Deliverable D7.9

Standardization Roadmap-v2

Editor(s):	Jesus Luna Garcia, Dominique Janssen
Responsible Partner:	Robert Bosch GmbH (Bosch)
Status-Version:	Final – v1.1
Date:	25.01.2024
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	Standardization Roadmap-v2
Due Date of Delivery to the EC	31.10.2023

Workpackage responsible for the Deliverable:	WP7 – Awareness, Sustainability and Standardization
Editor(s):	Jesus Luna Garcia (Bosch)
Contributor(s):	Iñaki Etxaniz (TECNALIA), Christian Banse (FhG), Thomas Ruebsamen (Bosch), Dominique Janssen (Bosch)
Reviewer(s):	Juncal Alonso (TECNALIA) Cristina Martinez (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	Recommended for WP2 – WP6

Abstract:	This deliverable presents the final status of relevant activities performed in the context of standardization and standards observation during the duration of the MEDINA project.
Keyword List:	Standardization, EUCS, EU CSA, OSCAL
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein.

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	08.07.2023	First draft version	Bosch
v0.4	01.09.2023	Second draft version	Bosch, TECNALIA, Fraunhofer
V0.7	03.10.2023	Final draft ready for internal review	Bosch
v0.8	16.10.2023	Internal review	TECNALIA
v0.9	18.10.2023	Addressed all comments received in the internal QA review	Bosch
v1.0	31.10.2023	Ready for submission	TECNALIA
v1.1	24.01.2024	Revised based on feedback from reviewers	Bosch

Table of Contents

Terms and abbreviations 7
Executive Summary 8
1 Introduction 9
1.1 About this deliverable 9
1.2 Relevant updates since Deliverable 7.8 (M18) 9
1.3 Addressing the Recommendations from Reviewers 10
1.4 Document structure 11
2 Updated Approach to Standardization in MEDINA 12
2.1 Rationale 12
2.2 Influence of Revised Standardization Roadmap 12
2.3 Engagement with ESG, StandICT.eu and HSBooster.eu 13
3 Standardization Roadmap (Final version) 16
3.1 Scoping the Standardization Roadmap 16
3.1.1 Pillar One: EUCS 16
3.1.2 Pillar Two: Cybersecurity Compliance Metrics 17
3.1.3 Pillar Three: Automation of Cybersecurity Compliance Monitoring 17
3.2 Final Roadmap for Standardization 18
4 Updated Report on MEDINA's Standardization / Best-Practices Activities 20
4.1 EUCS-Related Activities 20
4.1.1 Recap of ENISA AHWG 20
4.1.2 Contribution to Thematic Groups (TG) of EUCS 21
4.1.3 CEN CENELEC JTC13 WG2 (EUCS1) 27
4.1.4 CISCO CCF 29
4.1.5 Future Work on EUCS Standardization 30
4.2 Metrics-Related Activities 31
4.2.1 Performance Measurement Guide for Information Security (NIST 800-55 release 2) 31
4.2.2 Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (ISO/IEC 27004) 31
4.2.3 Future Work on Metrics for Compliance 32
4.3 Automation-Related Activities 32
4.3.1 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017) 32
4.3.2 Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security (ISO/IEC 20078-3:2021) 34
4.3.3 Open Security Controls Assessment Language (NIST OSCAL) 34
4.3.4 The Gaia-X Initiative 37

4.3.5 Future Work on Automation for Compliance Monitoring 37
5 Conclusions 39
References 41
APPENDIX A: The Approach to Standardization in MEDINA (excerpt as originally reported in D7.8) 43
APPENDIX B: Standardization Roadmap (excerpt as originally reported in D7.8) 44
APPENDIX C: Signed Memorandum of Understanding with StandICT.eu 46
APPENDIX D: TG2 Contribution Sample – CSEP Proof of Concept 47
APPENDIX E: TG8 Contribution Sample – EUCS Guidance for Category CKM 48
APPENDIX F: Contribution to EUCS1 on Continuous Automated Monitoring 51
APPENDIX G: Contribution to NIST SP 800-55 Rev. 2 52
APPENDIX H1: Contribution to ISO/IEC 27017 on Automated Configuration Monitoring 53
APPENDIX H2: Contribution to ISO/IEC 27017 on Automated Monitoring Annex 54
APPENDIX I: Contribution to ETSI DTR/CYBER-0087 55

List of Tables

TABLE 1. CHANGE LOG FOR D7.9 WITH RESPECT TO D7.8 [1] 9
TABLE 2. MEDINA STANDARDIZATION ROADMAP (FINAL VERSION) 19
TABLE 3. ENISA EUCS' THEMATIC GROUPS (FINAL) 21
TABLE 4. STAKEHOLDER RECOMMENDATIONS RELATED TO STANDARDIZATION IN MEDINA 40
TABLE 5. MEDINA ROADMAP (D7.8 [1]) 44
TABLE 6. MEDINA COMMENTS RELATED TO "CSEP POC" 47
TABLE 7. MEDINA FEEDBACK SUBMITTED TO ENISA AD HOC WG EUCS TG8 (EXCERPT) 48
TABLE 8. MEDINA COMMENTS RELATED TO "ETSI DTR/CYBER-0087" 55

List of Figures

FIGURE 1. REVISED STANDARDIZATION APPROACH 12
FIGURE 2. FEEDBACK RECEIVED DURING 3RD ESG MEETING 14
FIGURE 3. PROGRESS ON EUCS AS REPORTED BY ENISA TO THE AHWG (SOURCE: ENISA) 21
FIGURE 4. PROCESS OF DEVELOPING A CERTIFICATION SCHEME (SOURCE: ENISA [13]) 22
FIGURE 5. TG2 REQUIREMENTS FROM EUCS INTEGRATED INTO MEDINA'S CATALOGUE 23
FIGURE 6. MEDINA'S ORCHESTRATOR IMPLEMENTING TG3'S NOTION OF CERTIFICATE LIFECYCLE MANAGEMENT. 24
FIGURE 7. TG8 IMPLEMENTATION GUIDANCE INTEGRATED INTO THE MEDINA'S CATALOGUE 25
FIGURE 8. TG8 IMPLEMENTATION GUIDANCE LINKED BY THE CCE COMPONENT 25
FIGURE 9. MEDINA'S CONTRIBUTION TO TG9 BEING DISCUSSED WITH THE AHWG DURING THE EUCS SUMMIT 26
FIGURE 10. TG9 QUESTIONNAIRE INTEGRATED INTO THE MEDINA FRAMEWORK 27
FIGURE 11. FINAL AGREEMENT ON EUCS1 28
FIGURE 12. FINAL AGREEMENT ON EUCS1 AUTOMATED MONITORING 29
FIGURE 13. MAPPING CISCO CCF TO EUCS (MEDINA INTEGRATION INTO CATALOGUE). 30
FIGURE 14. REQUEST FOR REVISION OF ISO/IEC 27004:2016 32
FIGURE 15. SUCCESSFUL MEDINA CONTRIBUTION TO ISO/IEC 27017 33

FIGURE 16. LEVERAGING OSCAL IN EUCS USING THE MEDINA FRAMEWORK (ETSI TR 103 923 DRAFT) 35
FIGURE 17. EUROSCAL LANDING PAGE AT WWW.EUROSCAL.EU 36
FIGURE 18. MEDINA'S APPROACH TO STANDARDIZATION (D7.8) 43

Terms and abbreviations

AI	Artificial Intelligence
AHWG	AdHoc Working Group
AISBL	Association Internationale Sans But Lucratif
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Conformance Assessment Body
CAM	Continuous Automated Monitoring
CCF	Cloud Controls Framework
CCM	Cloud Controls Matrix
CEN CENELEC	European Committee for Electrotechnical Standardization
CSA or EU CSA	EU Cybersecurity Act
CSP	Cloud Service Provider
DIN	Deutsches Institut für Normung
DoA	Description of Action
EC	European Commission
EUCS	EU Cybersecurity Certification Scheme for Cloud Services
ENISA	EU Agency for Cybersecurity
ESG	Expert Stakeholder Group
ETSI	European Telecommunications Standards Institute
GA	Grant Agreement to the project
IPR	Intellectual Property Rights
ISO/IEC	International Standards Organization / International Electrotechnical Commission
KPI	Key Performance Indicator
ISACA	Information Systems Audit and Control Association
NIST	National Institute of Standards and Technology
SDO	Standards Development Organization
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprises
SSO	Standards Setting Organization
SW	Software
TG	Thematic Groups
TOM	Technical and Organizational Measure
TS	Technical Specification
OSCAL	Open Security Controls Assessment Language
POC	Proof Of Concept
WG	Working Group
WP	Work Package

Executive Summary

This deliverable reports the final MEDINA's standardization activities performed during the second half of the project's lifetime (M19-M36). Obtained results are presented along with a summary of the discussions held with the engaged Standardization Development Organizations. Where applicable, this report updates the content of its predecessor "D7.8 Standardization Roadmap-v1" [1] so it can be considered a self-contained document. MEDINA's revised Roadmap takes a central role in the present report, as it serves to structure the presentation of contributions performed by the consortium in "pillar" topics needed for rolling out the notion of continuous (automated) cloud cybersecurity certification in the EU. Finally, we also include a series of recommendations targeting relevant standardization stakeholders (including ENISA, and Conformance Assessment Bodies), with the goal of enabling future usage of the MEDINA framework. Documented recommendations are part of MEDINA's sustainability actions and will be follow-up in upcoming activities from consortium's partners, including the Horizon Europe-funded projects COBALT and EMERALD.

1 Introduction

This section provides an updated overview of the content in this deliverable along with the main changes with respect to the previous release [1].

1.1 About this deliverable

During the duration of MEDINA, the topic of standardization played a central role given our goal to support the uptake of the new EU Cybersecurity Certification Scheme for Cloud Services (EUCS). By developing and adopting a two-facet strategy for standardization, where on one hand we constantly surveyed the standardization landscape (including industrial good practices) to ensure interoperability and freshness of the framework. And on the other hand, MEDINA actively contributed to a very specific set of initiatives identified in the so-called "Standardization Roadmap" [1]. Engaged initiatives referred not only to the activities of established Standards Developing Organizations (SDOs like ISO/IEC and ETSI), but also to those taking place within Standards Setting Organizations (SSOs e.g., ENISA). In both cases fruitful/efficient synergies were established, and are reported in the present deliverable.

This self-contained deliverable covers the whole duration of MEDINA and presents the methodological approach to internally leverage and influence relevant initiatives on the topic of continuous (automated) cybersecurity certification. Furthermore, it updates the proposed standardization Roadmap by identifying three main "pillars" in our strategy namely EUCS, cybersecurity compliance metrics, and automation of compliance assessments. Those foundations were identified during the execution of MEDINA, mainly thanks to the feedback received from the MEDINA ESG (Expert Stakeholder Group), external dissemination events, and engagements with the EU-funded projects HSBooster.eu [2] and StandICT.eu [3].

