already implemented, and the staff is familiar to this kind of process. When it comes to a follow-up, this time necessarily diminishes.

The period required for the actual certification process is, on average, a week for private sector and two weeks for public one. Sometimes, this process is split in two stages: the first to review the documented ISMS against the standard and the second to review the implementation of the ISMS within the business and evidence of adherence. Anyway, the size of the organization and the scope of the audit are an important factor to determine this duration. The certificates are usually granted for a three-year period, during which certified bodies need to be annually audited to ensure ongoing compliance with the standards. The certificate can be revoked if the annual audit finds reasons for it.

As for the cost of certification, it does not usually exceed the amount of 10000 €, which is considered in general terms good value for money, in the light of the benefits got from it.

Both public and private sector agree on the positive benefits brought by certification, highlighting that certification ensures a regular and systematic identification of risks to information security, and the evaluation and reduction of such risks to an acceptable and feasible degree by means of suitable security measures. Certification permits to audit annually the organization´s good practices, which requires continuous assessment with the aid of numerous system and process audits and leads to improvements of the implemented system and thus improvements to the organization of work. Thanks to the calculation of security indicators reflecting the efficiency of the system, continuous adjustment and further evolution in line with changing requirements can be achieved. The certification allows the management of information in a much more rigorous way than before. The certification also ensures sustainable security and safety. Finally, the certification introduces policy access rights to information systems and management of security incidents and vulnerabilities to the surveyed organization [4].

The benefits could be even higher if there were reliable statistics on the number of certificates and certified companies. The bodies issuing certificates are encouraged to keep updated records on certificates that they have issued, on the specific version of products/systems they certified, including information on the validity of the certificates.

Regarding the kind of profiles in charge of running the certification process and eventually authorizing the issuing of the certificates, these change from one organization to another. As an example, in the list below, the requirement an approving assessor must fulfill are enumerated:

- They must demonstrate knowledge of the Cloud Sector
    - Either through verifiable industry experience – this can include though assessing organizations
    - Or through completing CCSK [10] certification or equivalent
- They must be a qualified auditor working a ISO 27006 accredited CB
    - Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.
- They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification (This course will be carried out by BSI – British Standards Institute)

2.2. Justifying the need of certification

Despite the growing popularity and technical advances of cloud-based services, there still exists a confidence gap between the potential stakeholders when it comes to cloud adoption. While operating and finance personnel are generally excited about cloud because of the variety of powerful services and cost savings available, IT still has its reservations, largely related to perceptions of cloud security. For IT departments, the use of cloud can mean a loss of control, increased risk of intrusion or data loss and an aggressive shift in strategy. Also, should any security or privacy problems arise; the responsibility likely will fall back on the individuals responsible for IT.

As presented in the study realized by Accenture and the London School of Economics and Political Science's Outsourcing Unit called "Cloud and the Future of Business; From Costs to Innovation" shows that IT still sees issues like security and privacy as a barrier to cloud adoption. The study suggests that data security and privacy together with off-shore data housing and security are perceived to be the most significant risks for cloud.

A lot of research has been done, and is still on going to mind this perception gap. Cloud-based security services is an emerging market with rapid growth. It is estimated to rise to $3.1 billion in 2015 and expected to hit $4.13 billion by 2017. Gartner forecasts that two of the top three most sought-after cloud services will be web security services and identity and access management (IAM).

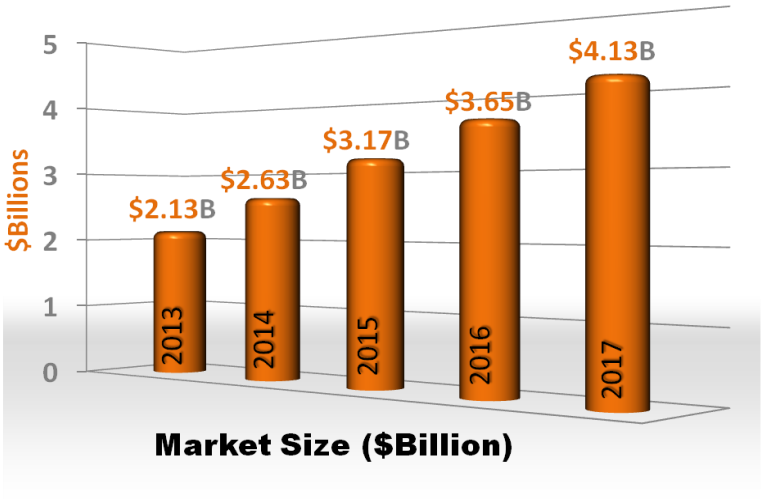

Figure 4. Cloud-Based Security Market Size Forecast (Source Gartner)

One of the reasons for this growth is the increasing adoption of Software as a Service (SaaS) applications and other cloud-based services that are encouraging organizations to adopt cloud-based security. Managed Security Services (MSS) are also driving adoption of cloud-based security services among enterprises. MSS delivery models are in turn being affected by demand for cloud-based security services, which is enabling security providers to become de facto MSS players.

Once decided the migration to cloud-based services, questions of security can make or break an IT department, which is why choosing the right provider is one of the most important decisions to make. In order to establish confidence that you will be working with a trusted cloud provider, Gartner suggest asking about security issues, such as, privileged user access, data location, data segregation or for instance, regulatory compliance. This last one is fully in line with the research done in CUMULUS since, takes into account the external audits or security certifications that the cloud provider has. So, definitely, to have these certifications can make a substantial difference towards market transformation.

Public cloud providers are not always able to provide the required transparency about the implemented policies, standards, and controls for truly trustworthy and interoperable cloud environments. Sometimes due to technological limitations, but often due to their reluctance to expose their operations. Furthermore, the market lacks independent and credible agents to examine and certify public cloud providers as suitable for the most sensitive information and applications. This lack of transparency and

reliable third-party verification is becoming an urgent issue as organizations seek to benefit from better economies of scale by moving processes and services to public clouds. Cloud provider cooperation and transparency inevitably improve with customer demands. For more restrictive services, cloud provider logs and attestations may not be enough. Organizations may ask for means for implementing tools that enable them to observe and measure cloud conditions and activities first-hand. Objective verification, not attestations, will ultimately emerge as the gold standard for ensuring trust in the public cloud.

Certification is considered as a valid answer to the lack of trust in the cloud. For instance, in the context of Trusted Cloud Europe4, certification comes strongly as a means to increase trust in the cloud. It is still unclear how this certification model should work, for instance the degree to which something is imposed or required and who requires it. What is aimed for EU level is to look at certifications and see what works best.

However, certification is not a panacea, since it costly process, particularly for SMEs, that in the end will have an impact on the cost of the cloud services. To this regard, the framework developed in CUMULUS project will help to automate a continuous certification framework that will help to reduce costs while providing a continuous assessment of the cloud services.

2.3. CUMULUS contribution from the point of view of the main stakeholders

2.3.1. The Cloud Certification Provider perspective

Most commercially available security certifications for the cloud are supported by well-established standards and best practices. As seen in ENISA's Cloud Computing Certification webpage5 (CCC), the underlying standards/best practices are developed by recognized standardization bodies (e.g., ISO/IEC in the case of 27001), or organizations (e.g., CSA for the Open Certification Framework). These will be referenced as "Cloud Certification Providers" (CCP) in the rest of this section. It is worth to notice that not always a CCP is the same entity that performs the security audit, and actually in many cases there is a clear separation among both activities. For example, in the case of CSA OCF the list of certified auditors can be found online6. Typically, the CCP will receive a payment (in the form of a royalty) depending on the number of audits performed based on its certification scheme.

The CUMULUS framework brings tangible business benefits for CCP's namely:

- Broaden their portfolio of certification schemes, by offering a "true" **continuous** certification solution. As discussed in Deliverable 7.6, a CUMULUS-based certification is something that customers are willing to pay for.
- Some CCP's sell training services in order to certify auditors on the offered scheme. The CUMULUS framework might allow CSP's to offer **training** services not only to auditors, but also to CSP's willing to integrate/deploy the CUMULUS contributed technology as part of their own services.
- CCP's might find a competitive advantage in offering new certification models suitable for complex cloud architectures. For example, cloud security certifications modeling the behavior of multi-cloud systems like supply chains or cloud federations. To the best of our knowledge, this is a gap at the state of the practice.
- Finally, the time-to-market associated with new CCP versions of existing certification schemes (e.g., adding/removing controls from the underlying standardized frameworks) will be reduced thanks to the systematic approach taken by CUMULUS. These "**incremental certifications**" are not offered by CCP's, just as observed from ENISA CCC.

[4] http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

[5] Please refer to https://resilience.enisa.europa.eu/cloud-computing-certification

[6] Please refer to https://cloudsecurityalliance.org/star/certification/#_auditors

2.3.2. The Cloud Auditor Perspective

A cloud auditor is a party that can perform an independent examination of cloud service controls (e.g., security, privacy, performance) with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through a review of objective evidence. A cloud auditor can evaluate the services provided by a CSP such as security controls, privacy impact, and performance. According to ISO/IEC 17789 [7], the audit activity involves:

1. request or obtain audit evidence;
2. conduct any required tests on the system being audited;
3. obtain evidence programmatically, through a set of interfaces provided by the system being audited;
4. redact the evidence, if necessary, in order to protect sensitive information or information subject to regulatory control (e.g., PII);
5. compare the obtained audit evidence against the audit criteria as described by the audit scheme or standard that is being used.

From the activities mentioned above, CUMULUS directly impacts 1 – 3 although in an indirect manner the technological contributions from CUMULUS also will reflect on 4 and 5. CUMULUS will benefit the cloud security audit function by providing the framework (techniques and tools) to automatically certify a selected set of security properties, directly from the target cloud service. Furthermore, as required by novel certification schemes like CSA Open Certification Framework (OCF7), CUMULUS will enable continuous certification. Overall, these aspects will have a direct effect on the following business aspects associated to the audit function:

- Savings through realistic levels of automation: our expectancy is that cloud auditors will save both time and economic resources thanks to the support provided by the framework/tools developed by CUMULUS. Ideally, most of the audit activity will have the potential of being automated without losing assurance guarantees, however we expect "realistic" levels of automation to be deployed by the involved parties. For example, some security properties will need still the human component in order to process evidence, like in the case of the physical security controls found on most of currently available certification schemes.
- **New business models based on the Security-as-a-Service paradigm**: a promising audit strategy is to obvert towards the creation of **tools and techniques to reason about the security properties**, as a basis to enable Security-as-a-Service. Such solutions can be offered by independent third parties (brokers/auditors), offering to the end users/regulators monitoring functionalities e.g., to be notified about certifications/SLA violations due to cyber incidents. Some FP7 projects, like SPECS, are building on this, and new H2020 projects starting in 2015 will continue to explore this field.

Intuitively, both incurred savings and development of new business models will result on economic benefits for cloud auditors, which in the short/mid-term should reflect on the rest of involved stakeholders who would increase notably their competitiveness (e.g., CSP being charged only by the audit services being consumed, and cyber-insurances lowering prices thanks to the continuous assurance achieved by CSP's).

2.3.3. The Cloud Provider Perspective

[7] Please refer to https://cloudsecurityalliance.org/star/

The increasing importance of cloud computing in the business world is forcing companies to adapt to this new paradigm. The likely loss of competitiveness they might suffer if not doing so is probably the most decisive factor leading them to make the decision. Nevertheless, regardless of this, security issues prevent the business from growing as it could be expected and desired. The demand of security is so high that any company is able to differentiate from competitors by offering such security. This would entail an important advantage.

In this sense, CUMULUS has several positive impacts:

- CUMULUS is somehow a way to encourage companies to implement new security measures. The catalogue of properties is quite appealing for any customer with high concerns of security. CUMULUS put providers on the way to accomplish these implementations.
- CUMULUS automates the evaluation of security and the certification of such security. On top of that, it provides continuous monitoring, a bit concern of the market, as it is shown in the results of questionnaire explained in D7.6.
- Such automation can decrease the number of hours devoted to auditing, and the price the company pays to the auditors.
- The reliability of CUMULUS as an appropriate certification environment could encourage insurance companies (those taking accountability in case of data breaches or the security being compromised) to lower their prices when offering their services. This has a double benefit: it makes the insurance company more competitive and reduces the expenses in this aspect the Cloud Service Provider has to face.
- CUMULUS will also increase cloud trust and transparency, supporting users and providers in their movement to the cloud

The flip side has to do with the adaptations the cloud infrastructure must face in order to be integrated with CUMULUS. Within this project, we have experience as for the number of hours that it takes to integrate CUMULUS in a couple of specific pilots. Nevertheless, as a result of internal analysis the conclusion says that it is not easily comparable to any kind of pilot. There will be a high uncertainty regarding the effort needed to adapt CUMULUS to a specific cloud infrastructure. This will have an impact in the balance sheet. Besides, as it is stated in D6.2, sometimes parts of the cloud need to be exposed in order to make possible to get evidences to produce the certificate. This is especially meaningful as for testing techniques, where hooks are usually needed. The companies must study this issue before accomplishing the integration of CUMULUS.

Another important risk has to do with the criteria used to consider that a certificate can be issued for a particular security property. These criteria might be considered rather subjective if there are no recognized standards on which the criteria are based. That is why it is necessary, as it is stated in D6.2, to study in depth those standards in order to place properly the metrics and criteria to issue the certificate. In the framework of the project, the criteria that will be studied are compiled in the protection profiles by the NSA. These protection profiles have been approved for use by vendors for evaluation of products under the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the Common Criteria Recognition Agreement (CCRA). Some protection profiles which are relevant for CUMULUS are those for IPSec VPN Clients [18], Enterprise Security Management Identity and Credential Management [19], and Certification Authorities [20]. These profiles, along with others, will be analyzed in order to develop the most rigorous and accurate metrics to decide whether or not issue the corresponding certificate.

2.3.4. The insurance companies and their accountability

Cloud insurance is an approach to risk management in which a promise of finantial compensation is made for specific potential failures on the part of a cloud computing service provider.

A cloud insurance policy protects the cloud provider who is held responsible for a service that was promised but not delivered as well as customers who believe they did not receive promised results. Cloud insurance may be provided as a part of a SLA with the provider or it may be purchased separately through a third-party insurance company. The introduction of liability insurance for Cloud Service Providers is a move towards offering higher levels of data assurance to end user clients.

Cloud insurance can offer compensation for several reasons, such as outages, unintentional data losses or security breaches, to name but a few. Another insurance service is that providing periodical backups, so that the information can never be definitely lost. In [21] a list of reasons to contract this kind of insurances can be checked.

CUMULUS can contribute to make insurance cheaper for cloud providers. If CUMULUS becomes a recognized and trusted tool able to certificate security and provide assurance, insurance companies could offer their protection for a cheaper price to any client counting on CUMULUS to take care of the security of their cloud assets.

Some companies, such as CGI Group8, Cloudinsure9 or MSPA Alliance10 members provide this kind of services.

2.4. Outlook and Next Steps

The following bullet points analyze the conclusions obtained from each of the evaluation criteria:

- Criterion 1: It has been properly applied to both Smart Cities and eHealth scenario. It can be also applied to any other scenario taking the needed care to analyze the scenario itself and the kind of security that can be certified on it.
- Criterion 2: The *protection profiles*, defined by the NSA, seem to be an appropriate set of criteria to define whether or not a security property is being fulfilled. These criteria will be studied in depth and applied to the validation for the rest of the project.
- Criterion 3: It has been properly applied to both scenarios, since the needed security mechanisms to make possible the certification of the corresponding security properties have been implemented, making possible such certification. It will continue to be applied for the rest of the project.
- Criterion 4: Regarding the costs of adaptation of the scenario to the framework, the only way to make some estimation is basing on previous experience, what is really difficult since there is not much in common among scenarios. Therefore such estimation in advance of costs, although could be done, would involve a big burden of uncertainty.
- Criterion 5: This criterion and the way to assess it are proposed on this deliverable.
- Criterion 6: Some references and figures have been provided showing the growing importance of the cloud market and the parallel market appearing with regard to cloud security. This is because security issues are the big threat to the success of the cloud as a new paradigm and as a business actually. CUMULUS is demonstrated to be fully aligned with the market demands and can really provide added value in terms of assurance.
- Criterion 7: A first approach to the analysis of the benefits of CUMULUS from the point of view of different providers has been given.

[8] https://www.cgi.com/en

[9] http://cloudinsure.com/

[10] http://mspalliance.com/

Besides, an overview about the current practices of certification, the way metaframeworks of certification operate and rate cloud services and infrastructures, and practical aspects about how public and private organizations undergo the process of certification and their reasons to do it have been provided within this section.

3. Evaluation of Certification Framework

In this Section we report full details about design, execution, and results of two validation sessions with external validators where the CUMULUS Certification Framework has been analyzed following the criteria defined in deliverable D6.2 [13]. The first validation session (Rome, January 13th 2015) has been already described in deliverable D6.5. That description is here reported for the reader convenience (Sections 3.1 and 3.2). Sections 3.3 and 3.4 contain new materials relative to the second validation session (Rome, July 2nd 2015). The descriptions given here are integrated by further materials (annexes) attached to this document.

3.1. Introduction

This section is envisaged to provide the first outcomes regarding the validation of the CUMULUS Framework following a set of concrete criteria, namely: usability, assurance, representation capability, cost effectiveness and security. In order to do this, a validation session, inspired to D6.2 criteria, was held in Rome on January 13rd 2015. In this section we report about design, execution and results of this session.

3.2. First Session with External Validators

3.2.1. Session Design and Execution

Introduction

The session was designed to be, as much as possible, consistent with the approach defined in [13]. Essentially, we involved external validators, who were requested to answer a questionnaire after being introduced to some aspects of CUMULUS project.

This first session was oriented to collect feedback about CUMULUS from security evaluation/certification experts (also called respondents), which is quite natural given the project objectives. We invited validators from Organismo di Certificazione della Sicurezza Informatica (OCSI) (Italian Body for ICT security certification according to the international standard ISO/IEC IS-15408 (or Common Criteria (CC) [15][16][17]) and from FUB. OCSI provided two official certifiers (unfortunately, one of them couldn't join the actual session) and FUB provided three experts of evaluation/certification (selected among people not involved in CUMULUS). In the following, the OCSI expert is denoted as R2 and the FUB experts are denoted as R1, R3 and R4.