Based on the developed standardization Roadmap, this deliverable also reports the corresponding standardization activities where interactions with relevant organizations (e.g., ENISA, NIST, CEN CENELEC, ETSI and ISO/EC) took place. The final version of MEDINA's standardization Roadmap aims to support sustainability of the proposed framework by providing a set of recommendations for relevant stakeholders to accomplish our ultimate goal of **leveraging automation, ensuring compliance, and enhancing trust**.

1.2 Relevant updates since Deliverable 7.8 (M18)

This deliverable is a self-contained document which incrementally updates the content of previous D7.8. For the sake of readability, the following table summarizes the main changes and updates performed to each one the sections in the present report.

Table 1. Change log for D7.9 with respect to D7.8 [1]

Section	Change
Section 2	The initially documented standardization approach is updated by presenting its evolution during the execution of the Roadmap, together with the engagement activities taking place in HSBooster.eu [2] and StandICT.eu [3]
Section 3	The final version of the standardization Roadmap is presented, which updates the one introduced in D7.8 by clustering the performed activities in three pillars designed to support both MEDINA's framework uptake and the topic of continuous (automated) certification.
Section 4	MEDINA's standardization engagements are aligned according to the same pillars/topics of our updated Roadmap. Furthermore, updated

Section	Change
	status of performed contributions to standards is reported.
Section 5	The conclusions from D7.8 are updated, and new content related to both sustainability and stakeholder recommendations is added.

1.3 Addressing the Recommendations from Reviewers

In this section are addressed the recommendations kindly provided during the project's first review meeting.

Recommendation 6 – Self-contained deliverables

The deliverables should be self-contained as much as possible. In this reporting period, deliverable D2.3 is an example of a deliverable that is very brief and would benefit from additional explanations.

Response from D7.9: The present deliverable is an incremental update of D7.8 [1] to make it a self-contained document, while at the same time making evident the new content based on the project's progress achieved during the second-half of its execution.

Recommendation 12 – Patents and standardization groups (WP7)

In terms of dissemination and exploitation, the decision of (not) patenting and the inclusion of essential patents in standardisation group should be elaborated, as well as mitigation actions against competition, e.g., publication of key results to have them in the public domain. The possibility to open upcoming native Cloud Provider tools to the tools delivered by the project thru standardisation or regulation should be addressed.

Response from D7.9: Specific activities aimed to disseminate key results, but without compromising the identified exploitable results, are reported in Deliverable D7.7 [4]. From a standardization perspective, performed activities have influenced relevant initiatives (including those from ENISA, ISO/IEC and NIST) towards paving the road for MEDINA's framework on continuous compliance monitoring. Tool development has been also influenced by MEDINA research, where EU-initiatives like Gaia-X have been a strategic target of the project. Further details are reported in Section 4 of the present deliverable.

Recommendation 21 – Standardization (WP7)

Concerning the deliverable D7.8 which is excellent and as discussed during the review meeting, the standardization landscape related to MEDINA could also include ISO 20078-3:2021 -Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security. It is suggested to explore this for the delivery of D7.9.

Response from D7.9: Despite the referred standard could not be contributed during the duration of the project (final revision dates from November-2021[1]) it is true that MEDINA's framework is flexible enough to cover non-EUCS certification schemes nor cloud security standards. As far as the "Generic Evidence Collector" [5] can be deployed in the Target of Evaluation, then it would be feasible to continuously monitor compliance notwithstanding the underlying technology (e.g., cloud, IoT, or smart vehicles). As a matter of fact, non-cloud use cases (namely Artificial Intelligence and Quantum Computing) leveraging core functionality of the MEDINA framework

[1] Please refer to https://www.iso.org/standard/80185.html

will be demonstrated in the upcoming Horizon Europe COBALT project. Further details on this respect are provided in Section 4.3.2.

Recommendation 22 – Risk on Cloud Providers' native tools (WP7)

Although identified in Risk 21, mitigation of the risk of being locked out of Cloud Providers' integrated native tools could be addressed.

Response from D7.9: Standardization activities in MEDINA have focused on three main topics which on one hand seek to enable continuous (automated) certification, and on the other hand to enhance interoperability (thus avoiding vendor lock-in). Example of these activities are EUROSCAL[2] (and contribution to OSCAL in general), the definition of standardized metrics for compliance, and the definition of a CAM tool based on MEDINA research (now under the Eclipse Foundation).

Recommendation 26 – New standardization strategies (WP7)

The Standardisation objectives are mainly related to scouting and influencing, and would benefit in the future of a documented position with respect to more aggressive strategies such as the introduction of essential patents or key technologies to gain an exploitation advantage.

Response from D7.9: As described above in Recommendation 12, the introduction of Key Results was driven by the project's exploitation activities as reported in Deliverable D7.7 [4]. These resulted in technological enablers being driven by project partners in initiatives like Gaia-X[3] (Fraunhofer), and EUROSCAL (Bosch and TECNALIA). These actions will continue after MEDINA has finalized and thanks to spin-off Horizon Europe innovation projects COBALT and EMERALD. Furthermore, our project's standardization activities were consulted with the Expert Stakeholder Group (ESG) on approaches to maximize the impact of the proposed framework. As a result, the standardization Roadmap was adapted to influence relevant stakeholders (in particular Regulators) in enabling processes and key technologies for continuous (automated) certification. Furthermore, based on feedback received from the HSBooster.eu's expert, the project's standardization activities kept focus on relevant initiatives (please refer to Section 3 and Section 4) and not the development of patents where IPR challenges could have appeared. Nevertheless, patent developing will take a primary role on upcoming Horizon EU innovation actions COBALT and EMERALD (both of which are participated by current MEDINA partners).

1.4 Document structure

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

- Section 2 updates the methodological approach developed by MEDINA to adopt/influence both SDOs and SSOs.
- Section 3 presents the final version of MEDINA's standardization Roadmap.
- Section 4 reports the project's contributions and engagements with relevant standardization initiatives.
- Finally, Section 5 presents our conclusions, stakeholder recommendations, and future work.

[2] Please refer to https://euroscal.eu/
[3] Please refer to https://gaia-x.eu/

2 Updated Approach to Standardization in MEDINA

The revised approach to standardization is presented in this section.

2.1 Rationale

During the first half of the project's lifetime, MEDINA's standardization activities focused on three main actions namely scouting, influencing and transferring. These were originally reported in Deliverable D7.8 [1] (also included in *APPENDIX A: The Approach to Standardization in MEDINA (excerpt as originally reported in D7.8) f*or readers' convenience). During the second half of MEDINA's execution, our standardization approach was updated to reflect feedback from the Expert Stakeholder Group (ESG), relevant EU-projects engagements (StandICT.eu[4] and HSBooster.eu[5]), and the execution of the standardization Roadmap. A graphical representation of the updated approach can be seen in Figure 1 and is discussed in the rest of this section.

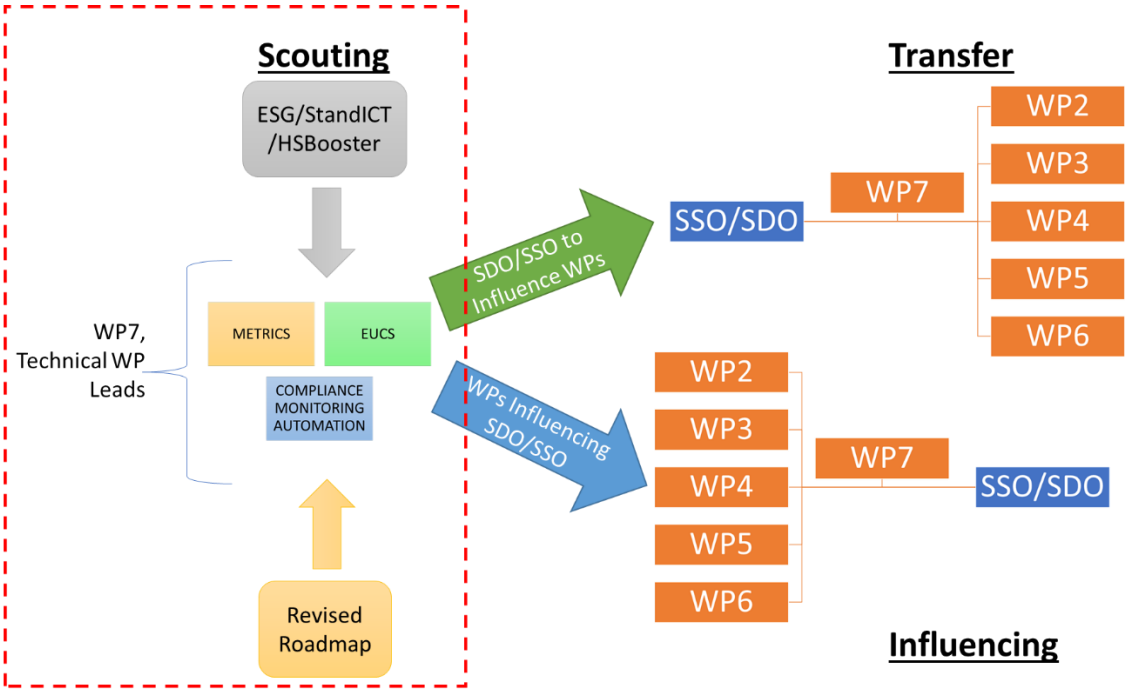

Figure 1. Revised standardization approach

2.2 Influence of Revised Standardization Roadmap

MEDINA's standardization Roadmap (originally presented in D7.8 [1]), covered a range of standardization initiatives which were identified as high-impact ones based on our "Scouting" approach. Once a relevant initiative was identified, the proposed approach managed it in any of two different manners namely "Influence" or "Transfer". In contributing project results to standardization initiatives, it became clearer that the initially scouted topics could be further scoped in EUCS, compliance metrics, and compliance monitoring automation to maximize the project's impact. A similar experience came with the "Transfer" part of the proposed approach, where contributions resulting from MEDINA's technical activities were used to influence selected standardization initiatives (e.g., the self-assessment questionnaires created by MEDINA, which were contributed to ENISA's EUCS as presented in Section 4.1).

[4] Please refer to https://standict.eu/
[5] Please refer to https://www.hsbooster.eu/

The need for scoping took our standardization activities to refine MEDINA's originally proposed standardization Roadmap, and in consequence also the adopted approach. The former will be presented in Section 3, whereas in the left-side of Figure 1 can be observed the changes affecting our standardization approach. Notice how our Scouting activities (and in consequence also our SDO-engagements) where positively affected by focusing on the three topics from the revised Roadmap. We refer not only about making more efficient use of allocated resources (consider that relevant initiatives like EUCS1[6] standardization by CEN CENELEC took more than 18 months to be achieved), but also by having a greater impact and positioning MEDINA in core topics like compliance monitoring automation where spin-off activities like EUROSCAL[7] where triggered.

A summary of our main contributions to standards (categorized according to the revised Roadmap's topics, and leveraging the approach presented above) will be presented in Section 4.