Session Design

Based on both availability of validators and session objectives, we decided to have a four hours session to cover, at some extent, all the analyses considered for the CUMULUS framework in [13] (usability, representation capability, perceived security, assurance, cost effectiveness). Accordingly, we discussed both aspects to be presented and corresponding questions to be asked to the validators. Finally, we grouped the selected aspects along with the corresponding questions in four sections and structured the session accordingly.

SESSION SECTIONS

A brief description of the sections follows (some more details are given in table 5) (for a complete view, we refer to the session materials attached to this document):

- CUMULUS Framework (Section I): Introduction to both use cases and corresponding functional and security requirements as given in [23] (with suitable simplifications and

special focus on the certifier actor), with corresponding questions from Q-1 to Q-6 (see table 5) supporting the exploration of usability and perceived security (see below);

- CUMULUS Meta Model (Section II): Introduction to both structure and objectives as given in [24] (with suitable simplifications and special focus on how it attempts to capture the basic concepts of a general approach to certification), with corresponding questions from Q-7 to Q-13 (see table 5) supporting the exploration of usability, representation capability, and assurance (see below);
- CUMULUS Test Based Certification Model (Section III): Introduction to both structure and objectives as given in [24] (with suitable simplifications and special focus on how it attempts to capture the basic concepts of test execution in a generic certification process, with emphasis to Common Criteria processes), with corresponding questions from Q-14 to Q-20 (see table 5) supporting the exploration of usability, representation capability, and assurance (see below). Notice that questions from Q-14 to Q-20 are deliberately got, mutatis mutandis, from questions Q-7 to Q-13, respectively, right to validate the two levels of description provided by the Meta Model and by a Certification Model;
- CUMULUS Framework Adoption (Section IV): Introduction to cost and benefit estimation (based on key factors and corresponding raw cost and benefit estimation focusing on the possible adoption of the CUMULUS Framework in the Common Criteria context), with corresponding questions from Q-21 to Q-24 (see table 5) supporting the exploration of cost effectiveness.
- CUMULUS Monitoring Based Certification Model (Section V): Introduction to both structure and objectives of the monitoring based certification model, with the main focus on how it attempts to capture the basic concepts of the monitoring process and the definition of the different kind of conditions that need to be checked in the certification process.

QUESTIONNAIRE DESIGN

Table 5 provides the list of the questions selected as to be proposed to the validators, along with the corresponding possible answers and the contributed dimension explorations.

We considered only closed-answer questions of two possible types: questions with Yes/No answer (with request for written explanation conditioned on the provided answer) and questions with five level scale answer (Excellent, Good, Neutral, Poor, Very Poor). We decided to provide free text room for each question with five level scale answer so to gather as much feedback as possible from the validators. Moreover, we decided to provide free text room both for each session section and for the overall session so to allow the validators to report any extra relevant comment. The questionnaire was designed so to suitably instruct the validators about their role (for a complete view, we refer to the session materials attached to this document).

EXPLORED DIMENSIONS

It is important to notice that, due to some constraints, we needed to restrict the validation session as to investigate the CUMULUS framework just at a conceptual level. A first constraint was the actual availability of validators, leading to arrange only one validation session, only in the period between the end of 2014 and the beginning of 2015, and taking only half a day. A second constraint was the internal objective to try to contribute as much as possible all the analyses considered in [13]. The third constraint (related to the second one) was the need to introduce in a suitable way a number of concepts related to CUMULUS work. The given constraints suggested both to avoid showing a framework in action and to stay on concepts (many ones, in fact), though suitably presented. The main effects on the session design were:

- Presenting the CUMULUS Framework based just on use cases and corresponding functional and security requirements (as described in [23]);
- Presenting a simplified version of the CUMULUS Meta Model (as described in [24]);

- Presenting a simplified version of the CUMULUS Test Based Certification Model (as described in [24]) with no concrete example instances.
- Presenting a simplified version of the CUMULUS Monitoring Based Certification Model (as described in [24]).

All this produced also:

- A partial satisfaction of the general evaluation criteria (common across all dimensions) given in [13], since we couldn't actually introduce any contextualization to pilot scenarios;
- The need of suitably adapting to the session context the analyses considered in [13] (see the relevant remarks given below).

USABILITY ANALYSIS REMARKS

The designed validation session contributes, though in a non standard way, the usability analysis defined in [13] by covering the aspects of technical quality [13] of CUMULUS Framework functionalities—as foreseen at requirement levels [23]—and (user) satisfaction [13] about CUMULUS Meta Model and Test Based Certification Model.

As for the technical quality aspect, based on functionalities foreseen at requirement levels, the session enables to:

- Explore both sufficiency [13] and necessity [13] of the reference functionalities (CUMULUS Framework Section, questions Q-1 and Q-2, respectively);
- Gather from the validators a relevant overall rating (through the concept of *completeness*) of the reference functionalities (CUMULUS Framework Section, question Q-3).

As for the (user) satisfaction aspect, the session enables to:

- Gather from the validators a relevant overall rating (through the concept of *easiness of comprehension*) of the reference models (CUMULUS Meta Model Section, question Q-7, CUMULUS Test Based Certification Model Section, question Q-14, and CUMULUS Monitoring Based Certification Model Section Q1).

The main point here is that the analyses enabled by the designed session, even being significant, use only a *conceptual* validation platform (see [13]) and this produces a partial satisfaction of the specific criteria given in [13].

REPRESENTATION CAPABILITY ANALYSIS REMARKS

The designed validation session contributes the representation capability analysis defined in [13], since it enables to:

- Explore the ability of the CUMULUS Meta Model to capture the significant aspects of both a generic and a Common Criteria security certification process (CUMULUS Meta Model Section, questions Q-8 (generic process), Q-10 (generic process), and Q-11 (testing in Common Criteria));
- Explore the ability of the CUMULUS Test Based Certification Model to capture the significant aspects of both a generic test based and a Common Criteria security certification (CUMULUS Test Based Section, questions Q-15 (generic process), Q-17 (generic process), and Q-18 (testing in Common Criteria));
- Explore the ability of the CUMULUS Monitoring Based Certification Model to capture the significant aspects of the monitoring based certification process (CUMULUS Monitoring Based Certification Model Section Q2-5);
- Gather from the validators an overall rating of the ability of the CUMULUS Meta Model and Test Based Certification MODEL and Monitoring Based Certification Model to capture the significant aspects of security certification of cloud services (CUMULUS Meta Model and Test Based

Certification Model Sections, questions Q-9 and Q-16, respectively, and Monitoring Based Certification Model Section Q6);

There are no particular remarks for this analysis.

PERCEIVED SECURITY ANALYSIS REMARKS

The designed validation session contributes the perceived security analysis defined in [13], since it enables to:

- Explore the completeness of the security functionalities foreseen at requirements level for the CUMULUS Framework (CUMULUS Framework Section, questions Q-4 and Q-5);
- Gather from the validators an overall rating of the security level that stems out from the CUMULUS Framework security requirements (CUMULUS Framework Section, question Q-6).

Also the perceived security analysis enabled by the designed session, even being significant, uses only a *conceptual* validation platform (see [13]) and this produces a partial satisfaction of the specific criteria given in [13].

ASSURANCE ANALYSIS REMARKS

The designed validation session contributes the assurance analysis defined in [13], since it enables to:

- Analyze if the current definitions of the CUMULUS Meta Model and Test Based Certification Model could affect negatively the assurance of the certification processes described according to them (CUMULUS Meta Model Section, questions Q-12; CUMULUS Test Based Certification Model Section, questions Q-19);
- Gather from the validators positions about if/how introduce in the CUMULUS Meta Model and Test Based Certification Model any component/rule explicitly related to the assurance of the certification processes described according to them (CUMULUS Meta Model Section, questions Q-13; CUMULUS Test Based Certification Model Section, questions Q-20).

The main point here is that the assurance analysis enabled by the designed session, even being significant, uses only the CUMULUS Meta Model and the CUMULUS Test Based Certification Model (to collect possible requirements for their refinement) and this produces a partial satisfaction of the specific criteria given in [13].

COST EFFECTIVENESS ANALYSIS REMARKS

The designed validation session, as with other dimensions considered, focuses on a conceptual level but it covers all the specific criteria given in [13].

The presentation includes a list of key factors apparently relevant for a cost effectiveness analysis of the adoption of the CUMULUS Framework within a security certification process. For these key factors, a raw estimation for the specific case of the Common Criteria certification process is also included. Table 4 reports a synthesis of the considered key factors along with the corresponding raw estimation (for a complete view, we refer to the session materials attached to this document).

Key cost factor	Raw estimation for Common Criteria
Identification of the certification process steps to be automated	LOW

Certification Model definition and CUMULUS Framework integration	HIGH
Training	LOW
Key benefit factor	
Increase in speed	MEDIUM
Increase in uniformity	MEDIUM
Increase in repeatability	HIGH
Reuse of defined Certification Model	MEDIUM

Table 4. Synthesis of the cost effectiveness analysis presented to the session with external validators

The session contributes the cost effectiveness analysis in [13], since it enables to:

- Gather a feedback from the validators regarding the completeness of the aspects considered as costs and benefits factors for cost effectiveness analysis (CUMULUS Framework Adoption Section, question Q-21);
- Gather the validators opinion about the accuracy of the raw estimation on costs and benefits of the adoption of the CUMULUS Framework in a Common Criteria certification process (CUMULUS Framework Adoption Section, questions Q-22 and Q-23);
- Obtain an overall rating of the cost effectiveness of the CUMULUS Framework adopted in a Common Criteria certification process (CUMULUS Framework Adoption Section, question Q-24).

#	Text	Possible Answers	Explored Dimensions	Reference Section
Q-1	Are the functionalities foreseen in the CUMULUS Framework sufficient? If not, please explain.	Yes No	Usability	CUMULUS Framework (I)
Q-2	Are the functionalities foreseen in the CUMULUS Framework all necessary? If not, please explain.	Yes No	Usability	CUMULUS Framework (I)
Q-3	How would you rate the completeness of an actual CUMULUS Framework implementing the foreseen functionalities?	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Framework (I)
Q-4	Are the security functionalities foreseen in the CUMULUS Framework sufficient? If not, please explain.	Yes No	Perceived Security	CUMULUS Framework (I)
Q-5	Are the security functionalities foreseen in the CUMULUS Framework all necessary? If not, please explain.	Yes No	Perceived Security	CUMULUS Framework (I)
Q-6	How would you rate the level of security of an actual CUMULUS Framework implementing the foreseen security functionalities?	Excellent Good Neutral Poor Very Poor	Perceived Security	CUMULUS Framework (I)
Q-7	How do you rate the easiness of comprehension of the CUMULUS Meta-	Excellent Good	Usability	CUMULUS Meta Model (II)

	Model?	Neutral Poor Very Poor		
Q-8	Is the CUMULUS Meta-Model adequate to represent the key aspects of security certification? If no, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-9	How do you rate the CUMULUS Meta-Model completeness in capturing the key aspects of security certification of cloud services?	Excellent Good Neutral Poor Very Poor	Representation Capability	CUMULUS Meta Model (II)
Q-10	Does the CUMULUS Meta-Model need to be reduced/extended/refined? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-11	Does the CUMULUS Meta-Model miss any key aspect of test activities occurring in CC approach to security certification? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-12	Does the CUMULUS Meta-Model limit, in any way, the assurance that can be obtained by certification processes specified according to it? If yes, please, specify.	Yes No	Assurance	CUMULUS Meta Model (II)
Q-13	Should the CUMULUS Meta-Model include an explicit coverage of the concept of assurance? If yes, please, provide possible reasons for that.	Yes No	Assurance	CUMULUS Meta Model (II)
Q-14	How do you rate the easiness of comprehension of the CUMULUS Test Based Certification Model?	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Test Based Certification Model (III)
Q-15	Is the CUMULUS Test Based Certification Model adequate to represent the key aspects of security certification? If no, please, specify.	Yes No	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-16	How do you rate the CUMULUS Test Based Certification Model completeness in capturing the key aspects of security certification of cloud services?	Excellent Good Neutral Poor Very Poor	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-17	Does the CUMULUS Test Based Certification Model need to be reduced/extended/refined? If yes, please, specify.	Yes No	Representation capability	CUMULUS Test Based Certification Model (III)
Q-18	Does the CUMULUS Test Based Certification Model miss any key aspect of test activities occurring in CC approach to security certification? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-19	Does the CUMULUS Test Based Certification Model limit, in any way, the assurance that can be obtained by test based certification processes specified according to it? If yes, please, specify.	Yes No	Assurance	CUMULUS Test Based Certification Model (III)
Q-20	Should the CUMULUS Test Based Certification Model include an explicit coverage of the concept of assurance? If yes, please, provide possible reasons for that.	Yes No	Assurance	CUMULUS Test Based Certification Model (III)
Q-21	Does the costs/benefits analysis miss any key aspects? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q-22	Does the costs/benefits estimation underrate any key factors? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)

Q-23	Does the costs/benefits estimation overrate any key factors? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q-24	How would you rate the benefit of an actual CUMULUS Framework capable to automate the execution of tests in a CC certification process?	Excellent Good Neutral Poor Very Poor	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q1	Do you think that CUMULUS Monitoring Based Certification Models (MBCMs) are capable of representing comprehensively continuous security certification processes for cloud services security?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Usability	CUMULUS Monitoring Based Certification Model (V)
Q2	Do you think that the assertion rules specified as part of a CUMULUS Monitoring Based Certification Model are capable of representing accurately and effectively the continuous collection of evidence required for the assessment of security properties and/or the effectiveness of control mechanisms realising these properties in the cloud?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q3	Do you think that the life cycle models specified as part of a CUMULUS Monitoring Based Certification Model are capable of representing effectively the processes of collecting evidence, and generating and managing certificates based on it?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q4	Do you think that the evidence sufficiency conditions that may be specified as part of a CUMULUS Monitoring Based Certification Model (number of events, period of monitoring, expected behaviour of target of certification) are capable of representing effectively the circumstances under which the evidence collected would be enough to make a decision about issuing a certificate or otherwise?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can	Representation Capability	CUMULUS Monitoring Based Certification Model (V)

		think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of		
Q5	Which of the following parts of CUMULUS Monitoring Based Certification Models, do you think that it would be difficult for someone with expertise in cloud security to specify even after training?	None Assertions expressing the collection of evidence for security properties/anomalies Evidence sufficiency conditions Life cycle models	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q6	Are there any key elements/requirements that continuous security certification processes for cloud services should address but CUMULUS Monitoring Based Certification Models fail to cover?	Yes No	Representation Capability	CUMULUS Monitoring Based Certification Model (V)

Table 5. Questions proposed for the session with external validators

RECOMMENDATIONS FOR FUTURE SESSIONS

Based on the remarks given before, possible future validation sessions involving security evaluation/certification experts could be extended so to:

- Use more concrete validation platforms
  - Involve architecture design and/or component implementation;
- Consider a more significant coverage of the relevant dimensions
  - For usability analysis, possibly include also efficiency and learnability aspects [13];
  - For assurance analysis, possibly include also instances of Certification Models;
- Cover advanced concepts of CUMULUS Framework
  - Exploit knowledge acquired by validators already involved.

SESSION EXECUTION

The session started with a presentation of the session structure and objectives, followed by an introduction to the relevant aspects of CUMULUS. Then, according to the planned duration, each section was executed, taking about 15 to 30 minutes for slide presentation and about 15 minutes for questionnaire answering. Further details were given to meet requests from validators (to clarify presented concepts and/or proposed questions). Where needed, the validators were requested to clarify their answers to the questionnaire.

3.2.2. Session Results

INTRODUCTION

This section reports an analysis of the results of the validation sessions with external validators. Consistently with [13], given the session context, a quantitative analysis is not so significant, so the analysis follows a qualitative approach, where the main objective is to extract from the validator

feedback (filled questionnaires) as many as possible recommendations and suggestions to guide the next CUMULUS activities.

Accordingly, both answers and comments from the validators are first discussed question by question. The more relevant suggestions and recommendations emerged from the discussion are then summarized at the end of the section.

Validation results

Table 6 provides the raw answers of the validators to the questions proposed to them, while in the next subsections the answers to each question are discussed in detail along with the relevant comments provided by the validators (for a complete view of the feedback from validators, we refer to the session materials attached to this document).

#	R1	R2	R3	R4
Q-1	Yes	Yes	No*	Yes*
Q-2	Yes	Yes	Yes	Yes
Q-3	Neutral*	Excellent	Excellent	Good
Q-4	Yes	Yes	No*	Yes
Q-5	Yes	Yes	Yes	Yes
Q-6	Neutral	Good	Good	Excellent
Q-7	Neutral*	Good	Neutral*	Neutral*
Q-8	Yes	Yes	Yes	N/A
Q-9	Neutral*	Neutral*	Good	N/A*
Q-10	No	No	No	No*
Q-11	No	No	Yes*	No
Q-12	No	No	No	No
Q-13	N/A*	No*	Yes*	*Yes
Q-14	Good*	Good	Neutral*	Excellent
Q-15	Yes	Yes	Yes	Yes
Q-16	Neutral*	Neutral*	Good	Excellent
Q-17	N/A*	No	Yes*	No
Q-18	Yes	No	No	No
Q-19	No	No	No	No*
Q-20	No	No	Yes*	No
Q-21	Yes*	No	Yes*	No
Q-22	No	No	No	No
Q-23	No	No	No	No
Q-24	Neutral*	Good	Poor	Poor
Q1	>90%	>90%	>90%	>90%
Q2	N/A*	>90%	>90%	>90%
Q3	>90%	>90%	>90%	>90%
Q4	N/A*	>90%	>90%	50-74%
Q5	Assertions	None	Assertions	Evidence Sufficiency Conditions
Q6	Yes*	No*	Yes*	No*

Table 6. Raw results of the responders to the questionnaire.

Answers enriched by significant comments (see below) are asterisked (the reader can retrieve all validators´comments by checking the annexes attached to this deliverable).