2.3 Engagement with ESG, StandICT.eu and HSBooster.eu

As seen in Figure 1, our originally proposed standardization approach was also revised based on external feedback. We refer in particular to discussions held within our Expert Stakeholder Group (ESG), and active *service* engagements with both StandICT.eu [3] and HSBooster.eu [2]. Further details are provided next.

Feedback from the ESG was requested during the virtual meeting held on April-25th 2023, where the standardization Roadmap was presented and discussed with the experts (including German BSI, US NIST, CEN CENELEC, and ENISA). Our three main standardization topics (i.e., EUCS, Metrics and Automation) were supported by the ESG (see Figure 2), although there was a general opinion that major focus should be given to both EUCS and automation. The topic of metrics for EUCS compliance was also considered important for the uptake of MEDINA, however the experts saw it has a challenge to be addressed after EUCS is released. Furthermore, there was consensus on the need to further explore automation topics related to OSCAL as presented later in Section 4.3. Feedback from the ESG was considered and dully integrated into the revised versions of both roadmap and standardization approach. Further details associated to this meeting can be found in the corresponding MEDINA blogpost [6].

[6] The technical specification EUCS1 (Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services) is developed by CEN CENELEC under mandate of the European Commission to standardize the requirements from EUCS. More in Section 4.1.3

[7] Please refer to https://euroscal.eu/

Figure 2. Feedback received during 3rd ESG meeting

Similarly, MEDINA also received support from the EU-funded StandICT.eu [3] and HSBooster.eu [2] projects. The former had as goal to support EU in having presence in the international ICT standardization scene. HSBooster.eu provides expert services to EU projects to help them increase and valorise project results by contributing to the creation / revision of standards. In the case of StandICT.eu project there was a Memorandum of Understanding (MoU [7], see *APPENDIX C: Signed Memorandum of Understanding with StandICT.eu*) signed by both initiatives to cooperate on activities connected to the "EUOS – European Observatory for ICT Standardisation." MEDINA supported the creation of EUOS (e.g., cloud security and certification topics) and provided support in creating synergies with other projects and initiatives active in the ICT standardisation domain. Example of those synergies where MEDINA's engagement with CYRENE [8], where our standardization approach was presented, and feedback was gathered from the audience.

Another important collaboration resulting from the MoU with StandICT.eu was the one developed with HSBooster.eu [2]. In this case MEDINA requested support from the offered expert services, which resulted in being consulted by Mrs. Juozapaitienė, who specializes in cybersecurity standardization topics and is part of HSBooster.eu's pool of expert advisors [9]. During the period March – September 2023, out project received a total of three consulting sessions (overall 3 hrs) via teleconference with Mrs. Juozapaitienė. The main discussion was first on refining the project's approach to standardization and its proposed Roadmap, where we confirmed our decision to keep scoped in the referred topics of EUCS, metrics, and automation. Related to the latter, we were advised to trigger a so-called CENELEC Workshop Agreement (CWA) to build a community of experts to discuss OSCAL and its support to compliance automation. In this particular case, MEDINA decided for a more community-driven approach (EUROSCAL) which will be presented in Section 4.3.3.2[8]. Furthermore, we also consulted our assigned expert on how MEDINA could approach the topic of patents from a standardization perspective (based on feedback from the first project's review meeting). Given the potential IPR incompatibilities between MEDINA's contribution to standards and potential patents, and the planning which could be required within the project's lifetime, it was decided that this venue would not be followed. However, the expert also agreed that upcoming EU-funded projects

[8] This decision also obeyed avoiding conflict of interest and overlaps between similar initiatives being supported by US NIST and ETSI Cyber, as seen in Section 4.3

EMERALD and COBALT[9] could explore the topic of patenting given their strong commitment to innovation.

All in all, the feedback from experts was taken into consideration for revising not only the presented approach to standardization, but also MEDINA's Roadmap to standardization as shown in the following section.

[9] Both projects were funded under the call HORIZON-CL3-2022-CS-01-04, however at the time of writing none of these has yet started. Therefore further details are not available beyond those shown in https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard

3 Standardization Roadmap (Final version)

Next, we present the revised standardization Roadmap, which departs from the one originally proposed in Deliverable D7.8 [1] (excerpt shown in *APPENDIX B: Standardization Roadmap (excerpt as originally reported in D7.8*) for the sake of completeness) and was updated based on MEDINA's standardization engagements and refined approach.

Not to forget is that the revised Roadmap kept being a "guiding light" not only for MEDINA's standardization activities taking place during the project's lifetime, but also as future sustainability guide.

3.1 Scoping the Standardization Roadmap

In analogy to MEDINA's standardization approach, the Roadmap also became a living document which was maintained and updated during the duration of the project. Furthermore, based on the very same external feedback described in Section 2.3 the Roadmap was also restructured in the following three topics:

1. EUCS
2. Cybersecurity Compliance Metrics
3. Automation of Cybersecurity Compliance Monitoring

Details associated to each one of these "pillars" will be presented below, including a glimpse on planned sustainability actions to take place after the finalization of MEDINA.

3.1.1 Pillar One: EUCS

While executing the standardization approach with the Roadmap initiatives identified in Deliverable D7.8 [1], we realized that major efforts needed to be invested in the finalization of EUCS, which has been delayed due to multiple factors. Not only EUCS is central for MEDINA, but it also represents a major step in the direction of continuous (automated) monitoring as required for the uptake of MEDINA's framework. It became clear that EUCS (and the related activities presented in Section 4.1) should be a priority in the Roadmap, so adequate efforts could be invested.

Standardization initiatives related to this pillar included on the one hand those driven by ENISA in its corresponding Ad-Hoc Working Group (AHWG), and on the other hand those delegated to CEN CENELEC in its role of EU-standardization body nominated for developing the companion technical specifications. EUCS-related initiatives have been developing in parallel to MEDINA, which gave our project the unique opportunity to showcase its key results and influence selected topics thanks to our close collaboration with ENISA. Special emphasis was put by MEDINA's standardization activities on refining and supporting the notion of "continuous (automated)" monitoring, which was seen as a disrupting notion in EUCS and therefore required major efforts from our side to guarantee its place on the final version of the corresponding CEN CENELEC technical specification.

It is our belief that EUCS will become a game changer in the field of cybersecurity certifications for cloud services not only in the EU, but also internationally. Therefore, part of MEDINA efforts on this pillar were also devoted to influencing well-known industrial activities like Cisco Cloud Controls Framework [10], where mappings to EUCS were contributed and fruitful discussions took place in the ESG[10].

[10] Mr. Prashant Vadlamudi, creator of the CISCO CCF is part of MEDINA ESG.

As in the case of the other two pillars in our standardization Roadmap, selected project partners (in particular Bosch, TECNALIA, and Fraunhofer) are expected to keep contributing to EUCS activities even after the finalization of MEDINA.

Further details in MEDINA contributions to EUCS are provided in Section 4.1.

3.1.2 Pillar Two: Cybersecurity Compliance Metrics

As in the case of the EUCS topic, similar situation occurred with the next identified pillar: cybersecurity compliance metrics. Here, the technical team in MEDINA came fast to the realization that the notion of metrics is core for enabling automation in certification processes. However, equally important was our observation that non-standardized metrics would contribute nothing to the envisioned EUCS-ecosystem, but by the contrary they could introduce fragmentation in the way automated compliance assessments were supposed to happen. If every cloud service provider adopts its own/proprietary metrics, then comparability and assurance would be negatively affected. Therefore, our Roadmap was modified to prioritize the topic of cybersecurity metrics for compliance.

Despite the notion of cybersecurity metrics has existed for a long time, we found that having it applied to "compliance assessments" (as expected in certification processes linked to EUCS) was not yet fully embraced by the community. There are still some misconceptions about the role of metrics for compliance and how they differ from more "traditional" cybersecurity metrics. Notwithstanding these challenges, MEDINA's Roadmap was scoped in identifying relevant standardization initiatives where impact of our key results could be maximized. In this field we engaged with NIST while revising their corresponding standard (see Section 4.2.1), and at the time of writing we were waiting to start collaborating on the revision of the corresponding ISO/IEC standard (see Section 4.2.2).

Having *standardized* metrics associated to EUCS (and re-mapped to other controls frameworks) will greatly benefit the uptake of MEDINA's technical key results and at the same time, such metrics will enhance assurance and comparability among the cloud ecosystems. It is our expectation that once EUCS is live (estimated between 2024-2025 according to the latest information from ENISA on the AHWG), we can start working on contributing the corresponding metrics developed by MEDINA [11] as part of the project's sustainability actions.

More details about specific MEDINA contributions to standards in the field of metrics for compliance can be found in Section 4.2.

3.1.3 Pillar Three: Automation of Cybersecurity Compliance Monitoring

Last, but not least is the final pillar in the revised approach namely "automation of cybersecurity compliance monitoring". In this case our interaction with the ESG (where ENISA, BSI and US NIST are members), supported us to confirm that automation and involvement of Regulators are essential for the future adoption of MEDINA. An interoperable and standardized Automation approach can per-se solve technological challenges identified in MEDINA, however the lack of acceptance from Regulators can only bring few steps forward our key results. Having Regulators aware and engaged into the benefits that automation can bring to existing (EUCS) certification processes is seen as a necessary step for achieving the ultimate vision of MEDINA. Given promising results obtained using OSCAL [12] in the FedRAMP certification scheme in the US[11], our project decided to revise its Roadmap by including this pillar.

[11] Please refer to https://cloud.google.com/blog/products/identity-security/announcing-google-cloud-first-complete-oscal-package?hl=en

Once this topic was added to our Roadmap, the presented MEDINA's Standardization Approach was triggered (see Section 2) and the corresponding "scouting" actions started. As an outcome, the project identified NIST OSCAL as a promising initiative with the unique potential of influencing industrial stakeholders and Regulators towards adopting automation for implementing continuous compliance processes. Furthermore, MEDINA identified "satellite" OSCAL initiatives driven by relevant SDOs like ETSI, where our project's contribution was much appreciated by the editors. As presented later on this deliverable, given the open collaboration and discussions maintained between MEDINA – NIST – ENISA on the OSCAL topic and its relevance for EUCS (and other cybersecurity certification schemes from Member States like the German BSI C5), it was decided to further explore OSCAL as an exploitation venue for partner Bosch which in consequence released the EUROSCAL initiative. This community-driven activity is expected to become a sustainability action from MEDINA to provide fruitful discussions and ad-hoc collaborations to start empowering industry, CABs, and Regulators on the use of automation for cybersecurity certification processes.

More details on MEDINA's contribution to relevant standards related to this third Roadmap pillar can be found in Section 4.3.

3.2 Final Roadmap for Standardization

Based on the arguments presented so far, which resulted in focusing standardization efforts on three well-identified "pillars", the revised (and final) version of MEDINA's standardization Roadmap is shown in Table 2. It is important to notice that *all* topics from the original Roadmap have been covered on this revised version, but more important is the way they have been reorganized to allow scaling and integrating new standardization topics even after the finalization of MEDINA[12].

Furthermore, our revised Roadmap also shows the standards and related initiatives where MEDINA contributions succeeded and brought value to refine the project's technical activities. More details on each one of the referred standards can be found in Section 4.

Finally, MEDINA's standardization Roadmap also summarizes the actual engagement / contribution provided by the consortium by following the Standardization Approach presented previously on this deliverable. MEDINA contributions are also phrased in terms of the benefit they brought to the project, in particular considering the number of experts reached by these activities and the sustainability actions which were generated (in particular EUROSCAL). As mentioned earlier in this section, our Roadmap was not only used to advise the project's tasks during MEDINA's lifetime, but it can be also used to guide future activities on this field.

[12] This is an action planned to be follow-up by the new Horizon Europe project COBALT, where MEDINA partners Bosch and Fraunhofer participate.

Table 2. MEDINA Standardization Roadmap (final version)

Roadmap Topic (Revised)	Rationale	Contributed MEDINA Standards	Summary of MEDINA Contributions / Benefit	Mapping to Roadmap v1 (see Appendix A)
EU Cybersecurity Certification Scheme for Cloud Services	EUCS is central notion in MEDINA, around which the overall framework has been built (even though it can be extended to other cybersecurity certification schemes). EUCS natively integrated the notion of continuous (automated) monitoring.	ENISA AHWG thematic groups on assurance levels, security controls, assessment methods, guidance, and self-assessment questionnaire. CEN CENELEC JTC13 WG2 – EUCS1 Cisco CCF	Notion of continuous compliance monitoring maintained in EUCS and the corresponding CEN CENELEC specification. MEDINA framework widely disseminated in the ENISA AHWG and related certification community. Feedback compiled from relevant industrial stakeholders and Regulators was used to improve the framework.	*Provide implementation guidance about EUCS requirements where some degree of automated monitoring is needed.* *Provide audit/assessment guidance related to EUCS requirements needing some degree of automated monitoring.*
Cybersecurity Compliance Metrics	Metrics are an essential enabler in the MEDINA framework for implementing continuous compliance monitoring and (EUCS) certification	NIST 800-55 ISO/IEC 27004	MEDINA catalogue of Metrics contributed to NIST as a proof of concept that compliance can be achieved with metrics. This notion will be extended on the planned contribution to ISO/IEC.	*Provide a catalogue of metrics as part of the implementation guidance for EUCS.*
Automation of Cybersecurity Compliance Monitoring	Automation is the third identified standardization pillar as required to support uptake of MEDINA's framework. The notion of automation for compliance/certification processes is novel for SDOs.	ISO/IEC 27017 NIST OSCAL ETSI CYBER OSCAL Gaia-X Initiative	MEDINA's framework as a proof of concept that automation for purposes of compliance is possible. This eased successful contribution to relevant international initiatives. EUROSCAL is created for supporting adoption of OSCAL automation in Europe.	*Support the notion of continuous (automated) assessments.* *Support development of machine-readable formats.* *Guidance on selecting tools/technologies for automated (continuous) monitoring.*

4 Updated Report on MEDINA's Standardization / Best-Practices Activities

This section provides an incremental update of the consortium's activities with relevant SDO/SSO initiatives, which took place during the second half of MEDINA's duration. For the sake of consistency and readability, reported activities are structured according to the three main "pillars" identified in our Roadmap (see Section 3) and complement those discussed in D7.8 [1]. As feasible, this section also provides or references evidence associated to MEDINA's contributions to standards, although most SSOs keep that information as confidential (e.g., ISO/IEC and CEN CENELEC). Finally, please also notice that due to internal SDO rules it was not always feasible to include the relevant EU acknowledgement on the provided contributions (instead only the expert/Member State contributor can be found).

4.1 EUCS-Related Activities

Probably the most relevant standardization activity from the MEDINA perspective is the one being led by ENISA on the topic of EUCS because it represents the foundation of our project. The novel EUCS notion of continuous (automated) compliance monitoring has greatly influenced our contributed framework.

4.1.1 Recap of ENISA AHWG

On March 2020, ENISA launched the so-called ad-hoc working group (AHWG) to support the European Commission (EC) in preparing the draft candidate cybersecurity certification scheme for cloud services (EUCS[13]).

Twenty (20) members were selected "*according to the highest standards of expertise, aiming to ensure appropriate balance according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry, users, and academic experts in network and information* security"[14].

According to the terms of reference in the call for candidates, the group of experts was expected to provide ENISA with input on the scope, purpose, requirements, assurance level definitions, conformity assessment methodologies and monitoring of the compliance, statement of conformity, and certification lifecycle related to the novel EUCS.

Out of the twenty selected members, MEDINA's technical manager (Dr. Jesus Luna Garcia, Bosch) was part of the AHWG. The work in the AHWG of ENISA has been distributed in Thematic Groups (TG), which are dedicated sub-groups working extensively and exclusively in specific topics as needed by the certification scheme. At the time of writing the AHWG activities are expected to be extended -at least- until 2026 as seen in Figure 3. Our project's engagement activities with those TG are reported next.

[13] https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG02

[14] https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG02/tor_ahwg02_cloud/@@download/file/ToR%20ahWG-Cloud%20Services.pdf

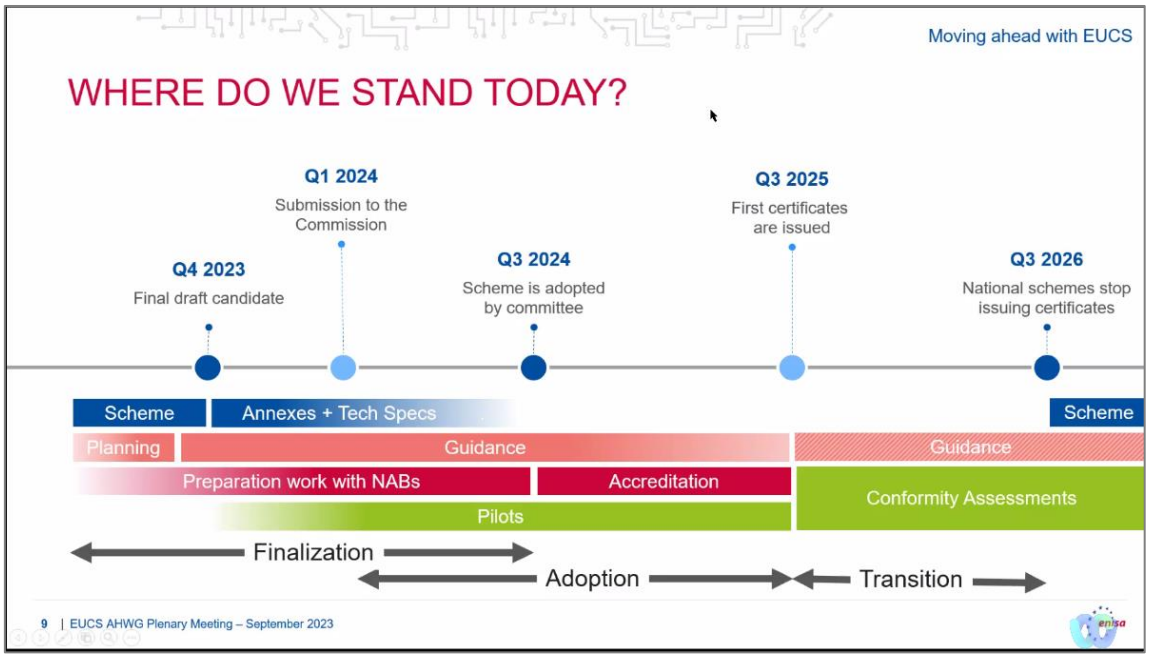

Figure 3. Progress on EUCS as reported by ENISA to the AHWG (source: ENISA)

4.1.2 Contribution to Thematic Groups (TG) of EUCS

When the AHWG was created, ENISA defined *nine* TGs out of which MEDINA actively contributed to *five* (see D7.8 [1]). During the reporting period covered by the present deliverable, ENISA further refined/scoped the list of TGs just as shown in Table 3. Based on the approach described in Section 2, MEDINA decided to focus efforts on all TGs with exception of TG3[15]. Specific contributions are mentioned in the rest of this section.

Table 3. ENISA EUCS' Thematic Groups (Final)

TG	Name	Terms of Reference
TG1	Core Scheme	Governance rules, implementing act
TG2	Requirements for cloud services	CEN CENELEC EUCS1
TG3	Conformity assessment for cloud services	CEN CENELEC EUCS2
TG8	Guidance on requirement	Implementation guidance and good practices for stakeholders
TG9	Questionnaire for the "basic" level of assurance	Self-assessment questionnaire
TG10	Mapping to other standards	Relationship to other cybersecurity certification frameworks

4.1.2.1 TG1 – Core Scheme

During this reporting period, the original goal of TG1 (i.e., to determine the different scope and dimensions needed to define the assurance levels that EUCS needed) was changed to it could define the governance rules for EUCS (e.g., certificate maintenance lifecycle) and prepare the draft scheme for the "Implementation Act". As explained by ENISA in [13], an implementing act is the final step needed to have fully functional certification scheme. The implementing act is a

[15] The whole notion of continuous (automated) monitoring was "migrated" from TG3 to TG2 by ENISA.

self-contained document which is delivered to the EC and contains all EUCS requirements, governance rules, concepts, etc. At the time of writing, the Implementing Act for EUCS was still work in progress (see Figure 3 and Figure 4)-

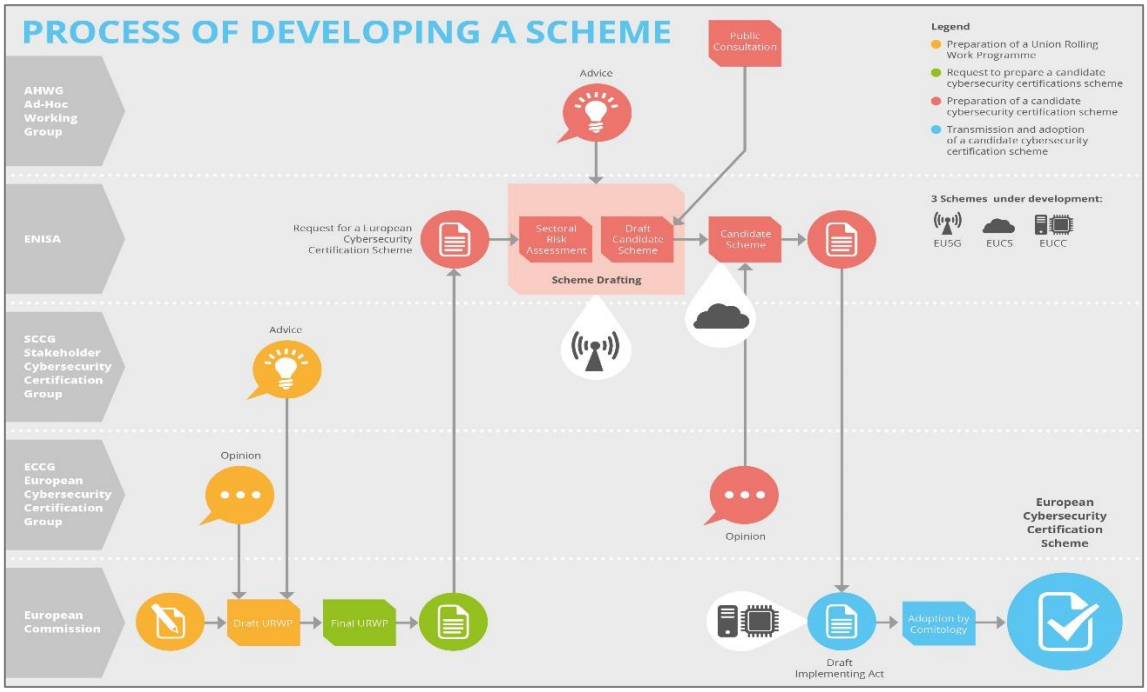

Figure 4. Process of developing a certification scheme (source: ENISA [13])

MEDINA's representative at the AHWG contributed with the overall alignment of the core scheme with respect to the discussions taking place at CEN CENELEC (see Section 4.1.3) particularly related to the notion of continuous (automated) monitoring. Being a central concept in MEDINA, where very few industrial experiences exist, our contributions greatly supported the work from TG1. Also beneficial for MEDINA was the feedback received from its interactions with the AHWG (for example during the ENISA EUCS Winter summit in 2022[16]), where TG1 concepts like operational efficiency and composability generated fruitful discussions.