Usability analysis

CUMULUS FRAMEWORK SECTION

Questions Q-1, Q-2 and Q-3 referred to the CUMULUS Framework section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 5) through analyzing the technical quality of the CUMULUS Framework foreseen functionalities.

The feedback from the validators was fully positive (once the comments from the validators have been analyzed (see below) and can be summarized as follows:

- All the respondents with one exception (R3) agreed that the functionalities foreseen in the CUMULUS Framework are sufficient (see raw answers to Q-1 in table 6);
- All the respondents agreed that the functionalities foreseen in the CUMULUS Framework are all necessary (see raw answers to Q-2 in table 6);
- All the respondents with one exception (R1) rated Excellent or Good the completeness of an actual CUMULUS Framework implementing the foreseen functionalities (R1 rated such completeness Neutral) (see raw answers to Q-3 in table 6).

The answers that seemed to be critical were especially analyzed, looking at the motivations provided by the validators and directly interacting with them. It turned out that such answers finally do not affect the technical quality of the CUMULUS Framework foreseen functionalities, for the following reasons:

- R3 motivated the negative answer to Q-1 by explaining that an integrity check for the evidence collected from the cloud system could be useful. Anyway, such integrity check is already considered in the requirements for CUMULUS Framework, although implicitly. This point, which was not highlighted during the session due to the limited time available for the presentation, can be detailed as follows:
    - The CUMULUS Framework is foreseen to provide for the evidence collection session the security protections that are specified in the corresponding certification configuration (Requirement 6019.SEC of [23]). These security protections (motivated by possible attacks to the connection between CUMULUS Framework and a Cloud System) may include protection of integrity of the evidence since it has been collected in the Cloud System. Once acquired, the collected evidence is part of an evidence collection trace that is stored by the CUMULUS Framework (Requirement 3015.FUN of [23]). The CUMULUS Framework is foreseen to maintain the integrity of each evidence collection trace (Requirement 6020.SEC of [23]);
- R1 interpreted completeness in Q-3 as not limited to the objectives of the CUMULUS Framework (and especially to the automatic execution of a CUMULUS certification process), but extended to a generic certification process that is partially delegated to the CUMULUS Framework by a human certifier. Based on this, R1 motivated the Neutral rating in the answer to Q-3 by commenting that such a completeness depends on how much of a generic certification process can be actually delegated to the CUMULUS Framework by a human certifier.

The overall positive feedback received should just be completed with a general recommendation to not underrate the needs of the human certifiers that will use the CUMULUS Framework. This concern was especially felt by R4, as detailed below:

- In a comment to Q-1, though giving a positive answer, R4 anyway pointed out that a certifier would like to have documentation on the available services, on how to use those services and on inputs to be provided to the interfaces;
- In an extra comment to the CUMULUS Framework section, R4 stressed that a certifier expects help from the CUMULUS Framework, and not extra work to be done.

CUMULUS META MODEL SECTION

Question Q-7 referred to the CUMULUS Meta Model section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 5) through (user) satisfaction about CUMULUS Meta Model.

At a first sight the feedback from the validators seemed to be critical, since only R2 rated Good easiness the of comprehension of the CUMULUS Meta Model that was instead rated Neutral by all the other respondents (see raw answers to Q-7 in table 6). Anyway, the impact of these prevailing Neutral answers has been reduced by looking at the motivations provided by the validators and directly interacting with them. After such analysis, it turned out that only one of the respondents who gave Neutral ratings (R4) actually raised doubts on the overall comprehension of the CUMULUS Meta Model, and this position was motivated with the difficulty to find a parallel with the usual Common Criteria evaluation work done by R4. On the other hand, the Neutral ratings by R1 and R3 were based on single specific aspects that do not actually affect the (user) satisfaction about CUMULUS Meta Model. These were, respectively:

- For R1, the overlapping between the type of Evidence and the type of Certification Model;
- For R3, the lack of uniformity with the vocabulary used by security standards as the Common Criteria.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Question Q-14 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 6) through (user) satisfaction about CUMULUS Test Based Certification Model.

The feedback from the validators was essentially positive, since all the respondents with one exception (R3) rated Excellent or Good the easiness of comprehension of the CUMULUS test based Certification Model (see raw answers to Q-14 in table 6). R1 especially pointed out that all is relatively clear, except what the element ToC (Target of Certification [24]) exactly specifies. Only one respondent (R3) gave a Neutral answer, which anyway was motivated by the fact that R3 did not deem himself as an expert in model description and not by negative considerations on the CUMULUS Test Based Certification Model.

CUMULUS MONITORING BASED CERTIFICATION MODEL SECTION

Questions Q1 refer to the CUMULUS Monitoring Based Certification Model section and aimed to support usability analysis and user satisfaction about CUMULUS Monitoring Based Certification Model.

The overall feedback from the validators was essentially positive, however they stated that there were some of the elements difficult and a bit complex to understand in order to define some elements.

Assurance analysis

CUMULUS META MODEL SECTION

Questions Q-12 and Q-13 referred to the CUMULUS Meta Model section and, as explained in Section 3.2.1, aimed at supporting assurance analysis (see table 5).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS Meta Model does not limit in any way the assurance that can be obtained by certification processes specified according to it (see raw answers to Q-12 in table 5);
- Actually all the respondents with one exception (R3) did not agree that the CUMULUS Meta Model should include an explicit coverage of the concept of assurance (see raw answers to Q-13 in table 5 plus the observations below).

As for Q-12, all the positive answers were basically motivated by the very high level of the description provided by the Meta Model.

When answering to Q-13, two respondents (R3 and R4) seemingly agreed that the CUMULUS Meta Model should include an explicit coverage of the concept of assurance but only R3 actually agreed and motivated this with the need for comparison of certified products. A direct interaction with the respondent clarified that R4 actually did not agree. In fact R4 explained in a comment to Q-13 that nothing more can be done at the Meta Model level, since the relevant values to determine assurance are set at the Certification Model level. Also R2 did not agree and explained in a comment to Q-13 that an explicit coverage of assurance by the Meta Model is not necessary, provided that the actual Certification Models cover in some way the concept. Finally, R1 did not answer, but actually did not agree. In fact, in a comment to Q-13, R1 assumed that the assurance concept is somehow included in the element Security Property and explained that, under this assumption, there is no need of an explicit coverage of assurance in the Meta Model.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Questions Q-19 and Q-20 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting assurance analysis (see table 5).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS Test Based Certification Model does not limit in any way the assurance that can be obtained by certification processes specified according to it (see raw answers to Q-19 in table 5);
- Actually all the respondents with one exception (R3) did not agree that the CUMULUS Test Based Certification Model should include an explicit coverage of the concept of assurance (see raw answers to Q-20 in table 5).

As for Q-19, R4 just pointed out in a comment that the assurance is probably limited only by how the CM is instantiated.

As for Q-20, all the respondents that answered No pointed out in their comments that the provided assurance may be somehow derived from the contents of the Certification Model. On the other hand, R3 justified his Yes answer as that to Q-13, with the fact that an explicit coverage of assurance is needed for comparison of certified products.

Representation capability analysis

CUMULUS META MODEL SECTION

Questions Q-8, Q-9, Q-10 and Q-11 referred to the CUMULUS Meta Model section and, as explained in Section 3.2.1, aimed at supporting representation capability analysis (see table 5).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents except one (R4) agreed that the CUMULUS Meta Model is adequate to represent the key aspects of security certification (see raw answers to Q-8 in table 5);
- Only one of the respondents (R3) rated Good the CUMULUS Meta Model completeness in capturing the key aspects of security certification of cloud services. Two other respondents (R1 and R2) rated it Neutral and R4 did not answer (see raw answers to Q-9 in table 5);
- All the respondents agreed that the CUMULUS Meta Model does not need to be reduced/extended/refined (see raw answers to Q-10 in table 5);
- All the respondents except one (R3) agreed that the CUMULUS Meta-Model does not miss any key aspect of test activities occurring in CC approach to security certification (see raw answers to Q-11 in table 5).

The answers that seemed to be critical were especially analyzed (especially those to Q-9), looking at the motivations provided by the validators and directly interacting with them. It turned out that such answers do not substantially affect the representation capability of the CUMULUS Meta Model, based on the observations that follow.

As for Q-8, R4 did not answer and pointed out in a comment that it is not clear how the Meta Model could represent actual evaluation activities.

As for Q-9, the impact of the Neutral ratings is reduced by the motivations provided for them. In fact, in their comments to Q-9, R1 motivated the rating with a single specific aspect (to R1, it all depends on how the element ToC [24] is defined) and R2 by an alleged poor knowledge of cloud systems security. Finally R4 did not answer, but in direct interaction explained to have several doubts on the concept of Meta Model itself (this is consistent with other answers by R4 to questions about the Meta Model, e.g., Q-8).

In a comment to Q-10, R4 pointed out that the Meta Model could just be made easier to understand (this is consistent with other answers by R4 to questions about the Meta Model: see, e.g., Q-7). Moreover, in an extra comment to the CUMULUS Meta Model section, R3 suggested that the addition of extra information that permits composition of ToCs [24] may simplify the certification of complex ToCs.

In the comments to Q-11, the No answers were all basically motivated by the very high level of the description provided by the Meta Model; on the other hand, R3 motivated his Yes answer by specifying that in the Meta Model the strength of security functions is missing. Anyway, since the strength of security functions is a possible metrics for penetration tests, it may be covered within the CUMULUS Test Based Certification Mode, especially by the element Test Metrics.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Questions Q-15, Q-16, Q-17 and Q-18 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting representation capability analysis (see table 5).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS test based Certification Model is adequate to represent the key aspects of security certification (see raw answers to Q-15 in table 5);
- Half of the respondents rated Excellent or Good the CUMULUS test based Certification Model completeness in capturing the key aspects of security certification of cloud services, whereas the other half rated it Neutral (see raw answers to Q-16 in table 5);
- Half of the respondents agreed that the CUMULUS test based Certification Model does not need to be reduced/extended/refined (see raw answers to Q-17 in table 5);
- All the respondents except one (seemingly R1, but actually R3 (see observations below)) agreed that the CUMULUS Meta-Model does not miss any key aspect of test activities occurring in CC approach to security certification (see raw answers to Q-18 in table 5).

The answers to Q-16, Q-17 and Q-18 that seemed to be critical were especially analyzed, looking at the motivations provided by the validators and directly interacting with them. It turned out that such

answers do not substantially affect the representation capability of the CUMULUS Test Based Certification Model, based on the observations that follow.

In the comments to Q-16, the respondents who gave Neutral ratings (R1 and R2) gave motivations that reduce the impact of such rating. In fact, R1 motivated her answer with the fact that it is difficult to "force" significant specifications without limiting the possible cases, but also noted that this problem is common to any model, whereas R2 motivated her answer by an alleged poor knowledge of cloud systems security.

As for Q-17, R1 did not take a position, giving in a comment essentially the motivation that the time provided was not sufficient to give a satisfactory answer. Finally, only one respondent (R3) answered Yes and, recalling their comment to the CUMULUS Meta Model section, specified that the CUMULUS Test Based Certification Model could be refined by adding some information to permit the composition of ToCs [24], thus simplifying the certification of complex ToCs.

As for Q-18, all the respondents except (seemingly) R1 answered No. Anyway, direct interaction with the respondents clarified that R1 answered Yes by mistake, whereas R2 answered No but actually thought that some aspect was missing. In fact, in a comment to Q-18, R2 pointed out that the CUMULUS Test Based Certification Model does not seem to cover aspects as test coverage and depth. As for this comment, it may be noted that the CUMULUS Test Based Certification Model does not explicitly address these aspects, but nevertheless provides a way to specify them (as much as they can be adapted to the context of cloud services) through the element Test Metrics.

CUMULUS MONITORING BASED CERTIFICATION MODEL SECTION

Questions Q2-6 referred to the CUMULUS Monitoring Based Certification Model section and aimed at supporting representation capability analysis (see table 5).

The overall feedback from the validators was that the Monitoring Based Certification Model is able to represent the key aspects of the monitoring based certification process. However, there were some comments whether the monitor can detect any changes that might occur in a service that is being monitored and certified, in order to adapt the certification process according to them. This comments lead to the necessity of having the incremental certification process, which will be covered in the CUMULUS project. Finally, some certifiers also proposed to combine the monitoring-based certification process with a test-based process, to check that no changes have occurred in the service that is being certified, which leads to the necessity for a hybrid certification process.

Perceived security analysis

CUMULUS FRAMEWORK SECTION

Questions Q-4, Q-5 and Q-6 referred to the CUMULUS Framework section and, as explained in Section 3.2.1 , aimed at supporting perceived security analysis (see table 5).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents except one (R3) agreed that the security functionalities foreseen in the CUMULUS Framework are sufficient (see raw answers to Q-4 in table 5);
- All the respondents agreed that the security functionalities foreseen in the CUMULUS Framework are all necessary (see raw answers to Q-5 in table 5);
- All the respondents with one exception (R1) rated Excellent or Good the level of security of an actual CUMULUS Framework implementing the foreseen security functionalities (R1 rated such completeness Neutral) (see raw answers to Q-6 in table 5).

As for Q-4, R3 motivated the negative answer in a comment by pointing out that an integrity check for evidence provided by the cloud system could be useful. This motivation is the same given by R3 for his answer to Q-1 and has been discussed when reporting the answers to Q-1.

As for Q-5, R3 in a comment just raised some doubts about the scope and the purpose of non-repudiation and on its meaning from the point of view of the cloud system owner. Actually, the CUMULUS Framework is foreseen to assure the non-repudiation of Certification Results (Requirement 6014.SEC of [23]). The purpose is to provide support to resolution of disputes about the fact that a given certification result has been originated in the CUMULUS Framework. Therefore, from the point view of the cloud system owner, non repudiation is a protection in possible disputes with a Certifier that uses the CUMULUS Framework.

As for Q-6, R4 in a comment pointed out that security requirements should be transparent for the certifier, to avoid complicating the work to be done. Finally, R1 motivated their Neutral answer with the comment that it is impossible to answer if an actual implementation is not available. These answers seem to notify that the overall security level perceived by the validators for the considered conceptual Framework level is good, and to suggest to extend the analysis to a more concrete Framework.

It is relevant for perceived security also the extra comment of R3 to the CUMULUS Framework section, noting that the separation of privileges between Administrator and Auditor may relax the assumptions to be done about the Administrator, which in this way would be controlled at some extent by the Auditor. Even if this sounds as a good suggestion, since it is not about one of the main objectives of the project it seems that a possible revision of the requirements and assumptions would be not necessary in this case.

Cost effectiveness analysis

CUMULUS FRAMEWORK ADOPTION SECTION

Questions Q-21, Q-22, Q-23 and Q-24 referred to the CUMULUS Framework adoption section and, as explained in Section 3.2.1, aimed at supporting cost effectiveness analysis (see table 5).

When answering to Q-21 two of the respondents indicated that the analysis could miss a key factor. R1 identified this missing factor as the "cost of preparing automation tools/framework" but recognizing that it could be included (as it actually is) in the cost of preparing appropriate CMs and integrating the CUMULUS Framework in a given certification process. R3, on the other hand, underlined that CUMULUS view does not explicitly consider a distinction between the evaluation and the certification process, which is a basic distinction in a Common Criteria certification process. R3 highlighted that the CUMULUS Framework best fit into the CC evaluation process, but should consider as a key cost factor the interaction between the Certification Body and the Evaluation Facility. After a direct interaction with the respondent he recognized that the missing cost was indeed present in the factor taking into account the definition of CMs and the integration of these in the CUMULUS Framework. To better clarify the importance of the aspects considered, R3 suggested, for a possible future estimation (that could be done for example for a second validation session), to split the relevant key factor and to estimate separately the cost of defining CMs and the cost of integrating them in a certification process.

When answering to Q-22 and Q-23 all the respondents agreed that the raw estimation provided in the presentation rated in a correct way (neither underrated nor overrated) all the identified key factors. These positive answers confirm the results of the raw estimation: even if an important factor to be considered is the cost of generating new CMs, this cost could be in a long-term phase mitigated by the reuse of other CMs already generated and moreover other benefits factors like the increase in speed, uniformity and repeatability of certification results would have an important impact in overall cost effectiveness of adopting the CUMULUS Framework.

When answering to Q-24, two of the respondents rated as good the benefit coming from the automation of a part of the CC certification process that could be provided by a tool like the CUMULUS Framework. On the other hand R1 expressed a neutral opinion justified by the fact that the advantages of adopting a tool like the CUMULUS Framework are relevant only if a good reuse in the definition of CMs is possible. Another respondent (R3) considered as Poor the overall benefit of adopting the CUMULUS Framework in a CC process since the time saving would be very low. Both these comments seems to be strictly related

to the peculiarities of the CC certification process since in this process a huge part of the work done by an evaluator is "manual" (e.g. analysis of documental evidence) and it is difficult to automate and reuse. This seems to be confirmed also by the additional comment provided by R4 stating that the initial overhead of setting up an appropriate CM for a CC certification process seems to be high. In this sense, even if adopting the CUMULUS Framework in a CC certification process would bring limited advantages as of today, considering a different and more cloud-oriented certification process or even a modified CC process adapted to the cloud context needs, the cost effectiveness of the CUMULUS Framework would considerably increase.

Three of the respondents also provided general comments to this section. R1 suggested that also part of the document revision that is done during a CC evaluation could be automated (e.g. by verifying the presence of given paragraphs/sections) thus suggesting that the CUMULUS Framework functionalities could be extended and consequently the raw estimation could be revised by considering also this point. Even though the suggested automation cannot be readily included in the CUMULUS scope, it makes some sense in that the CUMULUS Framework could provide automatic tools for assessing, at some extent, some kind of correctness (e.g., the syntactical one) of the artefacts it processes (e.g., of the CM instances). Moreover, R2 suggested that the tools provided by CUMULUS could be used also in the automation of tests done in a standalone non-cloud context. From this point of view, R4 added that his rating regarding the adoption of the Framework (i.e. Q-24) has not fully taken into consideration the cloud nature of the context analyzed. Once considered the context R4 noticed that the overall benefit would be even better.