Also, worth to notice was the project's contribution to the TG1 concept of "cloud security extension profile (CSEP)", where a proof of concept was developed for an IoT Cloud use case (therefore aligned to Bosch's contribution to MEDINA's validation task). The contributed PoC document can be found as *APPENDIX D: TG2 Contribution Sample – CSEP Proof of Concept*[17]. The project's CSEP contribution is expected to be maintained in the candidate scheme to be submitted for the EC's implementing act process.

4.1.2.2 TG2 – Requirements for Cloud Services

Since the beginning of MEDINA, it was clear that TG2 would play a critical role in the technical activities related to the elicitation of technical and organizational measures (TOMs) for certifying a cloud service. Already during the first half of the project, important efforts were invested to propose in the AHWG requirements for EUCS taking as baseline existing schemes and control catalogues. General terminology and specific concepts were also aligned between both initiatives, just as reported in D7.8 [1].

[16] Please refer to https://medina-project.eu/blog/medina-discussions-at-the-enisa-eucs-winter-summit-2022/

[17] Given the nature of the AHWG, this contribution could not include the MEDINA acknowledgement.

Although TG2 officially finished its activities in December 2021, MEDINA played a primary role in follow-up tasks which took place in the context of CEN CENELEC (cf. Section 4.1.3). As part of our "transfer" standardization approach, the consortium decided to take the set of requirements elicited by TG2 are part of MEDINA's *Catalogue of Controls and Metrics* (please refer to D2.2 [11]). The TG2 controls are organized into the 20 security categories. A total of 119 controls are defined, and the user can list all the controls of EUCS, and filter them the list by name or code. The catalogue implementation also allows users to navigate from a selected category to its specific control list. The control properties include a description, and each control is linked to its list of security requirements (TOMs).

The user interface in the Catalogue allows and easy navigation from the category to the controls, and from here to the related requirements, and finally to the metrics related to it. The navigation can also be done backwards. Each requirement is tied to one of the three assurance levels defined in EUCS. A total of 998 requirements elicited by TG2 were included in the Catalogue.

The mapping of EUCS with other schemes has also been incorporated in the Catalogue, in the feature called "similar controls". There, a list of EUCS controls is shown along with the controls that are equivalent in other schemes (C5:2020, SecNumCloud, ISO/IEC 27002, ISO/IEC 27017, and Cisco CCF). A snapshot of the Catalogue showing the EUCS requirements elicited by TG2[18] can be seen in Figure 4.

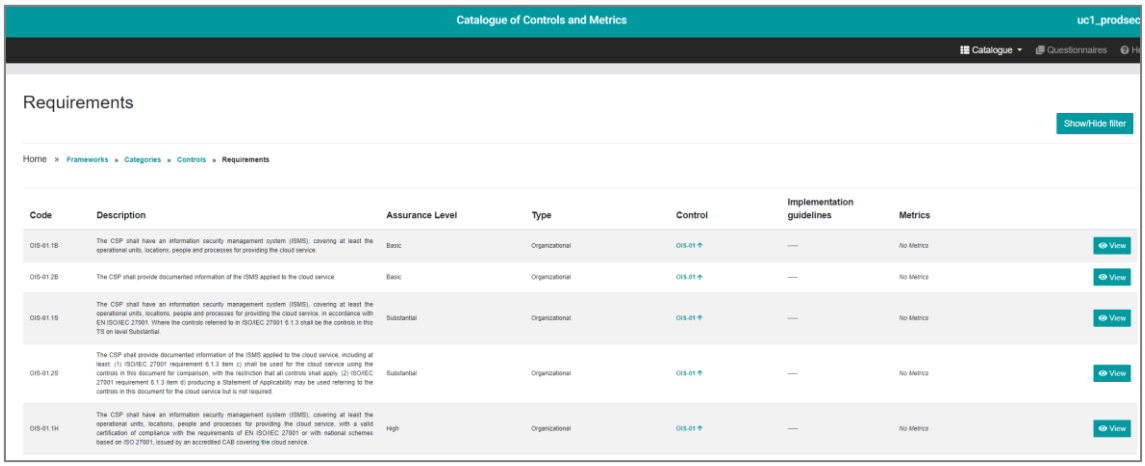

Figure 5. TG2 requirements from EUCS integrated into MEDINA's Catalogue

Given its participation in TG2, MEDINA obtained a clear advantage by having early access to draft versions of the EUCS catalogue so it could be integrated into the project's activities. Also, this allowed us to timely detect implementation issues with the elicited requirements, provide early feedback to the AHWG, and disseminate MEDINA findings to practitioners interested on EUCS.

4.1.2.3 TG3 – Assessment Methods

As reported previously in D7.8 [1], this foundational thematic group was devoted to the definition of the conformity assessment method(s) that will be used by EUCS once it is published. One of the main outcomes from TG3, that drove the project activities during the second half of its duration, was the notion of certificate's life-cycle management as implemented by our framework's *Orchestrator*. This is another clear example of the positive impact that our "transfer" approach had for MEDINA's technical activities. Although not directly contributed by

[18] At the time of writing the TG2 catalogue of EUCS requirements is not anymore distributed by ENISA on its public web page. It has been moved to CEN CENELEC so a copy can be bought from interested stakeholders.

MEDINA, the outcomes from TG3 also drove the dynamic risk management methodology of the project just as documented in D4.5 [8]. Both features (i.e., dynamic risk management and certificate life cycle management) as contributed by MEDINA's participation in TG3, became integrated into the final version of the prototype as seen on the screenshot below.

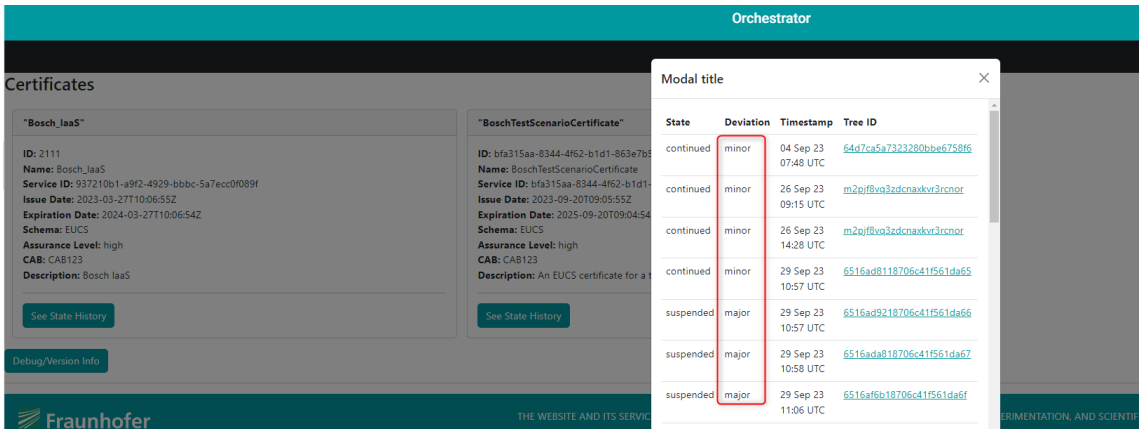

Figure 6. MEDINA's Orchestrator implementing TG3's notion of certificate lifecycle management.

After the finalization of TG3, the standardization work of EUCS' conformance assessment methodology was taken over by CEN CENELEC JTC13 WG3. MEDINA maintained its role of observer to continue "transferring" relevant results into the project.

4.1.2.4 TG8 – Guidance on Controls

TG8 targets the development of guidelines with good practices related to implementing and auditing EUCS. These guidelines complement the work of TG2 and TG3 (including the associated CEN CENELEC standards) with information which is considered useful for early adopters of EUCS. MEDINA has played an important role in the development of these guidelines (in particular those related to the EUCS security requirements) from two different perspectives. Firstly, our "influencing" approach has been used by our AHWG representative (Dr. Jesus Luna Garcia, Bosch) to position MEDINA as main contributor for guidelines related to the implementation of technical requirements e.g., cryptography as seen in *APPENDIX E: TG8 Contribution Sample – EUCS Guidance for Category CKM*. MEDINA contribution has been shaped based on the feedback received from the project's technical leads and paving the road towards the introduction of compliance metrics and EUCS automation.

Secondly, the *Catalogue of Controls and Metrics* is the MEDINA tool that has gathered the TG8's paper-based guidance and implemented them in the MEDINA framework also as "Implementation guidelines". Each of the guideline is accompanied by references and description of the control, reference and description of the requirement, and a table of key concepts used in the guideline. Furthermore, these machine-readable guidelines are also linked from the *Continuous Certification Evaluation* (*CCE*) to aid MEDINA users (e.g., security engineers) fixing detected non-compliances. Screenshots of both features can be seen in Figure 7 and Figure 8 respectively.

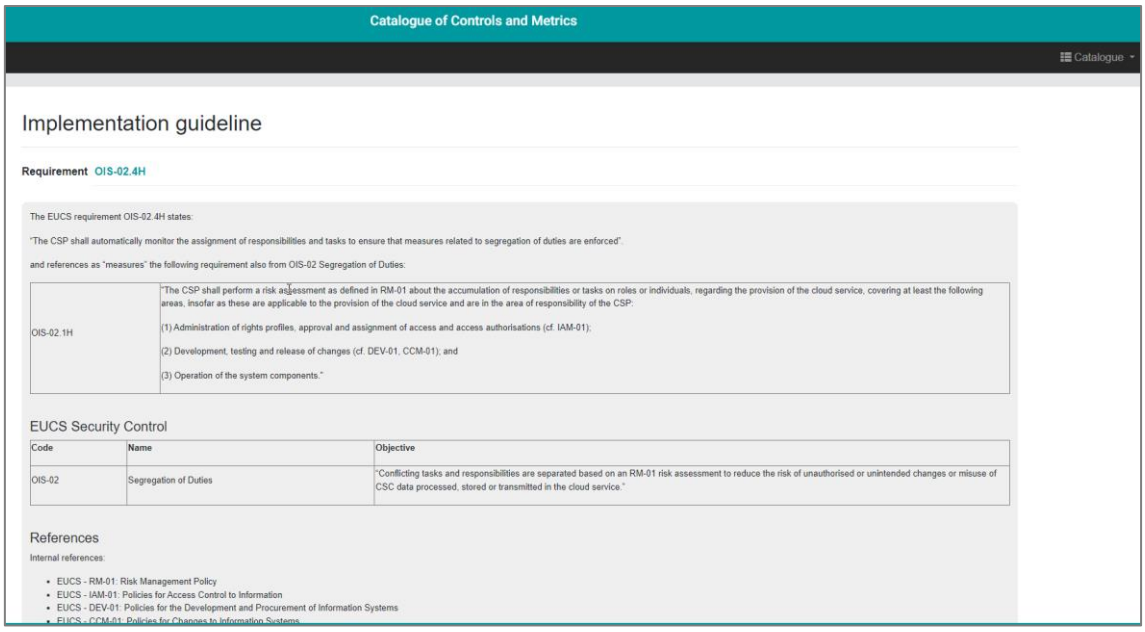

Figure 7. TG8 implementation guidance integrated into the MEDINA's Catalogue

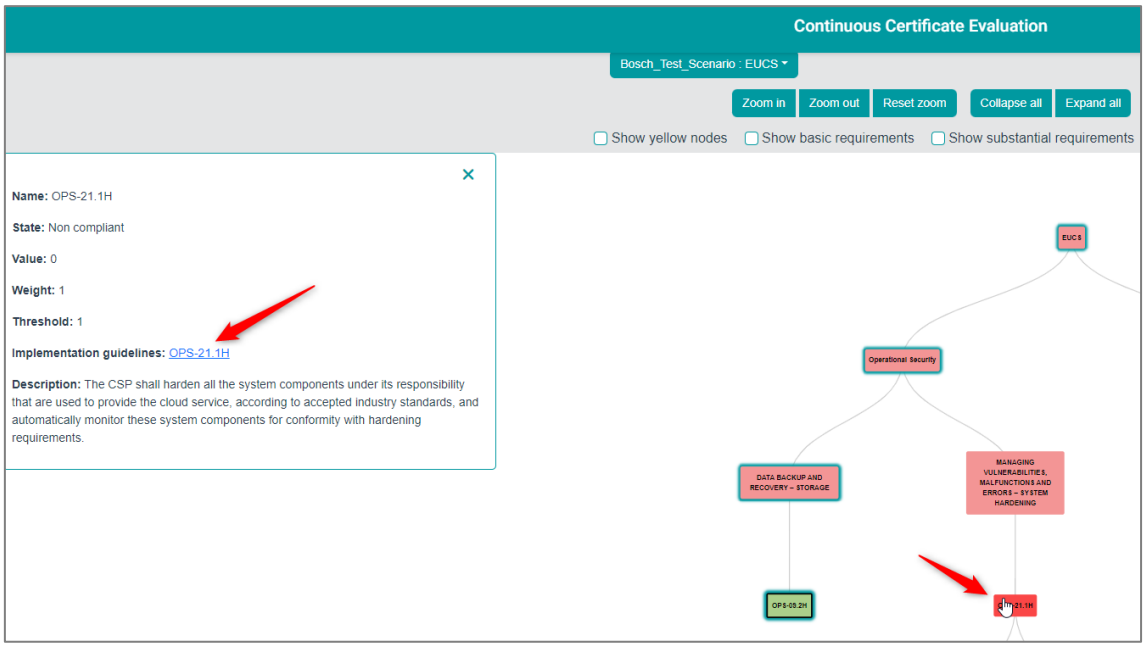

Figure 8. TG8 implementation guidance linked by the CCE component

It is worth to notice that the work in TG8 strongly depended on a final version of the EUCS requirements being developed by CEN CENELEC (see Section 4.1.3), which unfortunately did not come during the duration of MEDINA. Notwithstanding this fact, the project's contribution took a due diligent approach by considering the material being produced by our technical activities and the discussions within the AHWG.

4.1.2.5 TG9 –Questionnaire for Basic Assurance

Since the creation of EUCS, the notion of basic assurance certification with self-assessments was considered as a strong requirement from the EU Cyber Security Act (EUCSA). As a result, the ENISA AHWG started investing efforts in developing an assessment methodology and questionnaire for guiding CSPs and CABs in aspects related to the achievement of a basic

assurance EUCS certificate. These activities were also part of MEDINA's technical activities (cf. D3.3 [14]) and intermediate results have been continuously shared and discussed with ENISA by our AHWG liaison (see Figure 9).

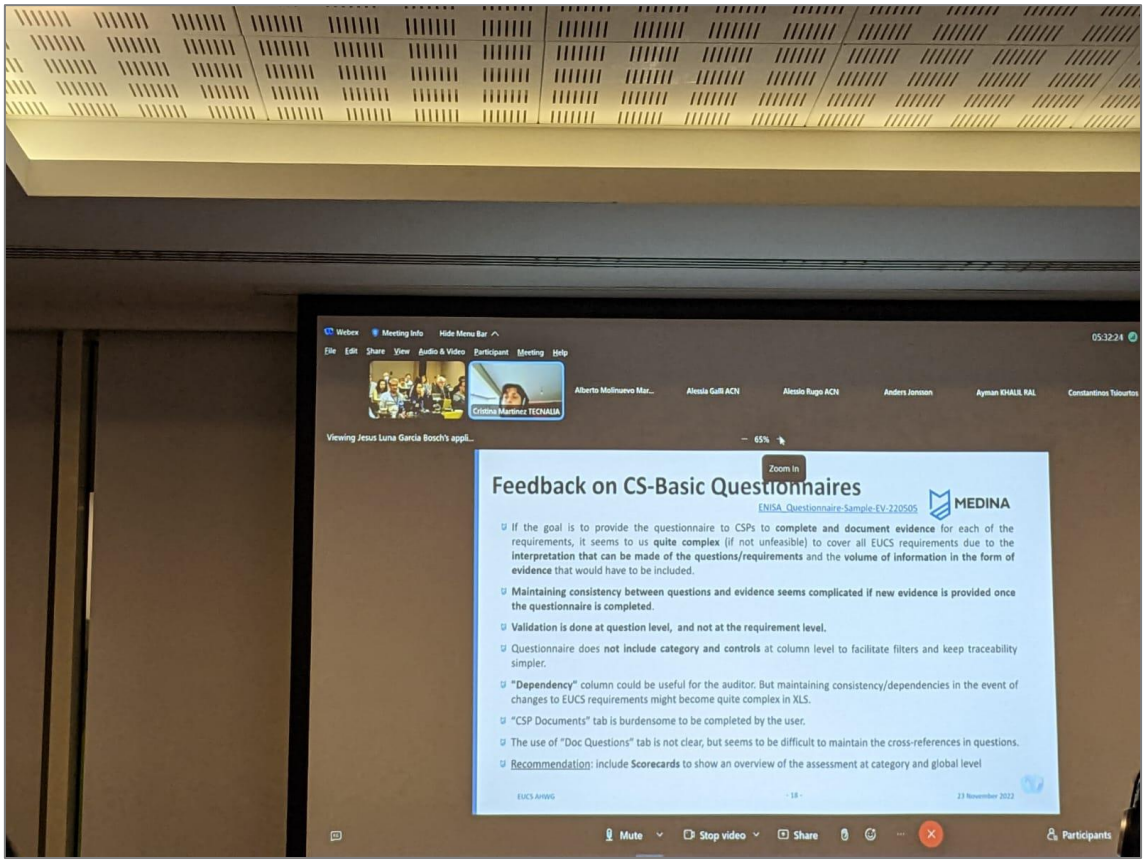

Figure 9. MEDINA's contribution to TG9 being discussed with the AHWG during the EUCS Summit[19]

Part of MEDINA's results shown to the reported AHWG is the questionnaire feature which is included in the MEDINA *Catalogue of Controls and Metrics*. There, the user can select a cloud service and perform a self-assessment questionnaire. Apart from the Basic assurance level, the tool allows to assess the Substantial and High levels too. The number of questions to be answered increases with the level, as an upper level includes the requirements of the lower level too. Concretely, the questionnaire is composed by 504, 857 and 1003 questions respectively for Basic, Substantial and High levels[20].

The questions are at requirements level, with each requirement having one or more questions. Every question has a closed list of (four) possible answers: Fully supported / Partially supported / Not supported at all / Not applicable. Once all the questions of a Requirement have been answered, the degree of Compliance of the Requirement is calculated and displayed.

The questionnaire allows to introduce Evidence and Comments for each question. Moreover, if the user has an auditor role, the tool allows to introduce non-conformities for each requirement. The tool also allows to store and recover questionnaires, to resume unfinished work. And the

[19] Please refer to https://medina-project.eu/blog/medina-discussions-at-the-enisa-eucs-winter-summit-2022/

[20] Although self-assessment only applied to EUCS-Basic, it is the opinion of our project that such approach can also be used as "CSP preparedness" activity for both Substantial and High.

user can finally generate a PDF report with all the results, including charts with the evaluation information. A screenshot of this MEDINA framework's feature is shown below.

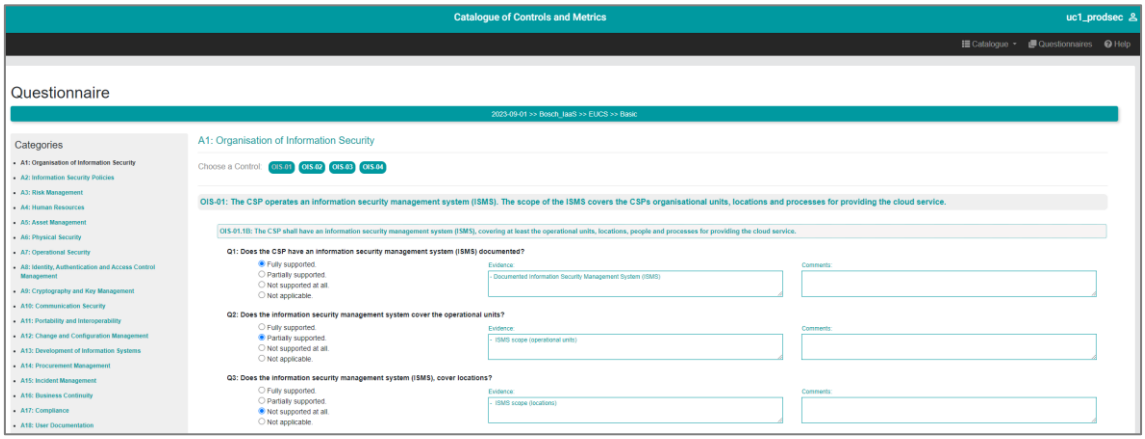

Figure 10. TG9 questionnaire integrated into the MEDINA framework

4.1.3 CEN CENELEC JTC13 WG2 (EUCS1)

As stated in D7.8 [1], CEN CENELEC JTC13 WG2 was delegated by the EC to develop a "technical specification" for EUCS (EUCS1 - Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services). EUCS1 is aimed to become a formal standard containing a revised set of the EUCS requirements published by ENISA in draft form last December 2020. The development of this technical specification follows the internal CEN CENELEC processes Including the participation of Member States experts and Observers. Started in November 2021, **MEDINA (represented by Jesus Luna Garcia, Bosch) was designated by ENISA as technical expert for supporting the development of EUCS1**.