General comments to the session

Only one respondent gave a general comment to the overall session by stating that the CC certification could be adapted to be automated in a more significant portion but also recognized that this seems to be out of CUMULUS scope.

The validators also provided interesting comments during the session by asking questions about the project and specifically about the topics presented in the slides.

One of this comments was about the Meta-Model (MM) asking the rationale behind the fact that the MM does not share the same terminology with the CC for similar concept like the ToC (Target of Certification, MM term [24]) and TOE (Target Of Evaluation, CC term [15]). After a more precise and detailed description of the ToC and even other concepts, the validators understood that since there isn't a perfect overlapping between the concepts in MM and CC world, the project has deliberately chosen a different term in order to avoid to create confusion and misunderstandings.

Another comment from the validators was about the fact that they considered very difficult to answer to some questions (e.g., the ones about adequateness of the CUMULUS Framework functionalities) without interacting with a concrete tool and without knowing more specific details about how the project has implemented the requirements that it has specified. This could be a good suggestion for the design of a possible second validation session in order to gather a more significant feedback from the validators.

3.2.3. Outlook and Next Steps

The session produced a set of suggestions from the validators that are of two main kinds: suggestions for guiding the rest of the CUMULUS project development and suggestions for improving possible future validation sessions.

As far as the first kind of suggestions is concerned, the validators provided the following advices:

- It could be useful to foresee an explicit coverage of the assurance concept within the Certification Model in order to ease the comparison of two different certified services;
- It could be useful to consider the composition concept that is used in the Common Criteria when defining advanced Certification Models like the multilayer ones;
- The CUMULUS Framework could consider to provide support for syntactical checks of Certification Model instances.

Regarding the second kind of suggestion, the validators provided the following advices:

- The definitions of the key factors identified as relevant for the cost effectiveness analysis could be refined;
- The session could involve a more concrete analysis of the CUMULUS Framework so to allow the validators to get a deeper understanding of its capabilities.

The project will try to take advantage as much as possible of these suggestions to improve the quality of both the CUMULUS Framework and possible future session for its validation, which should be designed considering also the recommendations given in Section 3.2.1.

3.3. Second Session with External Validators

In this Section we report full details about design, execution, and results of the second validation session (Rome, July 2nd 2015). The description given here is integrated by further materials (annex) attached to this document. Section 3.3.1 provides details about session design and execution. Section 3.3.2 provides the session results and a discussion of these. An outlook is finally given in Section 3.3.3.

3.3.1. Session Design and Execution

Introduction

The session was designed to be, as much as possible, consistent with the approach defined in D6.2 [13], which was already adopted for the first session (see [40]). Essentially, we involved as external validators some security evaluation/certification experts, who were requested to answer a suitable questionnaire after being introduced to some advanced aspects of the CUMULUS project.

Session Design

We designed the session by taking into account the Recommendations for Future Sessions given in [13], which produced the following (preliminary) session objectives:

- To involve the same validators exploited in the first session, so to allow the coverage of advanced concepts of CUMULUS;
- To deepen description/representation of the CUMULUS Framework supporting the session;
- To improve the analysis of the relevant dimensions (see [13]).

Actually, we involved in the session the same validation group of the first session: one official certifier from OCSI—Organismo di Certificazione della Sicurezza Informatica (Italian Body for ICT security certification according to the international standard ISO/IEC IS-15408 or Common Criteria (CC) ([15][16][17]) and three evaluation/certification experts (not involved in CUMULUS) from FUB. In the following, the OCSI validator is denoted as respondent R3 and the FUB validators are denoted as respondents R1, R2 and R4.

Many session aspects were influenced by the time availability of the validation group—4 hours, at most. Based on this, we had to:

- Limit the CUMULUS Framework representation to a suitable description of the CUMULUS Framework architecture plus a demo (videoclip) showing the CUMULUS Framework in action;
- Restrict the analyzed dimensions to assurance and usability.

At the end, we structured the session core in two sections, covering assurance and usability, respectively. We decided to introduce the advanced materials supporting the analysis of assurance and usability by a preliminary short presentation to recall the validators some relevant basic concepts of CUMULUS.

SESSION SECTIONS

A brief description of the sections is given here (some more details are given in Table 7) (for a complete view, we refer to the session materials attached to this document):

- CUMULUS Assurance (Section I): Introduction to some specific aspects of the CUMULUS test-based certification process and to the possible contribution of such aspects to the overall CUMULUS certification assurance, as respectively given in [41] and [32] (with suitable simplifications), with corresponding questions from Q-1 to Q-9 (see Table 7) supporting the exploration of assurance and (at some extent of) usability (see below);
- CUMULUS Usability (Section II): Overview of the CUMULUS Framework architecture and functionalities, as given in [42] (with suitable simplifications and special focus on the CUMULUS Dashboard (the CUMULUS Framework GUI) [42]), to analyze, by means of questions from Q-10 to Q-12, the usability of the CUMULUS Framework (see below). To ease the validators responses, the presentation exploited also a short videoclip[11] showing the CUMULUS Framework and its Dashboard in action.

QUESTIONNAIRE DESIGN

Table 7 (see below) provides the list of the questions proposed to the validators, along with the corresponding possible answers and the contributed dimension explorations.

We kept the same questionnaire structure exploited for the first session (see [40]) (only closed-answer questions of two possible types: questions with Yes/No answer (with request for written explanation conditioned on the provided answer) and questions with five level scale answer (Excellent, Good, Neutral, Poor, Very Poor); provision of free text room for each question so to gather as much feedback as possible from the validators; provision of additional free text room both for each session section and for the overall session so to allow the validators to report any extra relevant comment; provision of instructions for the validators). For a complete view, we refer to the session materials attached to this document.

EXPLORED DIMENSIONS

As introduced before, the session to be designed had to support the analysis of assurance and usability. To do this, we considered how to adapt to the session context the reference assurance and usability analyses considered in [13] in such a way to produce some improvements in view of the previous analyses reported in [40]. As for the actual support that the designed session could provide to the intended analyses, the following remarks can be done.

ASSURANCE ANALYSIS REMARKS

The designed validation session contributes the assurance analysis defined in [13] by covering the contributions to the overall certification assurance respectively provided by the following specific aspects of a CUMULUS test-based certification process (see [41] and [32]): test qualification, trust model, certificate life cycle, additional elements related to evidence collection.

As for test qualification, the session enables to:

- Gather from the validators an overall rating of the contribution to the assurance provided by test qualification based on metrics specified by Test Based Certification Models (see [32) (CUMULUS Assurance Section, question Q-1);
- Explore the possibility of enforcing through the Test Based Certification Models hierarchy the contribution to assurance provided by tests by using the methods proposed in [32] (CUMULUS Assurance Section, question Q-2);

[11] The shown videoclip was a simplified version of a videoclip prepared by CITY to demonstrate the functionalities of the CUMULUS Framework with respect to a monitoring-based certification model exploited for eHealth pilot certification.

- Explore the possibility of facing possible assurance requirements by exploiting the qualification of tests specified by Test Based Certification Models (see [32]) (CUMULUS Assurance Section, question Q-3).

Notice that questions Q-2 and Q-3 contribute to satisfy a criterion for assurance analysis given in [12] since they respectively analyze Test Based Certification Models with regard to the possibility of enforcing and verifying the wanted assurance.

As for the CUMULUS Trust Model, the session enables to explore how the trust relations given in [41] support the certificate users for the verification of their assurance requirements on process actors (CUMULUS Assurance Section, question Q-4).

As for the CUMULUS Certificate Life Cycle, the session enables to gather from the validators an overall rating of the support that an actual CUMULUS Framework implementing an example lifecycle given in [41] for Test Based Certification would provide to realize the concept of continuous assessment (CUMULUS Assurance Section, question Q-7) (notice that this concept in the Common Criteria context is known as assurance continuity).

As for additional assurance elements, the session enables to gather from the validators an overall rating of the potential contribution to the assurance of the CUMULUS certification process provided by the high transparency of the process (CUMULUS Assurance Section, question Q-8) and the specific approach to evidence collection (CUMULUS Assurance Section, question Q-9).

The assurance analysis enabled by the designed session is consistent with [13] and incremental with respect to the one reported in [40], where only a generic assessment was made of the capability of CUMULUS Certification Models to represent the assurance provided by corresponding certification processes. Anyway, due to time availability of validators and to their specific test-based certification background, only test-based certification processes were considered.

USABILITY ANALYSIS REMARKS

The designed validation session contributes the usability analysis defined in [13] mainly by covering the aspects of technical quality [13] of the CUMULUS Framework functionalities—given at architectural level [42]—and (user) satisfaction [13] about some CUMULUS Framework functionalities accessible through the Dashboard [42].

As for the technical quality aspect, the session enables to explore both sufficiency and necessity of the CUMULUS Framework functionalities (CUMULUS Usability Section, questions Q-10 and Q-11, respectively).

As for the (user) satisfaction aspect, the session enables to gather from the validators an overall rating of the Dashboard with respect to the operations shown in the videoclip (CUMULUS Usability Section, question Q-12).

An additional (non-standard) contribution to the usability analysis (technical quality aspect) defined in [13] comes from the CUMULUS Assurance Section, which enables to explore both sufficiency and necessity of the constraints fixed by a CUMULUS Certification Model to the specification of a certificate lifecycle [41] (CUMULUS Assurance Section, questions Q-6 and Q-5, respectively).

The usability analysis enabled by the designed session is consistent with [13] and incremental with respect to the one reported in [40]. Anyway, mainly due to time availability of validators, actual active interactions with the CUMULUS Framework are not considered (see *validation platform* in [13]).

#	Text	Possible Answers	Explored Dimensions	Reference Section
Q-1	Rate the contribution to the assurance of a CUMULUS Test Based Certification process provided by test qualification based on metrics specified in the corresponding Certification Models.	Excellent Good Neutral Poor	Assurance	CUMULUS Assurance (I)

		Very Poor		
Q-2	Apart from the ones proposed by CUMULUS to enforce assurance in Test Based Certification process (from a consistent certification model to one of a lower abstraction level, by test qualification based on preselected metrics/tests), should additional methods be considered? If yes, please, specify.	Yes No	Assurance	CUMULUS Assurance (I)
Q-3	Is the approach taken by CUMULUS (test qualification based on test metrics) unsatisfactory for facing possible assurance requirements associated with particular users/issuers of Test Based Certification Models? If yes, please specify.	Yes No	Assurance	CUMULUS Assurance (I)
Q-4	Does the CUMULUS Trust Model offer certificate users significant support to verify their assurance requirements on process actors? If no, please specify.	Yes No	Assurance	CUMULUS Assurance (I)
Q-5	Are the constraints fixed by CUMULUS for the specification of a certificate lifecycle (in a Test Based Certification Model, by means of states and state transitions) all necessary? If no, please, specify.	Yes No	Usability	CUMULUS Assurance (I)
Q-6	Should CUMULUS fix additional constraints for the specification of a certificate lifecycle (in a Test Based Certification Model, by means of states and state transitions)? If yes, please, specify.	Yes No	Usability	CUMULUS Assurance (I)
Q-7	Rate the support that an actual CUMULUS Framework implementing the presented example of CUMULUS Certificate Life Cycle would provide to realize the CC concept of assurance continuity.	Excellent Good Neutral Poor Very Poor	Assurance	CUMULUS Assurance (I)
Q-8	Rate the potential contribution of the high transparency of the CUMULUS certification process to the overall assurance.	Excellent Good Neutral Poor Very Poor	Assurance	CUMULUS Assurance (I)
Q-9	Rate the potential contribution to the overall assurance of the CUMULUS certification process of collecting evidence by relying on both agents deployed on the relevant cloud system and integrity checks of the underlying platform by means of TC mechanisms[12] .	Excellent Good Neutral Poor Very Poor	Assurance	CUMULUS Assurance (I)
Q-10	Are there any missing functionalities in the CUMULUS Framework? If yes, please specify.	Yes No	Usability	CUMULUS Usability (II)
Q-11	Are the functionalities provided by the CUMULUS Framework all necessary? If no, please specify.	Yes No	Usability	CUMULUS Usability (II)
Q-12	Overall rate the dashboard of the CUMULUS Framework for the presented operations (slides and videoclip).	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Usability (II)

Table 7. Questions proposed for the session with external validators

Session Execution

The session started with a presentation of the session structure and objectives and went on with an introduction to the relevant aspects of CUMULUS. Then, the materials supporting the two core sections were presented, taking a total time of about 2.5 hours. Finally, the validators filled in the questionnaires, taking a total time of about 30 minutes. Where needed, details were provided to validators to clarify

[12] This is the text of Q-9 that was actually considered by the validators (in the distributed one, reported in the annexes attached to this deliverable, there is a missing text typo).

either presented concepts and/or proposed questions. Where needed, the validators were requested to clarify their answers/comments to the questionnaire.

3.3.2. Session Results

Introduction

For the analysis of the feedback form the validators, we take the qualitative approach announced in [13] (and already adopted in the first session (see [40])).

Both answers and comments from the validators are first discussed question by question. Then, the more relevant suggestions and recommendations emerged from the discussion are summarized at the end of the section.

Validation Results

Table 8 provides the raw answers of the validators to the questions proposed, while in the next subsections the answers to each question are discussed in detail along with the relevant comments (for a complete view of the feedback from validators, we refer to the session materials attached to this document).

#	R1	R2	R3	R4
Q-1	Good	Good*	Good	Good
Q-2	No	No	No	No
Q-3	No	N/A*	No	No
Q-4	Yes	Yes	Yes	Yes
Q-5	Yes	Yes	Yes	Yes
Q-6	No	Yes*	No	No
Q-7	Good	Excellent*	Excellent*	Good
Q-8	Excellent	Good	Good	Good*
Q-9	Good	Good*	Excellent*	Good
Q-10	No	No	Yes*	No
Q-11	Yes	Yes	Yes	Yes
Q-12	Neutral*	Good	Good	Poor*

Table 8. Raw results of the responders to the questionnaire.

Answers enriched by significant comments (see below) are asterisked (the reader can retrieve all validators´comments by checking the annexes attached to this deliverable).

Assurance Analysis

CUMULUS ASSURANCE SECTION

Questions from Q-1 to Q-4 and from Q-7 to Q-9 aimed at supporting assurance analysis (see Table 7).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents rated Good the contribution to the assurance of a CUMULUS Test Based Certification process provided by test qualification based on metrics specified in the corresponding Certification Models (see raw answers to Q-1 in Table 8);
- All the respondents agreed that no additional methods should be considered apart from the ones proposed by CUMULUS to enforce assurance in Test Based Certification process (see raw answers to Q-2 in Table 8)

- All the respondents—with one exception (R2)—found it satisfactory the approach taken by CUMULUS for facing possible assurance requirements associated with particular users/issuers of Test Based Certification Models (R2 did not give an answer deliberately, alleging insufficient skill) (see raw answers to Q-3 in Table 8);
- All the respondents agreed that the CUMULUS Trust Model offer certificate users significant support to verify their assurance requirements on process actors (see raw answers to Q-4 in Table 8);
- All the respondents rated Excellent or Good the support that an actual CUMULUS Framework implementing the presented example of CUMULUS Certificate Life Cycle would provide to realize the CC concept of assurance continuity so confirming that such Life Cycle could provide a significant contribution to the assurance of a certification process based on the continuous assessment approach (see raw answers to Q-7 in Table 8);
- All the respondents rated Excellent or Good the potential contribution of the high transparency (based on tracking of all relevant actions related to evidence collection and maintenance of the corresponding results) of the CUMULUS certification process to the overall assurance (see raw answers to Q-8 in Table 8);
- All the respondents rated Excellent or Good the potential contribution to the overall assurance of the CUMULUS certification process of collecting evidence by relying on both agents deployed on the relevant cloud system and integrity checks of the underlying platform by means of Trusted Computing (TC) mechanisms (see raw answers to Q-9 in Table 8).

Some significant comments were also provided for specific questions.

When answering to Q-1, R2 pointed out that ranges of possible values should be defined for test metrics to be actually rated and compared.

When answering to Q-7:

- R2 had the feeling that, in the proposed lifecycle, the certificate status “follows” in a sense the service security status, which provides a sound contribution to the overall assurance;
- R3 underlined that a certificate lifecycle based on automatisms and on a digital signature framework could also significantly reduce controversies and legal issues.

When answering to Q-8, R4 pointed out that, to better satisfy possible assurance requirements coming from certificates end users and therefore increase the overall assurance of the certification process, CUMULUS should take care of implementing an infrastructure for managing identity and attribute certificates. After a direct interaction, the respondent recognized that implementing such an infrastructure is out of the CUMULUS scope. Notice that the potential contribution of digital signatures (and associated certificates) to the overall assurance is considered also by R3 when commenting to Q-7 (see before).

When answering to Q-9:

- R2 pointed out that, to rate more precisely the contribution of the evidence collection to the overall assurance of a CUMULUS certification process, additional information could be needed, e.g., about the developer of the agents and the agreements/commitments between the service provider and the accredited lab;
- R3 underlined that the nature of cloud services seems to force the use of trusted platform for testing. Moreover, in R3 opinion, the adoption of TC mechanisms by cloud providers should also enhance quality of service and not only security.

Usability Analysis

CUMULUS USABILITY SECTION

Questions Q-10, Q-11 and Q-12 aimed at supporting usability analysis (see Table 7) by exploring the technical quality [13] of the CUMULUS Framework functionalities and the user satisfaction about some functionalities accessed via the CUMULUS Dashboard.

The feedback from the validators was mostly positive (after analyzing the comments from the validators (see below)) and can be summarized as follows:

- All the respondents—with one exception (R3)—agreed that the functionalities provided by the CUMULUS Framework are sufficient (R3 pointed out that push notifications of specific events, especially those related to the certificate status, are apparently missing) (see raw answers to Q-10 in Table 8);
- All the respondents agreed that the functionalities provided by the CUMULUS Framework are all necessary (see raw answers to Q-11 in Table 8);
- Two of the respondents (R2 and R3) overall rated Good the CUMULUS dashboard for the operations presented, while the feedback from the other two respondents was Neutral (R1) and Poor (R4) (see raw answers to Q-12 in Table 8).

To clearly understand the answers to question Q-12 it was necessary to directly interact with the validators. It turned out that the motivation for the critical positions came from the fact that, with respect to the operations shown in the videoclip, both R1 and R4 found that the way the certificates and certification models are presented in the dashboard, by showing the raw XML, was not easily readable. This seems to be an interesting suggestion for improving the dashboard usability, although the functionality it addresses (XML rendering) is not directly connected to the specific objectives of CUMULUS.

CUMULUS ASSURANCE SECTION

Questions Q-5 and Q-6 aimed at supporting usability analysis (see Table 7) through an assessment of the technical quality [13] of the constraints fixed by CUMULUS for the specification of a certificate lifecycle.

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the constraints fixed by CUMULUS for the specification of a certificate lifecycle are all necessary (see raw answers to Q-5 in Table 8);
- All the respondents except one (R2) agreed that CUMULUS should not fix additional constraints for the specification of a certificate lifecycle (R2 motivated the disagreement with the possible need to specify a maximal time in which a state could last) (see raw answers to Q-6 in Table 8).

General Comments to the Session

R2 was the only respondent to report an extra comment. This comment about the CUMULUS Assurance Section suggested that, in the CUMULUS Test Based certification process, the Certification Authority could double-check a sample of the evidence provided by the Accredited Lab before issuing a Certificate (i.e. repeat a portion of the tests executed by the Lab). Even though this kind of verification is not explicitly considered in CUMULUS, it seems that it is consistent with the possible usage of the CUMULUS Framework.

The validators also provided interesting comments during the session by asking questions about the topics presented. The CUMULUS certificate life cycle and the possible role of a human actor (certifier) in its actual implementation were especially discussed. It was pointed out that direct intervention of the certifier could be required at least to:

- React on time to any problem that may occur during the execution of a Certification Model and should be promptly notified (such problems are among the events considered by R3 when motivating the answer to Q-10 reported above);

- Specify on a case-by-case basis some condition for transition, e.g., how long a certificate may be suspended (this type of consideration motivated the answer of R2 to Q-6 reported above).

In the resulting discussion it was highlighted to the validators that, even though the CUMULUS certificate life cycle, and, more generally, all the CUMULUS Framework concepts and operation, aim at automating the certification process as much as possible, the intervention of human actors is not ruled out at all.

3.3.3. Outlook

The overall results of the second validation session seem to be positive according to the feedback gathered from the validators through the questionnaire and the interactions during the session itself. As a matter of fact the answers provided by the validators indicate that, for the dimensions explored in the session (i.e. assurance and usability), the project satisfied their expectations.

Anyway, the validators provided the following advices:

- To better fulfill possible assurance requirements coming from users of CUMULUS certificates, an infrastructure for managing identity and attribute certificates could be implemented and some additional information could be provided (e.g., about the developer of the agents and the agreements/commitments between the service provider and the accredited lab);
- As for usability, the CUMULUS dashboard could be enhanced by providing a more accessible way of presenting the XML of the certificates and certification models and by providing push notifications of specific events, especially those related to the certificate status.

Such final suggestions seem to be non-critical from the point of view of the project since they are not directly connected to the CUMULUS main objectives. Nevertheless they could be considered as recommendations for possible future follow-up of the CUMULUS project and/or possible future implementations of the CUMULUS Framework to support a real world certification scheme.

4. Evaluation of Trusted Computing project results

4.1. Introduction and recapitulation from D6.2

As explained in the specification of CUMULUS evaluation criteria [13], Infineon undertakes a Common Criteria certification of its new TPM 2.0 chip. The corresponding security evaluation of the TPM security properties related to CUMULUS requirements is done within CUMULUS.

In the TPM 2.0 Protection Profile (PP) [14], the following requirements have been selected as CUMULUS validation criteria:

- **Cryptographic Security Functional Requirements (SFR)**

  The support of new cryptographic functions and the flexible usage of cryptographic algorithms facilitates the use of the TPM in CUMULUS scenarios and in the certification infrastructure.

- **Measurement and Reporting SFR**

  The TPM measuring and reporting functions are crucial to assure the integrity of CUMULUS components. The new TPM V2.0 support for more than one bank of PCRs adds additional flexibility.

- **Security Assurance Requirements (SAR)**

  The SARs describe the measures to be taken during development and evaluation of a product to assure compliance with the claimed security functionality. With respect to the evaluation of security properties related to CUMULUS requirements, the evaluation process and artefacts must comply with the SARs.

4.2. Overview of CC certification of Infineon TPM

Security evaluation is a crucial part of the Common Criteria (CC) certification process. The following figure illustrates the three main parties involved in the certification process and the process steps.

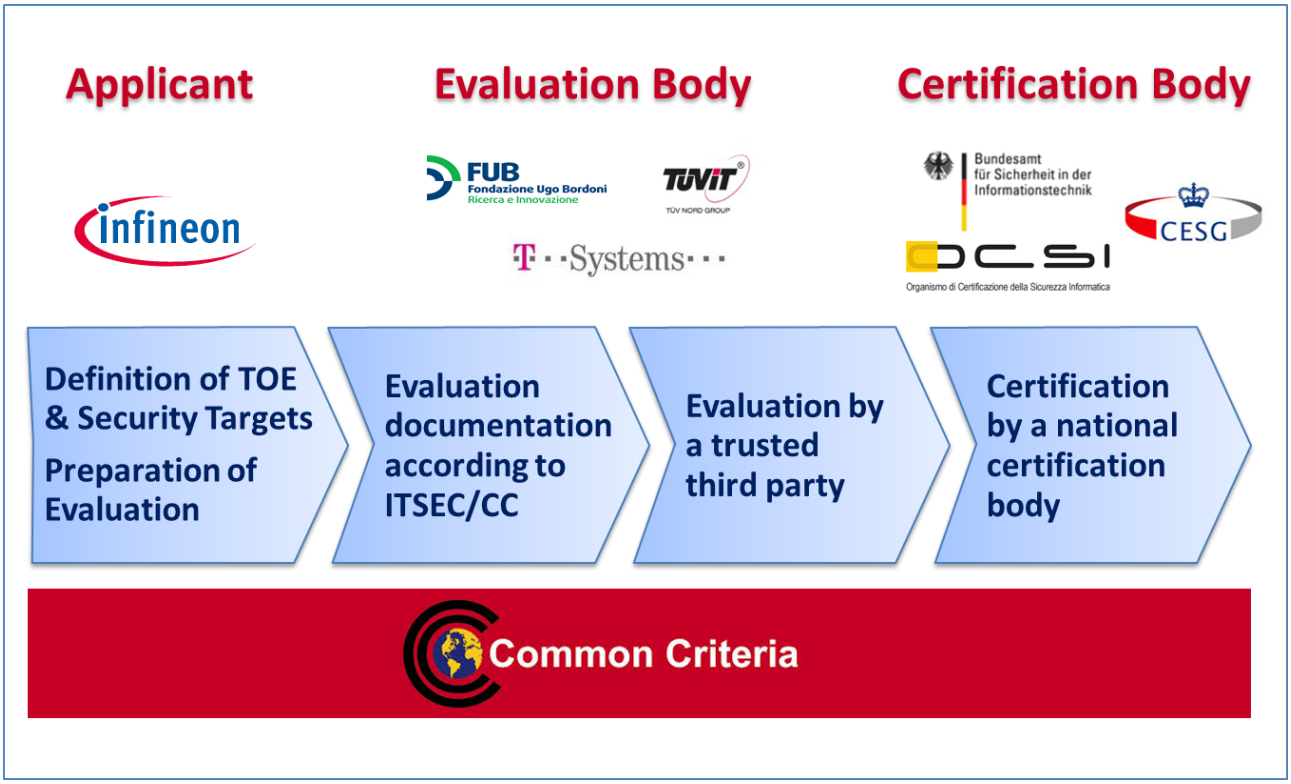

Figure 5. Common Criteria Certification Process

With respect to the TPM 2.0 certification, Infineon Technologies AG is in the role of the applicant. Infineon develops all artefacts necessary for the security evaluation, which includes developing and executing test cases related to the evaluation criteria and writing comprehensive documentation. The applicant's effort and costs exceed Infineon's planned effort in CUMULUS WP6 by far. On the other hand, not all properties covered in the security evaluation are CUMULUS specific. Therefore the work in CUMULUS task 6.3 focuses only the validation criteria listed in section 4.1.

CC defines seven Evaluation Assurance Levels (EAL) which determine the depth and rigor of an evaluation, [15] [16] [17]. Each EAL corresponds to a precisely defined set of security assurance requirements (SARs) covering the complete development of a product, with a given level of strictness, ranging from EAL1, which stands for functionally tested, up to EAL7, meaning formally verified, designed and tested. The following figure depicts the seven levels.

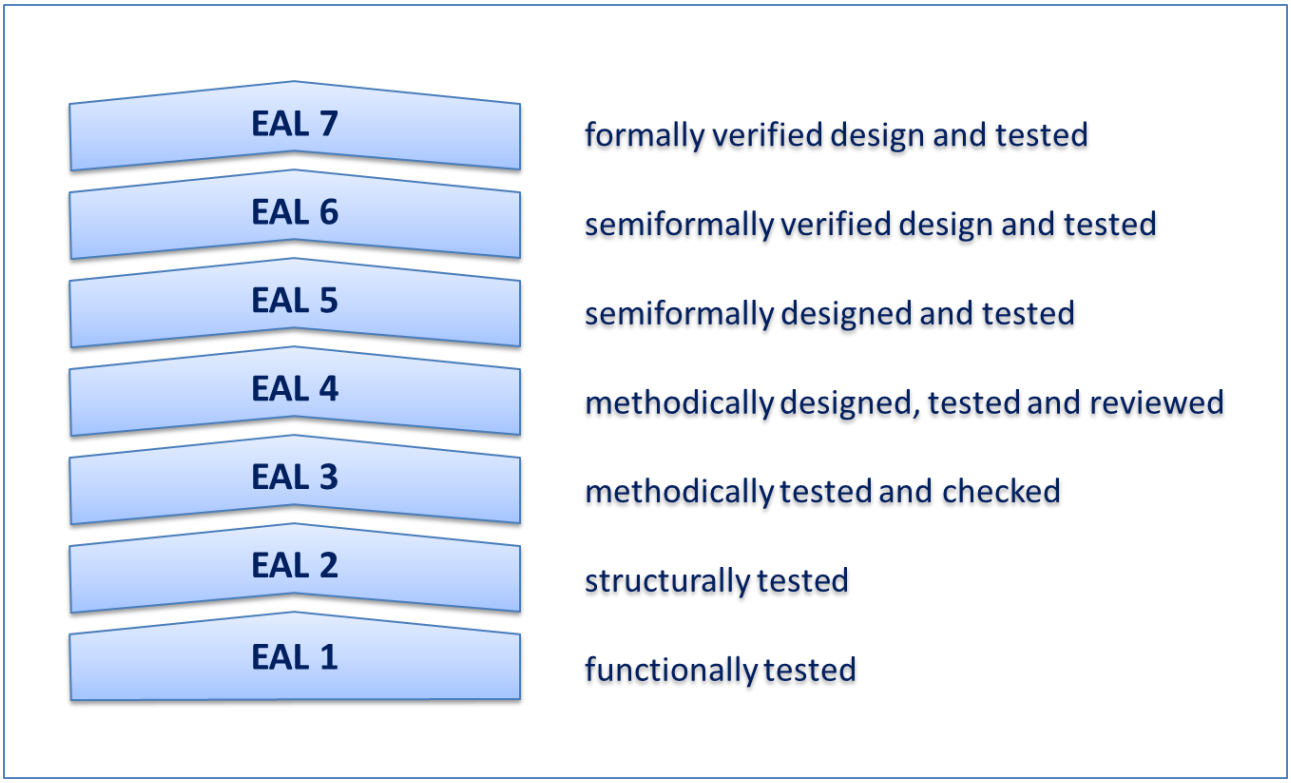

Figure 6. Common Criteria Evaluation Assurance Levels

To meet specific objectives for a given product category to be certified, an assurance level can be augmented by one or more additional SARs. In the EAL notation this augmentation is indicated by a '+' suffix, e.g. "EAL 4 augmented" is noted as "EAL 4+".

In CC Version 3.1 the targeted level of vulnerability analysis and attack potential is specified additionally for security products providing cryptographic functions (called "strength of function" or SOF in earlier CC versions). This corresponds to the minimum effort necessary to successfully attack the underlying security mechanisms. Possible values are basic, enhanced-basic, moderate and high.

The following figure explains the EAL notation, including augmentation and level of vulnerability analysis.

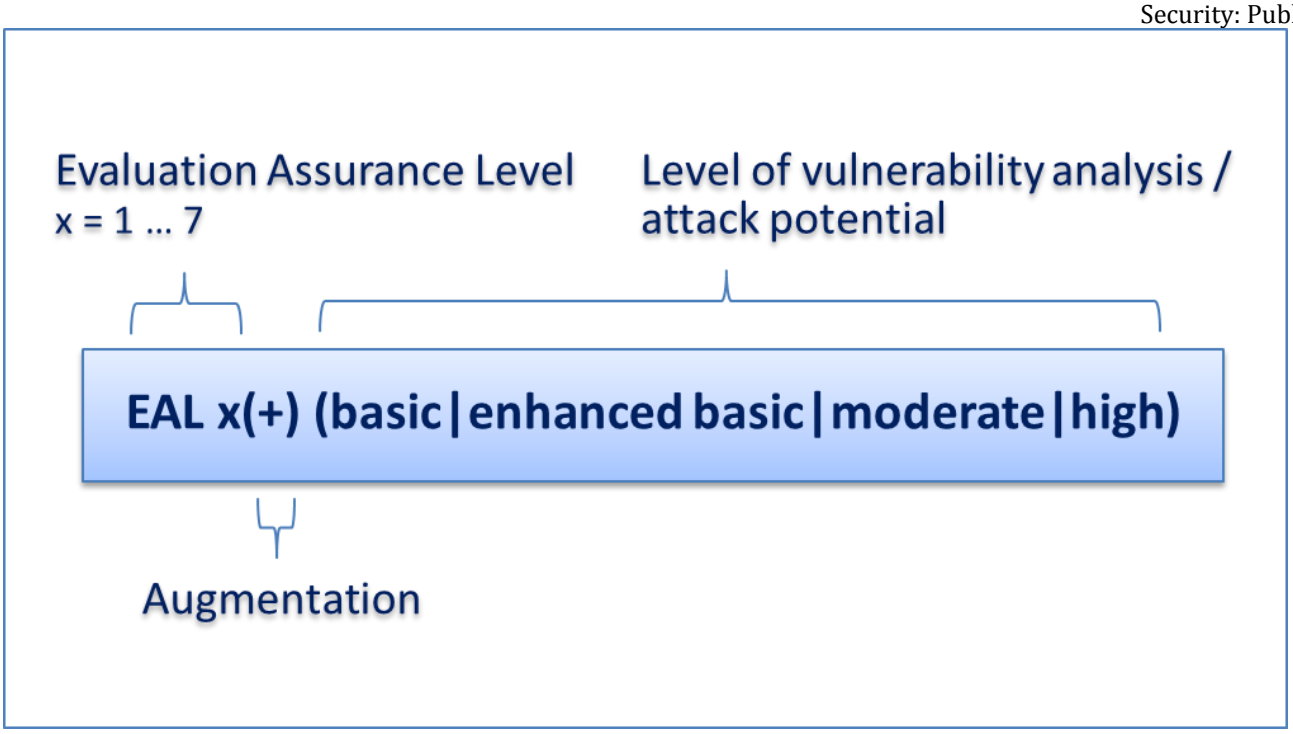

Figure 7. Evaluation Assurance Level Notation

The assurance level targeted by CC TPM 2.0 certification is EAL 4+ moderate (according to CC Version 3.1 Revision 4, [15] [16] [17]), which means:

- Methodically designed, tested and reviewed
- Augmented with specific additional SARs required for TPM certification (ALC_FLR.1 and AVA_VAN.4, see [13])
- The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the Target of Evaluation (TOE). Penetration testing is performed by the evaluator assuming an attack potential of Moderate (AVA_VAN.4, see [13]).

Typical characteristics for this assurance level are approximately 3000 pages of technical documentation and certification duration of 9 to 12 months.

Note that other Infineon products based on the same family of security ICs as the new TPM 2.0 chip are certified to higher assurance levels than EAL4.

4.3. Performed work and achieved results

When the specification of CUMULUS evaluation criteria [13] was written in the beginning of 2014, the release of the TPM 2.0 PP was expected in the second quarter of the same year. As of today, a public review version of the PP has been available for several months, but no released version. The review version does not have any changes concerning the validation criteria relevant for CUMULUS (see section 1.1), and there is no indication that the PP review process will lead to such changes. As a consequence the CC evaluation related work at Infineon could be started nearly as planned originally.

The following tasks have been performed by Infineon in order to define the TOE and Security Targets (ST) and to prepare the evaluation to be executed by an accredited evaluation body:

- Development of tests necessary for the evaluation
- Execution of all tests necessary for the evaluation
- Development of all certification documentation necessary to start the evaluation

In general the first feedback from the evaluation body indicates that the TOE (the new Infineon TPM 2.0 chip) can meet the requirements to be CC certified according to the aimed EAL.

4.3.1. TPM 2.0 Security Evaluation Test Tool

Infineon has developed a TPM 2.0 Security Evaluation Test Tool which covers all the requirements defined in the PP. In particular, for each SFRs listed in [13] a test case has been written. Also all SARs listed in [13] which are relevant for testing, have been considered in the design and implementation of the TPM 2.0 Security Evaluation Test Tool. The tests are integrated in Infineon's continuous build and delivery framework which means that they are fully automated and executed whenever the chip's embedded TPM software is built.

Prior to the start of the TPM 2.0 security evaluation at the authorized evaluation body, all CC related tests have been executed with success.

The following table provides an overview of CUMULUS relevant tests executed by Infineon to prepare CC security evaluation.