The original timeline of the EUCS 1 project was as follows:

- Circulation of 1st working draft: March-2022
- Acceptance of TS draft: September-2022
- Submission to vote on TS: December-2022
- Closure of vote on TS: March-2023
- Revision of TS (pre-standard): 2026

However, given all expert-driven discussions that took place within CEN CENELEC around the original set of EUCS requirements, a final agreement on EUCS was not achieved until the end of June 2023 (see screenshot below). This delay (almost 12 months considering the initial plan for September 2022, with by-weekly meetings starting January 2023) obeyed multiple causes out of MEDINA's control, although contributions from the project flowed as expected from our expert role delegated by ENISA.

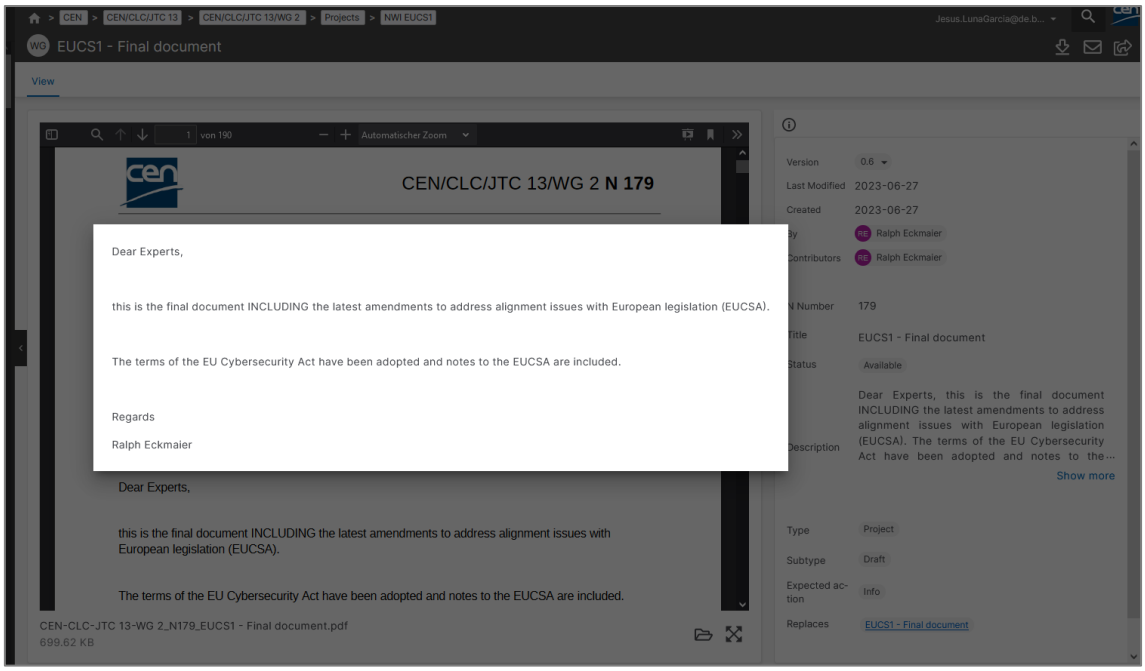

Figure 11. Final agreement on EUCS1[21]

Apart from the discussions related to the overall technical feasibility of the provided requirements (in particular for Basic, which is expected to be the entry point for EU SMEs), major MEDINA-related discussions came on the topic of "continuous (automated) monitoring" where the project was invited to present its insights during March 2023 (see *APPENDIX F: Contribution to EUCS1 on Continuous Automated Monitoring*). CEN CENELEC experts provided many arguments against the feasibility of EUCS-continuous based on the current state of practice, and expressed concerns related to its applicability for SMEs (even in the case of targeting High assurance). Although many arguments were not considered of a technical nature, it became clear that this topic (i.e., continuous / automated monitoring) could become a showstopper for the whole EUCS. Therefore, it was decided within the group of ENISA-nominated experts to greatly reduce the number of associated requirements[22] and bring the concept forward as part of the EUCS Implementation Act (expected 2024). This decision allowed for a final agreement with the CEN CENELEC members at the end of March 2023 as seen below[23]. At the time of writing, the internal voting for EUCS1 was still ongoing and expected to finalize by the end of 2023 or beginning 2024.

[21] Source: internal CEN CENELEC Portal.
[22] In the EUCS1 accepted by CEN CENELEC experts, the number of requirements mandating continuous/automated monitoring was reduced to only two (2).
[23] Due to the Intellectual Property rules of CEN CENELEC we cannot include a verbatim copy of the final decision document on this deliverable.

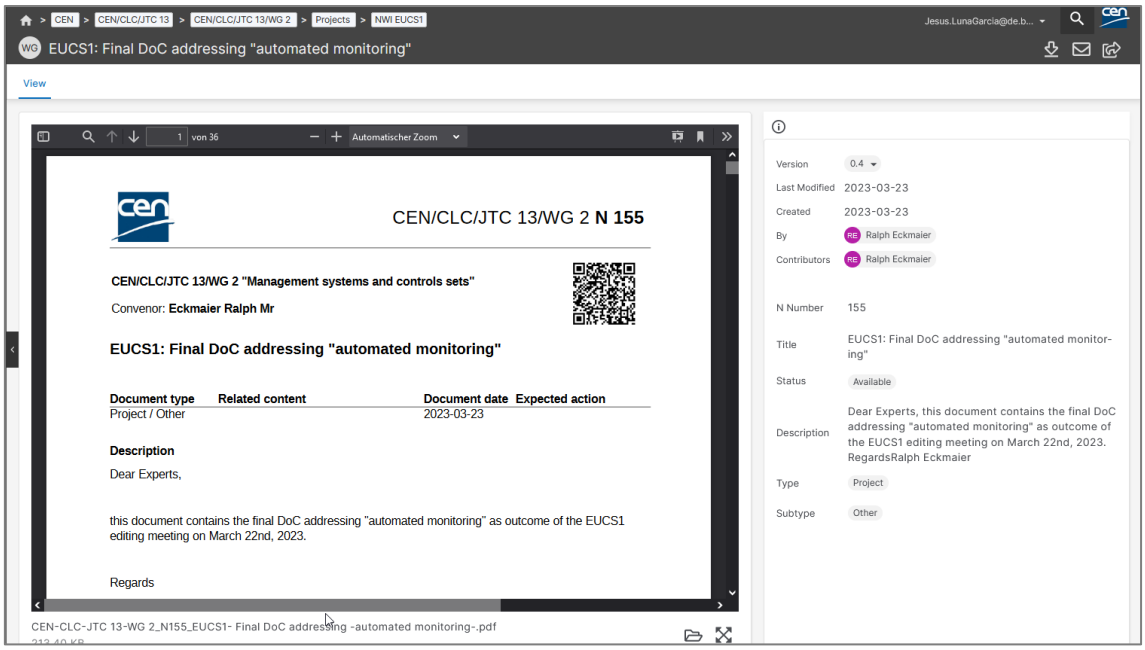

Figure 12. Final agreement on EUCS1 automated monitoring

4.1.4 CISCO CCF

As a recommendation received during the first review of the project, MEDINA also invested efforts in further investigating Cisco's Cloud Controls Framework (CCF) v1.0 [15]. Released in May 2022, the Cisco CCF is a comprehensive set of international and national cloud security compliance and certification requirements which have been aggregated into a single framework. It provides a structured, "build-once-use-many" approach for achieving multiple regional and international certifications[24], enabling market access and scalability, as well as easing compliance strain. Several international security compliance frameworks and certification standards were covered in CCF (up to a total of 14), including ISO/IEC 27001:2013, ISO/IEC 27017:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC27701:2019, Esquema Nacional de Seguridad (ENS), Cloud Computing Compliance Controls Catalogue (C5) and EU Cloud Code of Conduct (CoC), among others.

The MEDINA *Catalogue of Controls and Metrics,* in its final version, extended the "mapping of controls" feature to include CCF controls. This feature allows a user to check equivalencies among controls in EUCS with controls in other schemes (C5:2020, SecNumCloud, ISO/IEC 27002, ISO/IEC 27017, and Cisco CCF). This extension focuses on the subset of 26 controls related to the 34 high level EUCS requirements relevant for MEDINA.

The final mapping among EUCS with Cisco CCF and the other standards was described in D2.2 [11]. This mapping is available in the MEDINA *Catalogue* tool, under the "Catalogue"->"Similar Controls" menu option (see Figure 13).

[24] At the time of writing EUCS was not yet part of the Cisco CCF.

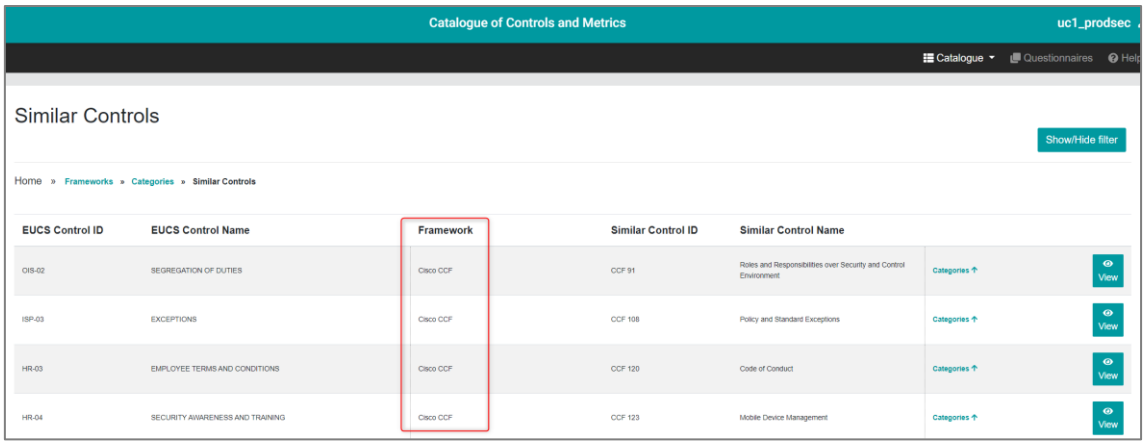

Figure 13. Mapping Cisco CCF to EUCS (MEDINA integration into Catalogue).

MEDINA established contact with the Cisco's creator of CCF (Dr. Prashant Vadlamudi), holding an online meeting in order to present him our contributed framework and identify possible synergies / future collaborations. As a result, Dr. Vadlamudi became part of MEDINA's Expert Stakeholder Group in April 2023[25].

4.1.5 Future Work on EUCS Standardization

Although the MEDINA project's lifetime is coming to an end, the ENISA TGs will continue running for at least few more months (or until the final version of EUCS is released by the EC). Therefore, aligned to our commitment related to MEDINA's sustainability, partner Bosch will continue its AHWG role and corresponding contributions to TG1 (active reviewer), TG2 (active contributor), TG8 (active reviewer), and TG9 (active validator). These decisions have been communicated and documented by ENISA during the EUCS AHWG plenary meeting from September 2023.

Furthermore, a new TG10 – EUCS Mappings has been created by ENISA with the purpose of supporting the so-called "statements of applicability", which are typically used by CSPs to become EUCS certified when a previous certification exists (e.g., BSI C5 or ISO/IEC 27001). This group resembles MEDINA's work on "EUCS mappings" which was also part of the technical activities related to the Catalogue (see D2.2 [11]), and it will be actively observed in case a contribution with the collaboration from TECNALIA can be feasible in the future.

From a CEN CENELEC perspective, after the finalization of MEDINA it is still expected to continue Bosch's contributions to the general EUCS1 and in particular to bring forward the notion of continuous / automated monitoring. The most likely way for this to happen is through the re-introduction of the topic in the Implementation Act, but this will have to be decided by ENISA by the end of 2023. Based on our MEDINA experience, we strongly believe that continuous / automated is feasible (even with current technology, as showed by our contributed framework) and it is a "must-have" for enabling true continuous-audit based certifications in the future. More on this topic will be discussed in Section 4.3.

Finally, related to CISCO CCF both TECNALIA and Bosch expect to keep looking for future synergies even after the finalization of the MEDINA project. Further exploration of related activities is expected to happen in the context of the upcoming Horizon EU funded projects EMERALD and COBALT.

[25] Please refer to https://medina-project.eu/blog/third-expert-stakeholder-group-meeting/

4.2 Metrics-Related Activities

The second "pillar" identified by our standardization Roadmap relates to the topic of metrics for compliance. Metrics provide the basis for building a uniform criteria to be used in conformance assessment processes (EUCS included), therefore paving the road towards a future "audit-once, certify-many". Just like in the case of EUCS requirements, metrics can be either organizational or technical, whereas the latter have a greater automation potential which benefits adoption of the MEDINA framework. Despite our "scouting" approach found that there are not many SDO initiatives on the field of metrics for compliance, this section summarizes the project's contribution to two major standardization activities in this area.

4.2.1 Performance Measurement Guide for Information Security (NIST 800-55 release 2)

Acknowledging the importance of the notion of metrics for checking compliance with the controls in NIST 800-53 [16], the associated metrics were released as NIST 800-55 in 2008 [17]. The latter not only explores the basic concepts related to the topic, but also presents elicitation processes which can be followed to support organizations in measuring their levels of compliance related to NIST 800-53. Finally, the original version of the standard also includes examples which can be used as guideline for eliciting further metrics in the organization. Although its contribution to metrics can be seen as scoped in the controls from NIST 800-53, it is also true that NIST 800-55 creates the basis for using metrics in certification processes under the FedRAMP[26] mandate. Extrapolating this goal to the upcoming EUCS in Europe, MEDINA decided to invest efforts in contributing to the second revision of NIST 800-55 in February 2023.

In response to the call for contributions[27] to the working draft of NIST SP 800-55 rev. 2, MEDINA submitted the contribution included as *APPENDIX G: Contribution to NIST SP 800-55 Rev. 2* of this deliverable. Provided feedback shows contributions coming from our project's technical activities (in particular D2.2 [11]) and also gathered opinions from our ESG industrial experts about the usefulness of metrics and measurements for compliance programs. Furthermore, we also pointed to related activities for NIST consideration to avoid unnecessary overlaps and support the creation of positive synergies. Explicit reference to leveraging machine-readable standards (e.g., NIST OSCAL) took a special place in MEDINA's contribution to NIST 800-55 rev. 2.

Although at the time of writing this report our consortium has not yet received any feedback from NIST, it is our belief that the topic of metrics for compliance will revamp as the revision of the ISO/IEC counterpart starts (see Section 4.2.2 for further details).

4.2.2 Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (ISO/IEC 27004)

As mentioned earlier in this section, despite the importance of the "metrics for compliance" topic, so far there are just few relevant initiatives being led by SDOs. One of those is ISO/IEC 27004 "Security techniques — Information security management — Monitoring, measurement, analysis and evaluation", which revision request was submitted to the ISO/IEC JTC 1/SC 27/WG 1 secretariat in October 2022 (please refer to Figure 14 below).

[26] Please refer to https://www.fedramp.gov/
[27] Please refer to https://csrc.nist.gov/pubs/sp/800/55/r2/iwd

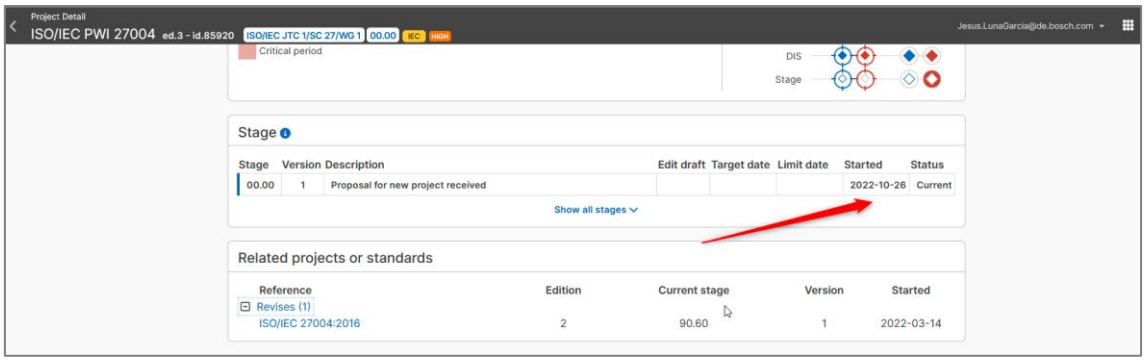

Figure 14. Request for revision of ISO/IEC 27004:2016

During the duration of MEDINA, no further updates appeared related to the revision of ISO/IEC 27004, however our official liaison to the corresponding ISO/IEC expert group (i.e., Jesus Luna Garcia, Bosch) has been already appointment by the German National Standardization Body (DIN) for providing contributions when the time comes.

4.2.3 Future Work on Metrics for Compliance

MEDINA's standardization work on this topic has concluded that although relevant works have existed for at least 5 – 10 years in the SDO ecosystem, apparently the topic has not yet achieved the level of acceptance / maturity needed by the industry. The "traditional" notion of cybersecurity metrics and Key Performance Indicators has made it through areas like monitoring of security events (SIEM) and steering of cybersecurity organizations, however much more work and awareness will be required for the uptake of metrics and measurements for compliance. Related to EUCS, during the duration of MEDINA several discussions have taken place with ENISA and its AHWG to guarantee that metrics can be included in the guidance being developed by TG8 (see Section 4.1.2.4). At the time of writing, no final decision has been taken by ENISA yet. Nevertheless, future research and innovation activities in both Horizon Europe EMERALD and COBALT will guarantee that this topic is diligently followed-up and contributed by the corresponding consortiums.

4.3 Automation-Related Activities

The third and final pillar in our standardization Roadmap is about automation support for compliance monitoring, a necessary piece to bring the contributed MEDINA framework a step closer to industrial practice. Being automation a major topic in MEDINA, it is not surprising that major efforts were invested in related standardization engagements, just as seen in the rest of this section.

4.3.1 Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017)

As introduced in D7.8 [1], the importance of ISO/IEC 27017 for MEDINA relies on the fact that it provides guidelines for information security controls applicable to the provision and use of cloud services. Having a similar goal to that pursued by ENISA TG8 (see Section 4.1.2.4), plus opening the possibility to introduce the notion of automation for compliance, it was decided by MEDINA to participate in the current revision period of ISO/IEC 27017 (published in the official ISO website[28]) expected to end by Q1/2024.

[28] Please refer to https://www.iso.org/standard/82878.html

Starting with its contributions on March 2022, MEDINA began to shape the revised ISO/IEC 27017 standard with contributions on topics like continuous (automated) monitoring to propose an EUCS-like approach. Submitted contributions came in two related topics:

1. Automated monitoring of cloud services' configurations based on standardized machine-readable templates. This contribution goes in the direction of the research performed in MEDINA with its *Clouditor* evidence collector, where compliance of Infrastructure-as-Code (IaC) deployments can be automatically monitored and reported to the *Orchestrator*. Details on provided contribution can be found in *APPENDIX H1: Contribution to ISO/IEC 27017 on Automated Configuration Monitoring*. Furthermore, at the time of writing, the 2nd working draft text for ISO/IEC 27017 already included the core proposal as seen in Figure 15.
2. Automated monitoring as preamble to automated auditing. This contribution refers to a full revision of the relevant parts of ISO/IEC 27017 where the notion of automated monitoring becomes more precise (i.e., rely on standards like NIST OSCAL) while paving the road to automation in conformance assessment processes. The provided contribution can be found in *APPENDIX H2: Contribution to ISO/IEC 27017 on Automated Monitoring Annex*, although at the time of writing the corresponding Secretariat has not yet provided the official decision on the contribution's approval.

12 **Guidance for cloud services**

Cloud service customer	Cloud service provider
The cloud service customer should ensure the allocated responsibilities regarding configuration management for the use of the cloud service. The cloud service customer should define and implement configuration management processes and tools for the cloud service considering: a) availability of documented information for the secure configuration of the cloud service; b) availability of configuration management capabilities provided by the cloud service provider; c) to continuously monitor whether the provided standard templates satisfy the security policy and requirement of the cloud service customer; d) ability to customize the standard templates provided by the cloud service provider to reflect its security policy or target security posture, which can be in different formats.	The cloud service provider should provide information to the cloud service customer about their configuration management responsibilities. The cloud service provider should provide capability and information about: a) the secure configuration for the use of the cloud service; b) configuration management capabilities for the cloud service customer; c) standard templates available for the cloud service.

Figure 15. Successful MEDINA contribution to ISO/IEC 27017

4.3.2 Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security (ISO/IEC 20078-3:2021)

Following the recommendations received from the Reviewers during the first reporting period, our "scouting" approach proceeded to review the referred ISO/IEC 20078 standard[29] and its relationship to MEDINA. The version of the