Requirement Category	Test Tool	Test Tool Component	Status
Cryptographic SFR	TPM 2.0 Security Evaluation Test Tool (newly developed by IFX, fully automated test execution)	TPM 2.0 Crypto tests	100% test cases executed with success
Measurement and Reporting SFR	TPM 2.0 Security Evaluation Test Tool (newly developed by IFX, fully automated test execution)	TPM 2.0 Measurement & Reporting tests	100% test cases executed with success
Security Assurance Requirements (SAR)	Considered in the design and implementation of the TPM 2.0 Security Evaluation Test Tool		

Table 9. Overview of CUMULUS relevant tests

4.3.2. Cryptographic Security Functional Requirements

The following table shows the mapping of cryptographic SFR and test cases, and the test execution status.

SFR ID	SFR	Test Case	Test Execution Status
FCS_RNG.1	Random number generation	Random number generation	Succeeded
FCS_CKM.1/PK	Cryptographic key generation (primary keys)	Generation of primary keys	Succeeded
FCS_CKM.1/RSA	Cryptographic key generation (RSA keys)	Generation of RSA keys	Succeeded
FCS_CKM.1/ECC	Cryptographic key generation (ECC keys)	Generation of ECC keys	Succeeded
FCS_CKM.1/SYMM	Cryptographic key generation (symmetric keys)	Generation of symmetric keys	Succeeded
FCS_CKM.4	Cryptographic key destruction	Key destruction	Succeeded
FCS_COP.1/AES	Cryptographic operation (symmetric encryption/decryption)	AES encryption and decryption	Succeeded

SFR ID	SFR	Test Case	Test Execution Status
FCS_COP.1/SHA	Cryptographic operation (hash function)	Hash value calculation	Succeeded
FCS_COP.1/HMAC	Cryptographic operation (HMAC calculation)	HMAC calculation	Succeeded
FCS_COP.1/RSAED	Cryptographic operation (asymmetric encryption/decryption)	RSA encryption and decryption	Succeeded
FCS_COP.1/RSASign	Cryptographic operation (RSA signature generation/verification)	RSA signature generation and verification	Succeeded
FCS_COP.1/ECDSA	Cryptographic operation (ECC signature generation/verification)	ECC signature generation and verification	Succeeded
FCS_COP.1/ECDAA	Cryptographic operation (ECDAA commit)	DAA signature generation	Succeeded
FCS_COP.1/ECDEC	Cryptographic operation (decryption)	Decryption of ECC key	Succeeded

Table 10. TPM V2.0 Cryptographic SFR

4.3.3. Measuring and reporting Security Functional Requirements

The following table shows the mapping of Measurement and Reporting SFR and test cases, and the test execution status.

SFR ID	SFR	Test Case	Test Execution Status
FDP_ACC.1/M&R	Subset access control (measurement and reporting)	M&R access control	Succeeded
FDP_ACF.1/M&R	Security attribute based access control (measurement and reporting)	M&R access control by security attribute	Succeeded
FMT_MSA.1/M&R	Management of security attributes (measurement and reporting)	M&R management of security attributes	Succeeded
FMT_MSA.3/M&R	Static attribute initialization (measurement and reporting)	M&R static attribute initialization	Succeeded
FCO_NRO.1/M&R	Selective proof of origin (measurement and reporting)	M&R proof of origin	Succeeded

Table 11. TPM V2.0 Measurement and reporting SFR

4.3.4. Security Assurance Requirements

The following table shows how the Security Assurance Requirements (SAR) are handled during TPM 2.0 security evaluation.

Assurance Class	Assurance components	Implementation	Evaluation
ADV: Development	ADV_ARC.1 Security architecture description	SLB9665_ARC.doc	Done by IFX
	ADV_FSP.4 Complete functional specification	SLB9665_FSP.doc	Done by IFX
	ADV_IMP.1 Implementation representation of the TSF	SLB9665_IMP.doc	Done by IFX
	ADV_TDS.3 Basic modular design	SLB9665_TDS.doc	Done by IFX
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	SLB9665_AGD.doc	Done by IFX
	AGD_PRE.1 Preparative procedures	SLB9665_AGD.doc	Done by IFX
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	Development_Prod-uction.doc SLB9665_CMS.doc SLB9665_ALC.doc	Done by IFX
	ALC_CMS.4 Problem tracking CM coverage	Development_Prod-uction.doc SLB9665_CMS.doc SLB9665_ALC.doc	Done by IFX
	ALC_DEL.1 Delivery procedures	Development_Prod-uction.doc SLB9665_ALC.doc	Done by IFX
	ALC_DVS.1 Identification of security measures	SLB9665_ALC.doc	Done by IFX
	ALC_LCD.1 Developer defined life-cycle model	Development_Prod-uction.doc	Done by IFX
	ALC_FLR.1 Basic flow remediation	SLB9665_ALC.doc	Done by IFX
	ALC_TAT.1 Well-defined development tools	Development_Prod-uction.doc SLB9665_ALC.doc	Done by IFX
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	SLB9665_SecTar.doc	Done by IFX
	ASE_ECD.1 Extended components definition	SLB9665_SecTar.doc	Done by IFX
	ASE_INT.1 ST introduction	SLB9665_SecTar.doc	Done by IFX
	ASE_OBJ.2 Security objectives	SLB9665_SecTar.doc	Done by IFX
	ASE_REQ.2 Derived security requirements	SLB9665_SecTar.doc	Done by IFX
	ASE_SPD.1 Security problem definition	SLB9665_SecTar.doc	Done by IFX
	ASE_TSS.1 TOE summary specification	SLB9665_SecTar.doc	Done by IFX
ATE: Tests	ATE_COV.2 Analysis of coverage	SLB9665_ATE.doc	Done by IFX

Assurance Class	Assurance components	Implementation	Evaluation
	ATE_DPT.2 Testing: security enforcing modules	SLB9665_ATE.doc	Done by IFX
	ATE_FUN.1 Functional testing	SLB9665_ATE.doc	Done by IFX
	ATE_IND.2 Independent testing - sample	Single Evaluation Report ETR-Part AVA	Done by Evaluation Body
AVA: Vulnerability assessment	AVA_VAN.4 Methodical vulnerability analysis	Single Evaluation Report ETR-Part AVA	Done by Evaluation Body

Table 12. Security Assurance Requirements for the TOE

4.3.5. TPM Security Evaluation Documentation

The following documents have been developed to prepare CC security evaluation.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
SLB9665_2.0 Security Target	Definition of the security requirements of the product	60 pages	Public (as soon as certification is completed)	Infineon
SLB9665_2.0 Functional Specification	Definition of the TOE Security Functionality Interfaces	50 pages	Confidential	Infineon
SLB9665_2.0 Security Architecture	Definition of the Security Architecture	120 pages	Confidential	Infineon
SLB9665_2.0 Literature_ Reference	Definition of the used Literature and References	20 pages	Confidential	Infineon

Table 13. TPM Security Evaluation Documentation

The following documents will be available after the security evaluation.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
SLB9665_2.0 Test Documentation	Definition of the TOE Test procedures	50 pages	Confidential	Infineon
SLB9665_2.0 TOE Design	Definition of the Design of hardware and firmware	180 pages	Confidential	Infineon
SLB9665_2.0 Guidance Documentation	Definition of the TOE User Guidance	10 pages	Confidential	Infineon
SLB9665_2.0 AIS20 Developer evidence for the DRNG	Definition of the TOE DRNGs	30 pages	Confidential	Infineon
SLB9665_2.0 Life-cycle Support	Definition of the TOE life cycle	15 pages	Confidential	Infineon
SLB9665_2.0 Configuration Management	Definition of the TOE configuration management	15 pages	Confidential	Infineon
SLB9665_2.0	Definition of the TOE	50 pages	Confidential	Infineon

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
Implementation	implementation and generation processes			
Production and Development	Definition of the TOE development, production, test and delivery processes	70 pages	Confidential	Infineon
Protection Profile PC Client Specific TPM	Definition of the TOE Security Requirements	110 pages	Public	Trusted Computing Group

Table 14. Documentation after evaluation

The following documents will be available after the CC certification.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
Protection Profile PC Client Specific TPM	Definition of the TOE Security Requirements	110 pages	Public	Trusted Computing Group
SLB9665_2.0 Security Target	Definition of the security requirements of the product	60 pages	Public	Infineon
Certification Report BSI-DSZ-CC-0965-2015 for SLB9665_2.0	Certification report of the Bundesamt für die Sicherheit in der Informationstechnik	40 pages	Public	Bundesamt für die Sicherheit in der Informations-technik

Table 15. Documentation after CC certification

4.4. Conclusions

The TPM 2.0 security evaluation has been completed as planned before in late summer 2015. In September 2015, the German Federal Office for Information Security (BSI) completed the certification of the new Infineon TPM 2.0 chip. Thus Infineon is the first TPM manufacturer with a TPM 2.0 chip certified according to Common Criteria, and CUMULUS TC based certification mechanisms can be used also with Common Criteria certified TPM 2.0 modules.

5. CUMULUS Engineering Tool Evaluation

Two focus-group sessions were carried out to evaluate the CUMULUS Engineering Tool (CET). Appendix 6 shows the English version of the questionnaire template used for the second evaluation session described below. For the first evaluation session a Spanish version of the questionnaire was prepared. Score range for answers to questions was the following: 5 - fully agree; 4 - mostly agree; 3 - neither agree nor disagree; 2 - mostly disagree; 1 - completely disagree. The results presented below summarise as positive answers those with scores 5 or 4, neutral with score 3, and negative with scores 2 or 1.

5.1. First Focus Group Evaluation

The first focus group was chosen to represent mainly system designers/developers in their early stage career but with experience using different frameworks for security requirements engineering and definition. The evaluation session took place on 3rd December 2014 at the University of Malaga with a total of 28 participants. An introduction to the CUMULUS engineering process and CET was given followed by hands-on of tool functionality in a controlled environment using early (alpha) release of the software delivered in D4.4. Then, we asked the focus-group users to create some basic security solutions and related artefacts (create a basic Domain Security Metamodel (DSM)) and use CET to apply those. The main goal was to evaluate both the usability and the learning curve of using the engineering framework, particularly to specify security knowledge (DSM) and apply that knowledge to a system model. We received quite positive responses regarding usability of CET and neutral-to-positive responses on learning to produce security knowledge for the engineering process. Particularly:

- 65% to 86% of positive answers with 29% to 11% of neutral answers and 6% to 3% of negative answers on all questions regarding usability of CET functionalities.
    - The lowest positive answer 65% was regarding the user-friendly aspects of CET with 29% neutral and 6% negative.
    - Regarding the usability of experts' security knowledge structured by means of DSM artefacts (partly reflecting on the learning curve of security knowledge representation), 68% answered positively to whether it is easy to understand what security knowledge (security requirements, properties, solutions) is applied to a system model, with 25% neutral and 7% negative answers.
    - Regarding the usability of the CUMULUS engineering process and its artefacts transformation phases, 79% answered positively to whether it is easy to apply the security knowledge from the Domain Security Metamodel (DSM) to the System Model, with 15% neutral and 6% negative answers.
    - The highest positive answer 86% was regarding the usability of CET with respect to the operations executed in the evaluation session (for engineering systems security), with 11% neutral and 3% negative answers.

- 85% responded to have encounter errors in generation of security knowledge (DSM). Thanks to the strong model validation capability of CET, 42% of those encountered errors responded positively on the usability of the model validation aspects of CET to correct the errors and produce a valid DSM, 54% responded neutral on usability of CET model validation as they had to additionally figure out how to correct (and complete) the security knowledge artefacts to produce a valid DSM, and 4% responded negatively on the usability of the model validation aspects of CET.

5.2. Second Focus Group Evaluation

The second focus group was chosen to represent experienced and industry fellows13 in the areas of cloud computing and cyber-physical system to evaluate the usability of the CET and its relevance to engineering secure systems. To do so, the second focus-group session was organised (took place) during LAW 201414. It gathered 11 leading practitioners and security experts in the areas. For the second evaluation session, an introduction to the CUMULUS engineering process and CET was given followed by a live demonstration of CET functionality using early (alpha) release of the software delivered in D4.4. Due to time restrictions (given the LAW workshop programme) no hands-on tool functionality was offered). Results were quite positive for usability of CET and its relevance to secure system engineering. Particularly, 55% to 91% of positive answers with 36% to 9% neutral answers and no negative answers on most of the questions regarding usability of CET functionalities except for two questions:

- 65% positive, 35% neutral and 0% negative answers to whether it is easy to understand what security knowledge (security requirements, properties, solutions) is applied to the system model. This aspect regards the usability of experts' security knowledge expressed by means of DSM artefacts (partly reflecting on the learning curve of security knowledge representation).
- 73% positive, 27% neutral and 0% negative answers to whether it is easy to apply the security knowledge from the Domain Security Metamodel (DSM) to the System Model. This aspect regards the usability of the CUMULUS engineering process and its artefacts transformation phases.
- 91% positive, 9% neutral and 0% negative answers to how successful CET is in performing its task for engineering systems security. This aspect mainly regards the relevance of CET to engineering systems security.
- 72% positive, 28% neutral and 0% negative answers to how likely it is you would recommend CET to a friend or colleague for engineering systems security. This aspect mainly regards the relevance of CET to engineering systems security.
- 55% positive, 36% neutral and 9% negative on how user-friendly CET is. This aspect mainly regards the usability of the GUI of CET to perform the intended functionalities for engineering systems security.
- 18% positive, 65% neutral and 18% negative answers to whether it is easy to understand the certification requirements/assurance aspects applied to the system model. This aspect regards usability of the CET functionality when applying certification requirements (defined in a DSM) to a system model and resolving those with certified services compliant with those requirements.

5.3. Conclusions

Several directions of improvements of CET functionality were suggested. User friendliness of CET is still to be improved by making its GUI easier and more intuitive to apply the engineering process and security artefacts into a system model, as well as the selection and import of DSMs from repositories. It was also suggested a better visualisation and distinction of what security knowledge is automatically added to a system model. Another important direction of improvement is the CET model validation functionality making it more rigorous, more interactive with a set-by-step validation, and more error-accurate for

[13] We got the following answers to the only question about participants to indicate type of organization and role: Industry (Tech Director), Academic & Industry, Academic, Governmental, Industry, Industry, Academic, Industry (CTO), Industry (Aerospace), Industry, Academic & NIST (The National Institute of Standards and Technology).

[14] 8th Layered Assurance Workshop (LAW-2014) collocated with 30th Annual Computer Security Applications Conference (ACSAC 2014) held in New Orleans, Louisiana, USA, December, 2014.

security artefacts generation. This is especially in relation to improve the learning curve of producing security knowledge for engineering.

Based on the received results, we improved the CET's GUI part corresponding to the step of the engineering process applying certification requirements to a system model and the step of resolving certification requirements to CUMULUS-certified services. This improvement was important to address the rather neutral to negative aspect of the realisation of certification requirements applicability in the CET. The improved CET was released with deliverable D4.4.

6. Legal Evaluation

6.1. Overview

In this section, we provide a supplemental analysis to the legal evaluation of the CUMULUS infrastructure described in deliverable D6.2 in 2014 [13]. As in the original report, the legal implications of providing and using the CUMULUS infrastructure have been examined from four broad criteria:

(1) contractual liability,
(2) non contractual liability,
(3) data protection, and
(4) other issues.

The supplemental analysis documented in this deliverable assumes the four parties, which were identified in [13] as having some form of legal relations in the various configurations of the operational use of CUMULUS, namely:

(i) The *CUMULUS software producer* – This is the party that has designed and created the CUMULUS infrastructure (this party is also referred to as CUMULUS consortium).
(ii) The *Certification Provider* – This is the individual or company that uses the CUMULUS infrastructure – under license or contract from the software producer – in order to test and monitor cloud security and produce certificates.
(iii) The *Cloud Operator* – This is the party who offers cloud services and who will rely on certificates produced by the Certification Provider using the CUMULUS infrastructure or directly by itself using the CUMULUS infrastructure (in cases of self-certification).
(iv) The *Cloud User* – This is any individual or company that uses the cloud services of the Cloud Operator for business or personal affairs.

In producing this supplemental analysis, we have:

(a) Identified and considered significant changes in the law affecting cloud computing certification audits and auditing techniques in England and Wales
(b) Identified and considered rules relating to evidence in court proceedings with regard to logs produced by the CUMULUS infrastructure for cloud service certification.
(c) Taken into account the latest version of the CUMULUS infrastructure.

It should be noted that as in [13], our analysis focuses on the law in England and Wales and cannot be considered a complete review of all the EU Member States. While EU law may affect some aspects of cyber security, consumer protection and data protection, harmonisation is not complete and there is as yet no complete harmonisation of contract law or the law of torts (non-contractual liability/delict). Consequently, there may well be differences between Member States, which will be relevant in cases of using CUMULUS for cross-border activities. It should also be noted that rules of court procedure may be particularly vulnerable to differences in approach.

6.2. Contractual Liability

As pointed out in [13], our analysis assumes the provision of the CUMULUS infrastructure as a software product. Given this, contractual liability arises if the CUMULUS software product is defective or not fit for use as set out in the terms of the contract under which it is offered.

In general, whilst goods purchased should be of satisfactory quality; this does not mean that they must be perfect. Case law accepts that software is unlikely to be completely free of bugs, but that a degree of testing and modification may be necessary – which in the case of bespoke systems may even be a lengthy

and laborious process (see *Saphena Computing* v. *Allied Collection Agencies*[15]) – provided that the software is capable of meeting its basic purposes (*St Albans District Council* v. *ICL*[16]).

As pointed out in [13], to the extent that liability to purchasers/licensees of the software might arise from faulty software, exposure to legal liability in respect of contracts with businesses might be limited through the appropriate drafting of contractual terms. Note that ultimately the ability to exclude liability is constrained by 'reasonableness' determined by taking into account a range of factors including the bargaining position of the parties. Exclusion of liability in the case of complete failure would not be reasonable. Here one would assume that auditors using the CUMULUS infrastructure (software) to assess compliance of cloud systems are reasonably knowledgeable in the field.

Limitation on liability can also be ensured through making clear what it is realistic to expect the CUMULUS infrastructure to achieve, the level of reliability that can be expected, as well as ensuring that the way the CUMULUS infrastructure should be used (e.g., only by those trained in its use – but c.f. *SAM Business Systems Ltd* v. *Hedley*), and its limitations (circumstances in which cross-checking might be necessary, for example) are set in clear terms – see for example: *South West Water Services* v. *International Computers Ltd*[17]; *Gretton (t/a Open System Design)* v. *British Millerain Co Ltd*[18]; *Gregg & Co (Knottingley) Ltd* v. *Emhart Glass*[19]; *Southwark LBC* v *IBM UK Ltd*[20]. This position has not changed since the previous report. It is still also true that precisely where the boundary between acceptable and unacceptable lies, especially in the absence of the parties' agreement on specifications, may be uncertain. Specifications here should be understood as criteria against which the contractual performance may be assessed; they set out what the parties agree the software should be capable of doing and may be described at a greater or lesser degree of specificity.

While the Consumer Rights Act 2015 is now in force, it is unlikely to affect the consortium as the consortium will most likely be dealing with either auditors or cloud providers, both of whom will not be considered 'consumers' in respect of this software. It is only much further down the chain of provision (as described in D6.2) that consumers are likely to enter into contractual arrangements, for example the relationship between cloud provider and end-user. Even for auditors, the most likely client is a business: the cloud provider.

Case law is developing in this area but while the courts and other regulatory authorities are recognising the significance of data breach, the onus seems to be falling on the user (whether this would be cloud service provider or end user) for not keeping up to date with developments, even where the breach was as a result of a malicious cyber-attack. So far, case law has not focussed on imposing duties further up to the chain to the software developers.

Should the producers of the CUMULUS infrastructure carry out the auditing themselves, they will be providing a service – presumably to another business. Again potential exposure can be limited through the contract terms and through setting out the level of acceptable performance in the agreement with their (business) customers.

Main points:

- *The analysis of contractual liability assumes the provision of the CUMULUS infrastructure as a software product.*
- *As any software product, the CUMULUS infrastructure should be of satisfactory quality and capable of meeting its main purpose, but testing and modifications are acceptable following its sale as long as they are within reason.*

[15] [1995] FSR 616
[16] [1996] 4 All ER 481 (CA)
[17] [1999] ITCLR 439
[18] (1998) (unreported)
[19] [2005] EWHC 804 (TCC)
[20] [2011] EWHC 549 (TCC)

- *Liability can be restricted by the contract under which the CUMULUS infrastructure is offered (e.g., by specifying what should be expected of it) although this cannot be beyond 'reasonableness'.*
- *The users of the CUMULUS infrastructure, i.e., auditors and cloud providers, are unlikely to be considered as 'consumers'. Hence, new consumer legislation, as the Consumer Rights Act 2015, is unlikely to affect contractual liability the CUMULUS infrastructure.*

6.3. Non contractual liabilitity: Tortious liability and Negligence

Tortious liability and particularly the tort of negligence is one the primary examples of non-contractual liability in relation to producers or suppliers of goods and services.

Although as discussed in D6.2 [13], it is unlikely that a tortious claim could succeed, in the context of the Consumer Protection Act and 'product liability', it is worth re-emphasising the role that specifications in a contract could have in influencing the courts' understanding of what is reasonable to expect from the product, and thus the question of whether there is a defect.

Main points:

- *In the vast majority of negligence and tortious liability cases the damage done is personal injury or physical damage.*
- *The use of the CUMULUS infrastructure is unlikely to cause such types of damages.*
- *Foreseeable damages that would result from CUMULUS infrastructure failures would be pure economic loss (e.g., loss of data, breach of data security and related financial penalties).*
- *Setting clearly the expectations of CUMULUS infrastructure in a contract is important in influencing court decisions in respect of tortious liability and negligence.*

6.4. Data protection and regulatory matters

As part of our evaluation, we have also considered the Network and Information Security Directive[21] (sometimes called "NIS" or "Security Directive"), which was proposed by the European Commission in 2013 with the aim to ensure a high common standard/level of cyber security within the EU that should be adhered to by each Member State. Although the directive has not been agreed yet, there is now significant impetus to finalise its terms.

The NIS Directive aims to ensure that those within in its ambit – essentially those providing infrastructure or essential services – take measures to safeguard against security risks, specifically through risk management and information sharing.

In addition to obligations on Member States, market operators responsible for critical national infrastructure would be subject to a series of new incident reporting requirements when the NIS Directive comes into force, although the directive does not impose any specific technical requirements for this purpose. The original draft of the NIS Directive contained a non-exhaustive list of such operators, which included operators in the energy, banking, health, transport and financial services sectors as well as cloud computer services. However, the European Parliament suggested a much narrower view. It also seems that Member States will have some discretion in the way they interpret the directive in the respective national implementation measures. While it may be that cloud providers do fall within the scope of the new directive, it seems less likely that those providing software (such as the CUMULUS infrastructure) to audit those systems will be subject to the obligation imposed (i.e., the new incident reporting requirements).

Thus, our expectation is that the effect of the NIS Directive on CUMULUS would be an indirect one, i.e., making more important the role of cloud service auditing and certification. We also expect that when the directive is agreed and adopted by member states, it could create an opportunity for using CUMULUS infrastructure as a tool for detecting and reporting cloud service incidents and/or auditing and certifying the incident reporting capabilities of cloud infrastructures.

[21] http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

Main points:

- *The NIS directive and the incident reporting requirements that it aspires to establish do not have a direct implication for CUMULUS.*
- *It may, however, create opportunities for using CUMULUS infrastructure as an incident capturing and reporting tool, or auditing and certifying the incident reporting capabilities of cloud infrastructures.*

6.5. Using CUMULUS Evidence in Court

The evaluation of CUMULUS from a legal perspective has also considered the potential of using the evidence captured and produced by the CUMULUS infrastructure as evidence in a court of justice. Our evaluation in this respect has focused on the position in England and Wales.

With regards to evidence, there are two main questions:

(1) whether evidence is admissible in the first instance; and
(2) the reliability of the evidence.

Evidence must satisfy the "hearsay" rule.[22] This rule requires evidence to be given of actual knowledge rather than what a witness was told by someone else. Note also that there might be different approaches to these questions between the civil courts and the criminal courts, as standards of proof are higher in the criminal context than in the civil arena given the seriousness of a criminal charge.

What follows is a brief summary of a complex area of law.

6.5.1. Criminal Law

The Police and Criminal Evidence Act made specific provision for computer generated evidence, which required the prosecution to demonstrate that the computer had been working properly. This in practical terms is difficult because glitches may occur as a result of operator error, as well as hardware or software problems. This problematic provision was repealed placing computer generated evidence on the same footing as any other form of evidence. The Criminal Justice Act 2003 now distinguishes between information that is generated by the computer (included within a category known as 'real evidence' which the court may inspect for itself) and that which 'depends for its accuracy on information supplied (directly or indirectly) by a person'. In the latter case, evidence is not admissible as evidence unless the underlying information is proved to be accurate. With regard to this, we might distinguish between logs, which are produced automatically by the software without human intervention, which would seem to fall into the former category, and logs, which are customised. If logs are produced only on request but are the product of an automated system, which is not reliant on human information, such logs would still seem to fall in the first category.

Based on the above considerations, it would seem that logs automatically generated by CUMULUS should be admissible. Any concerns about the reliability of such logs would be exposed by examining in court the operator of the CUMULUS infrastructure and/or an expert who has examined the machine/software as to how it might function in general terms.

Main points:

- *Evidence that is automatically generated by CUMULUS infrastructure should be admissible to a court of justice in connection with a criminal case.*
- *The reliability of such evidence might need to be confirmed through examining the operator of the infrastructure and/or experts on how the infrastructure functions.*

[22] http://www.drukker.co.uk/publications/reference/hearsay/#.VbtRXvlVhBc

6.5.2. Civil Law

Evidence is governed by the Civil Evidence Act 1995, which changed the law to allow hearsay evidence, but consideration must be given as to its reliability. As regards computer generated evidence, that falls within the definition of a 'document' and documents are admissible (pursuant to s. 8). Business records under s. 9 are also admissible. Such 'documents' may still be open to challenge as to their reliability. Parties may seek to adduce evidence as to how the system works, and the operators of the CUMULUS infrastructure may also be subject to examination as to how the infrastructure was used in practice.

There is a British standard that applies to electronic information, but it relates to documents stored on electronic systems (WORM), rather than logs generated by a computer system.

Main points:

- *Evidence that is automatically generated by CUMULUS infrastructure should be admissible to a court of justice in connection with a civil law case.*
- *The reliability of such evidence might need to be confirmed through examining the operator of the infrastructure and/or experts on how the infrastructure functions.*

7. Online Survey for external Evaluators

7.1. Introduction

To maximise the evaluation scope, an online survey has been developed additionally to face-to-face evaluation workshops. Moreover the project results to be evaluated have been summarized especially for evaluators participating in the online survey, with the following material being produced:

- Introduction to CUMULUS (Presentation Slides, see [31])
- Summary of CUMULUS Project Results (Report, see [32])
- Test-based Certification (Video, see [33])
- Monitoring based certification (Video, see [34])
- Trusted Computing based certification (Video, see [35])
- CUMULUS-aware Application Engineering (Video, see [36])

The corresponding slides, document and videos are available on the CUMULUS web site, and also the online survey can be started form there: http://www.cumulus-project.eu/index.php/online-survey

Next, external stakeholders such as developers, providers and users of cloud services, evaluators and certifiers of ICT security and other experts were asked to participate in the survey by filling out an online questionnaire, with the listed material as a reference to facilitate the survey.

The survey was communicated by all project partners via direct contacts within their networks and additionally via e-mails to the external CUMULUS mailing list. The online survey officially lasted about four weeks in July 2015, but is still open from technical point of view. This way, responses have been analyzed until project end, which is reflected in this report.

The same online survey has been filled-out by Advisory Board (AB) members in the third AB workshop, after the project results had been presented and discussed face-to-face (see [37]).

The questionnaire used in the online survey is available as a separate document ([38], see also Appendix 3).

7.2. Survey Results

The first 23 questions of the online survey ask for both numeric ratings and also free text feedback. The responses have been analyzed and the results have been elaborated for each question. The results are summarized in the next table.

Question	Average Rating	Scale	Comments
1. Is the CUMULUS infrastructure sufficiently secure for realizing certification processes?	3.6	1 Not secure at all 5 Very secure	Depends on the actual implementation. Further details needed.
2. CUMULUS makes use of Trusted Computing (TC) as an optional component to secure its infrastructure. How important do you think that this is for CUMULUS?	4.2	1 Not important at all 5 Fundamental	Could be combined with other security mechanisms.

Question	Average Rating	Scale	Comments
3. Rate the expressiveness of the CUMULUS schema for specifying Test Based Certification Models	3.9	1 Not expressive at all 5 Very expressive	According to one participant, difficult to evaluate.
4. Rate the expressiveness of the CUMULUS schema for specifying the Monitoring Based Certification Models	3.8	1 Not expressive at all 5 Very expressive	According to one participant, difficult to evaluate.
5. Rate the expressiveness of the CUMULUS schema for specifying the TC Based Certification Models	3.7	1 Not expressive at all 5 Very expressive	According to one participant, difficult to evaluate.
6. Rate the expressiveness of the CUMULUS schema for specifying the Incremental & Multilayer Certification Models	4.0	1 Not expressive at all 5 Very expressive	According to one participant, difficult to evaluate.
7. Rate the expressiveness of the CUMULUS schema for specifying the Hybrid Certification Models	3.5	1 Not expressive at all 5 Very expressive	According to one participant, difficult to evaluate.
8. Rate the sufficiency of the assurance flexibility of CUMULUS	3.9	1 Insufficient 5 Fully sufficient	Unclear what is meant by assurance flexibility.
9. Rate the usefulness of the assurance flexibility of CUMULUS	4.1	1 Not useful at all 5 Very useful	Unclear what is meant by assurance flexibility.
10. How important is it in your opinion to provide support for engineering of applications that can make use of CUMULUS certificates?	4.5	1 Not important at all 5 very important	Tools are critical.
11. How adequate is the support for engineering of CUMULUS applications provided by the framework?	3.4	1 Not adequate at all 5 Very adequate	Seems very useful, but further info needed.
12. What do you think would be the cost of specifying Test based Certification Models?	2.6	1 Very high 5 Very low	Hard to quantify. Support, training, expertise needed. Re-use of existing testing knowledge possible.
13. What do you think would be the cost of specifying Monitoring based Certification Models?	2.8	1 Very high 5 Very low	See question 12. According to one participant, could be a little bit more complex than test-based.

Question	Average Rating	Scale	Comments
14. What do you think would be the cost of specifying Trusted Computing based Certification Models?	2.6	1 Very high 5 Very low	See question 12. Additional TC-specific costs not clear.
15. What do you think would be the cost of executing Test based Certification with CUMULUS?	2.9	1 Very high 5 Very low	Once implemented and set-up, the costs should be low.
16. What do you think would be the cost of executing Monitoring based Certification with CUMULUS?	2.7	1 Very high 5 Very low	Computing resources could be quite high, If done per transaction basis, the resources needed could be significant.
17. What do you think would be the cost of executing Trusted Computing based Certification with CUMULUS?	2.9	1 Very high 5 Very low	According to one participant, difficult to evaluate.
18. Rate the benefits of CUMULUS approach with respect to automating security certification	4.4	1 No benefits 5 Very high benefits	One of the key benefits, in particular for re-certification and modularity.
19. Rate the benefits of CUMULUS approach with respect to cloud service accountability	4.3	1 No benefits 5 Very high benefits	Extremely important. Increase transparency and auditability.
20. Rate the business benefits of CUMULUS approach	4.0	1 No benefits 5 Very high benefits	Depends on business benefits for whom. Small companies, new businesses, certain CSP (who want to differentiate) can profit.
21. Rate the level of risks that CUMULUS might create for your organization	3.1	1 Very high risks 5 No risks	In principle it should reduce risk. CUMULUS infrastructure must be secure, correctly configured and administered.
22. Rate your overall trust in CUMULUS certification and certificates	3.8	1 Very low 5 Very high	If correctly implemented CUMULUS can support trust establishment and maintenance.
23. How likely would it be to use CUMULUS for a pilot certification in the future?	3.4	1 Very unlikely 5 Very likely	A deeper cost and applicability analysis would have to be conducted. Depends on a level of intrusiveness (changes to an operational environment).

Table 16. Online Survey Responses

Each question shown above comes with a rating scale from 1 to 5, where 5 represents the best rating. The average rating for each question ranges from 4.5 to 2.6. Noticeable, the average rating for each question about benefits of CUMULUS (business benefits, benefits with respect to cloud service accountability, benefits with respect to automation) are 4 and higher.

The overall average rating for questions 1 to 23 is 3.6.

The free text feedback fields in the questionnaire were well-accepted by participants, which provides helpful feedback. In some cases the answers here were antithetic, which might be due to the fact that the participants represent different organization types and have different expertise. The forth column of above table reflects selected comments which the CUMULUS consortium thinks are the most relevant and helpful ones. In some cases the comment fields were used to indicate that a rating cannot be easily given due to missing information or open questions. The complete set of comments for each question is presented in [39].

The remaining questions of the questionnaire were intended to collect supplementary information about the survey participants and their background. The results are shown in the following table.

Organization Type
Nearly 50% of the online survey participants are employed at Cloud Service Providers. Other represented organization types are Other Industry, Security Certification Body, Academic and Government.
Expertise
The majority of the online survey participants have expertise as Cloud Service Provider, Cloud Service User or ICT Security Evaluator/Certifier.
Years of Professional Experience
Most of the online survey participants have more than 10 years of professional experience (71,4%). This reflects the approach to address only experts.

Table 17. Online Survey – Participants' Background

The complete result analysis is available as a separate document ([39], see also Appendix 3).

7.3. Conclusions and Next Steps

The analysis of the responses provided in the CUMULUS online survey clearly shows that such a measure is a good approach to expand the group of external evaluators, and to get expert feedback even in cases where face-to-face meetings could not be arranged. The questionnaire concept of allowing to skip answers and to add comments facilitates situations where experts cannot answer all questions or where they have additional feedback.

On the other hand the feedback to some questions also suggests that some aspects of CUMULUS cannot be easily rated in without intensive dialog between the evaluator and the CUMULUS consortium and without investing a significant effort to get familiar with CUMULUS results, which is due to the nature of the project.

In conclusion, the overall results indicate that an online survey can lead to valuable assessment feedback from important stakeholders and potential users of CUMULUS results on the one hand, but that in many cases evaluation results are more significant, if there is a direct face-to-face contact with the evaluator, such as in the two validation sessions for the CUMULUS Certification Framework (see section 3), or in the third Advisory Board workshop (see [37]).

The CUMULUS consortium and all concerned project partners have started to consider and discuss survey responses from the beginning of the survey period, since the responses have always been available online in real-time.

An update of the analysis of survey responses shall be considered shortly before the final CUMULUS project review.

Beyond that, project partners will follow up on feedback regarding their own area of expertise and project results, in the context of project exploitation and continuation of CUMULUS-related work in new projects.

8. Appendix 1 – Evaluation of Certification Framework: First Validation Session

This deliverable is presented along with some confidential annexes related to the first validation session hosted in Rome in January 13th 2015 and analyzed in section 3. These annexes are the following:

- A presentation covering an overview of the CUMULUS Project, and going into detail for the following matters: CUMULUS Framework, CUMULUS Meta Model, CUMULUS Test Based Certification Model and CUMULUS Adoption Costs and Benefits.
- A questionnaire on the topics covered by this presentation
- A presentation on the CUMULUS Monitoring Based Certification Model.
- A questionnaire on the topics covered by the second presentation.
- The feedback collected from the validators

9. Appendix 2 – Evaluation of Certification Framework: Second Validation Session

This deliverable is presented along with some confidential annexes related to the second validation session hosted in Rome in July 2nd 2015 and analyzed in section 3. These annexes are the following:

- Presentation slides introducing some specific aspects of the CUMULUS test-based certification process and the corresponding contributions to the overall CUMULUS certification assurance;
- Presentation slides introducing the CUMULUS Framework architecture and functionalities;
- A short videoclip showing the CUMULUS Framework and its Dashboard in action;
- A questionnaire on the topics covered by this presentation;
- The feedback collected from the validators.

10. Appendix 3 – Online Survey for external Evaluators

The questionnaire used in the online survey for external evaluators and the analysis of responses are available as separate documents (see [38] and [39])

11. Appendix 4 – Summary of CUMULUS Project Results

The summary of CUMULUS project results has been produced as a separate document addressed to external evaluators to facilitate their project evaluation (see [32]).

12. Appendix 5 – Mapping ENISA CCSM to Cumulus Security Properties

The following table shows the results of mapping the ENISA CCSM security objectives to the security properties elicited by Cumulus. The obtained results are discussed in Section 2.1

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
SO 01 - Information security policy	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
SO 02 - Risk management	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Supply Chain Management, Transparency and Accountability	N/A
SO 03 - Security roles	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Human Resources	N/A
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
	Security Incident Management, E-Discovery & Cloud Forensics	SEF:incident-management-quality:mean-time-between-incidents; SEF:incident-management-quality:percentage-of-timely-incident-reports; SEF:incident-management-quality:percentage-of-timely-incident-resolutions;
	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
SO 04 - Security in Supplier relationships	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Supply Chain Management, Transparency and Accountability	N/A
SO 05 - Background checks	Human Resources	N/A
SO 06 - Security knowledge and training	Security Incident Management, E-Discovery & Cloud Forensics	SEF:incident-management-quality:mean-time-between-incidents; SEF:incident-management-quality:percentage-of-timely-incident-reports; SEF:incident-management-quality:percentage-of-timely-incident-resolutions;
	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Human Resources	N/A
SO 07 - Personnel changes	Human Resources	N/A
SO 08 - Physical and environmental security	Human Resources	N/A
	Datacenter Security	DCS:integrity:authentication-feature-count; DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
SO 09 - Security of supporting utilities	Datacenter Security	DCS:integrity:authentication-feature-count; DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
	Human Resources	N/A
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
SO 10 - Access control to network and information systems	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Supply Chain Management, Transparency and Accountability	N/A
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Encryption & Key Management	EKM:key-management:cryptographic-brute-force-resistance; EKM:key-management:key-generation-quality; EKM:key-management:key-access-control-level; EKM:key-management:cryptographic-module-protection-level;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Human Resources	N/A
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
SO 11 - Integrity of network and information systems	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Encryption & Key Management	EKM:key-management:cryptographic-brute-force-resistance; EKM:key-management:key-generation-quality; EKM:key-management:key-access-control-level; EKM:key-management:cryptographic-module-protection-level;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Mobile Security	N/A
	Supply Chain Management, Transparency and Accountability	N/A
	Threat and Vulnerability Management	TVM:vulnerability-management-quality:vulnerability-exposure-level; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-corrections; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-reports;
SO 12 - Operating procedures	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Datacenter Security	DCS:integrity:authentication-feature-count; DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
SO 13 - Change management	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Datacenter Security	DCS:integrity:authentication-feature-count;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
SO 14 - Asset management	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Datacenter Security	DCS:integrity:authentication-feature-count; DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
	Human Resources	N/A
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
SO 15 - Security incident detection and response	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Security Incident Management, E-Discovery & Cloud Forensics	SEF:incident-management-quality:mean-time-between-incidents; SEF:incident-management-quality:percentage-of-timely-incident-reports; SEF:incident-management-quality:percentage-of-timely-incident-resolutions;
SO 16 - Security incident reporting	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Security Incident Management, E-Discovery & Cloud Forensics	SEF:incident-management-quality:mean-time-between-incidents; SEF:incident-management-quality:percentage-of-timely-incident-reports; SEF:incident-management-quality:percentage-of-timely-incident-resolutions;
SO 17 - Business continuity	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
SO 18 - Disaster recovery capabilities	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
SO 19 - Monitoring and logging policies	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
SO 20 - System tests	Application & Interface Security	AIS:authentication:authentication-of-data-origin; AIS:authentication:network-mutually-authenticated-client-server-channel; AIS:authentication:network-authenticated-server-access; AIS:confidentiality:external-data-exchange-confidentiality; AIS:integrity:data-alteration-detection; AIS:confidentiality:data-access-level; AIS:integrity:data-alteration-prevention; AIS:integrity:software-integrity-protection; AIS:integrity:software-integrity-detection; AIS:integrity:malware-protection;AIS:non-repudiation:non-repudiation-of-origin; AIS:non-repudiation:non-repudiation-of-receipt; AIS:information-flow-control:blacklist; AIS:information-flow-control:whitelist; AIS:auditability:percentage-of-systems-with-time-synchronization; AIS:auditability:maximum-measured-time-drift; AIS:auditability:user-traceability; AIS:auditability:security-event-storage-integrity-level;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
	Mobile Security	N/A
	Supply Chain Management, Transparency and Accountability	N/A
	Threat and Vulnerability Management	TVM:vulnerability-management-quality:vulnerability-exposure-level; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-corrections; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-reports;
SO 21 - Security assessments	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Mobile Security	N/A
	Supply Chain Management, Transparency and Accountability	N/A
SO 22 – Checking compliance	Audit Assurance & Compliance	LSC:location-control:country-level-anchoring; LSC:presonal-data-privacy:consulation-hability ; LSC:presonal-data-privacy:modification-ability; LSC:presonal-data-privacy:deletetion-ability; LSC:presonal-data-privacy:timely-access;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Encryption & Key Management	EKM:key-management:cryptographic-brute-force-resistance; EKM:key-management:key-generation-quality; EKM:key-management:key-access-control-level; EKM:key-management:cryptographic-module-protection-level;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Human Resources	N/A
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Mobile Security	N/A
	Security Incident Management, E-Discovery & Cloud Forensics	SEF:incident-management-quality:mean-time-between-incidents; SEF:incident-management-quality:percentage-of-timely-incident-reports; SEF:incident-management-quality:percentage-of-timely-incident-resolutions;
	Supply Chain Management, Transparency and Accountability	N/A
SO 23 - Cloud data security	Application & Interface Security	AIS:authentication:authentication-of-data-origin; AIS:authentication:network-mutually-authenticated-client-server-channel; AIS:authentication:network-authenticated-server-access; AIS:confidentiality:external-data-exchange-confidentiality; AIS:integrity:data-alteration-detection; AIS:confidentiality:data-access-level; AIS:integrity:data-alteration-prevention;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		AIS:integrity:software-integrity-protection; AIS:integrity:software-integrity-detection; AIS:integrity:malware-protection;AIS:non-repudiation:non-repudiation-of-origin; AIS:non-repudiation:non-repudiation-of-receipt; AIS:information-flow-control:blacklist; AIS:information-flow-control:whitelist; AIS:auditability:percentage-of-systems-with-time-synchronization; AIS:auditability:maximum-measured-time-drift; AIS:auditability:user-traceability; AIS:auditability:security-event-storage-integrity-level;
	Audit Assurance & Compliance	LSC:location-control:country-level-anchoring; LSC:presonal-data-privacy:consulation-hability ; LSC:presonal-data-privacy:modification-ability; LSC:presonal-data-privacy:deletetion-ability; LSC:presonal-data-privacy:timely-access;
	Business Continuity Management & Operational Resilience	BCR:availability:percentage-of-uptime; BCR:availability:percentage-of-processed-requests;BCR:availability:percentage-of-timely-recoveries; BCR:availability:mean-time-between-failure; BCR:recovery:recovery-point-objective; BCR:recovery:recovery-time-actual; BCR:recovery:recovery-success-ratio; BCR:resource-control:elasticity-reserved-capacity; BCR:resource-control:percentage-of-timely-provisioning-requests; BCR:resource-control:allocation-limitation; BCR:resource-control:denial-of-service-attack-resistance;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Datacenter Security	DCS:integrity:authentication-feature-count; DCS:integrity:tamper-evidence; DCS:integrity:tamper-resistance
	Encryption & Key Management	EKM:key-management:cryptographic-brute-force-resistance; EKM:key-management:key-generation-quality; EKM:key-management:key-access-control-level; EKM:key-management:cryptographic-module-protection-level;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Supply Chain Management, Transparency and Accountability	N/A
SO 24 - Cloud interface security	Application & Interface Security	AIS:authentication:authentication-of-data-origin; AIS:authentication:network-mutually-authenticated-client-server-channel; AIS:authentication:network-authenticated-server-access; AIS:confidentiality:external-data-exchange-confidentiality; AIS:integrity:data-alteration-detection; AIS:confidentiality:data-access-level; AIS:integrity:data-alteration-prevention; AIS:integrity:software-integrity-protection; AIS:integrity:software-integrity-detection; AIS:integrity:malware-protection;AIS:non-repudiation:non-repudiation-of-origin; AIS:non-

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		repudiation:non-repudiation-of-receipt; AIS:information-flow-control:blacklist; AIS:information-flow-control:whitelist; AIS:auditability:percentage-of-systems-with-time-synchronization; AIS:auditability:maximum-measured-time-drift; AIS:auditability:user-traceability; AIS:auditability:security-event-storage-integrity-level;
	Encryption & Key Management	EKM:key-management:cryptographic-brute-force-resistance; EKM:key-management:key-generation-quality; EKM:key-management:key-access-control-level; EKM:key-management:cryptographic-module-protection-level;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Identity & Access Management	IAM:identity-assurance:user-authentication-and-identity-assurance-leve; IAM:credential-security:password-storage-protection-level; IAM:account-control:percentage-of-timely-suspension-of-unused-user-accounts; IAM:account-control:limitation-of-failed-user-authentications; IAM:account-control:inactive-session-blocking; IAM:account-control:limitation-parallel-active-sessions;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Supply Chain Management, Transparency and Accountability	N/A
SO 25 - Cloud software security	Application & Interface Security	AIS:authentication:authentication-of-data-origin; AIS:authentication:network-mutually-authenticated-client-server-channel; AIS:authentication:network-authenticated-server-access; AIS:confidentiality:external-data-exchange-confidentiality; AIS:integrity:data-alteration-detection; AIS:confidentiality:data-access-level; AIS:integrity:data-alteration-prevention; AIS:integrity:software-integrity-protection; AIS:integrity:software-integrity-detection;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
		AIS:integrity:malware-protection;AIS:non-repudiation:non-repudiation-of-origin; AIS:non-repudiation:non-repudiation-of-receipt; AIS:information-flow-control:blacklist; AIS:information-flow-control:whitelist; AIS:auditability:percentage-of-systems-with-time-synchronization; AIS:auditability:maximum-measured-time-drift; AIS:auditability:user-traceability; AIS:auditability:security-event-storage-integrity-level;
	Change Control & Configuration Management	CCC:compliance-control:percentage-of-compliant-devices; CCC:compliance-control:percentage-of-compliant-software;CCC:configuration-change-control:percentage-of-timely-configuation-change-notifications; CCC:configuration-change-control:configuration-change-reporting-capability
	Data Security & Information Lifecycle Management	DSI:data-disposal:data-deletion-quality-leve; DSI:data-disposal:percentage-of-timely-effective-deletions; DSI:data-leakage-control:data-leakage-detection; DSI:data-leakage-control:data-leakage-prevention; DSI:durability:storage-freshness; DSI:durability:storage-retrievability; DSI:durability:percentage-durability;
	Governance and Risk Management	GRM:risk-control:percentage-of-systems-with-formal-risk-assessmen; GRM:risk-control:percentage-of-systems-with-tested-control;
	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability
	Interoperability & Portability	IPY:portability:data-portabilit;
	Mobile Security	N/A
	Supply Chain Management, Transparency and Accountability	N/A
	Threat and Vulnerability Management	TVM:vulnerability-management-quality:vulnerability-exposure-level; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-corrections; TVM:vulnerability-management-quality:percentage-of-timely-vulnerability-reports;
SO 26 - Cloud interoperability and portability	Interoperability & Portability	IPY:portability:data-portabilit;

ENISA CCSM	CSA Cloud control Matrix	Cumulus Security Properties
SO 27 - Cloud monitoring and log access	Infrastructure & Virtualization Security	IVS:isolation:tenant-isolation-level; IVS:isolation:colocation-indistinguishability

13. Appendix 6 – CUMULUS Engineering Tool Evaluation Questionnaire

Q1) The CUMULUS Engineering Tool (CET) offers enough engineering functionalities to incorporate security aspects in system modelling.

- ☐ I fully agree
- ☐ I mostly agree
- ☐ I neither agree nor disagree
- ☐ I mostly disagree
- ☐ I completely disagree

Q2) It is easy to apply the security knowledge from the Domain Security Metamodel (DSM) to the System Model.

- ☐ I fully agree
- ☐ I mostly agree
- ☐ I neither agree nor disagree
- ☐ I mostly disagree
- ☐ I completely disagree

Q3) It is easy to understand what security knowledge is applied to the system model (security requirements, properties, solutions).

- ☐ I fully agree
- ☐ I mostly agree
- ☐ I neither agree nor disagree
- ☐ I mostly disagree
- ☐ I completely disagree

Q4) It is easy to understand the certification assurance aspects applied to the system model.

- ☐ I fully agree
- ☐ I mostly agree
- ☐ I neither agree nor disagree
- ☐ I mostly disagree
- ☐ I completely disagree

Q5) How user-friendly is the functionality of CET?

- ☐ Extremely user-friendly
- ☐ Very user-friendly
- ☐ Moderately user-friendly
- ☐ Slightly user-friendly
- ☐ Not at all user-friendly

Q6) How successful is CET in performing its task (engineering systems security)?

- ☐ Extremely successful
- ☐ Very successful
- ☐ Moderately successful
- ☐ Slightly successful
- ☐ Not at all successful

Q7) How do you rate CET for the operations executed in this session overall?

- ☐ Excellent
- ☐ Good
- ☐ Neutral
- ☐ Poor
- ☐ Very poor

Q8) How likely is it that you would recommend CET to a friend or colleague for engineering systems security?

Not at all Extremely

0	1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Q9) Do you have any suggestions to improve CET with respect to the operations executed in this session? If yes please specify.

Q10) Are there any functionalities missing given the CET operations that you have seen in the session? If yes please specify.

Please, provide extra comments for this session, if any.

Please, specify your role in the organization.

☐ Academic: _____

☐ Industry: _____

☐ Other: _____

References

[1] ENISA: European Union Network Information Security Agency: https://www.enisa.europa.eu/

[2] Marnix Dekker, Dimitra Liveri: *Certification in the EU Cloud Strategy*. ENISA. November 2014.

[3] CCM: Cloud Control Matrix: https://cloudsecurityalliance.org/research/ccm

[4] ENISA: Security Certification Practice in the EU. Information Security Management Systems – A case study. October 2013.

[5] C.Casper, A.Esterle: Information Security Certification. A Primer: People, Products, Processes. ENISA. December 2007

[6] ISO: *Glossary of terms and abbreviations used in ISO/TC Business Plans.* http://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/Glossary.htm?nodeid=2778927&vernum=0

[7] Information Technology — Cloud Computing — Reference Architecture. ISO/IEC 17789. 2014.

[8] International Telecommunications Union: Recommendation ITU-T Y.3501 Cloud Computing framework and high-level requirements. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. May 2013

[9] Monica Lagazio, David Barnard-Wills, Rowena Rodrigues, David Wright: *Certification Schemes for Cloud Computing. European Comission*. DG Communications Networks, Content & Technology. 2014

[10] Certificate of Cloud Security Knowledge: https://cloudsecurityalliance.org/education/ccsk/

[11] Cloud Security Alliance: Requirements for bodies providing STAR Certification. 2012

[12] Cloud Security Alliance: Auditing the Cloud Control Matrix. Guidance Document. August 2013

[13] D6.2 Specification of CUMULUS evaluation criteria – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[14] Protection Profile for PC Client Specific TPM, Family 2.0, Draft Revision 0.21 (Public Review Version), June 2014, Trusted Computing Group, Incorporated

[15] Common Criteria for Information technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1 Revision 4, CCMB-2012-09-001

[16] Common Criteria for Information technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-002

[17] Common Criteria for Information technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003

[18] Information Assurance Directorate: Protection Profile for IPSec Virtual Private Network (VPN) Clients v1.1. December 2012

[19] ESM Protection Profile Technical Community: Standard Protection Profile for Enterprise Security Management Identity and Credential Management. October 2013.

[20] National Information Assurance Partnership: Protection Profile for Certification Authorities. May 2014.

[21] MSP Alliance: *10 Reasons to buy cyber liability insurance*. Available on: http://www.mspalliance.com/wp/wp-content/uploads/2008/11/Cyber10Reasons.pdf

[22] ENISA: *Cloud Certification Schemes Metaframework.* November 2014. https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework

[23] D6.1 Specification of pilot scenarios and requirements – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[24] D2.3 Certification models v.2 – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[25] ISO/IEC 27001:2005: Information technology, security techniques, information security management systems, requirements. 2013

[26] NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. April 2013

[27] FEDRAMP Public Website: http://cloud.cio.gov/fedramp

[28] Payment Card Industry Data Security Standard: *Requirements and Security Assessment Procedures*. Version 2.0. October 2010.

[29] IT Governance Institute: COBIT Framework v4.1

[30] ENISA: Information Assurance Framework. November 2009

[31] Introduction to CUMULUS (Presentation Slides), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[32] Summary of CUMULUS Project Results (Report), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[33] Test-based Certification (Video), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[34] Monitoring based certification (Video), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[35] Trusted Computing based certification (Video), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[36] CUMULUS-aware Application Engineering (Video), Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[37] D7.10 Third Advisory Board Report, Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[38] "CUMULUS Evaluation Survey" Online Questionnaire, Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), July 2015.

[39] "CUMULUS Evaluation Survey" Analysis of Responses, Project CUMULUS Grant Agreement no.: 318580 (FP7-ICT-2011-8), September 2015.

[40] D6.5 Initial evaluation report – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[41] D2.4 Final CUMULUS Certification models – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[42] D5.4 CUMULUS Infrastructure v2– Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[43] US Government Cloud Computing Technology Roadmap, Volume I, Release 1.0 (Draft). High-Priority Requirements to Further USG Agency Cloud Computing Adoption. http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf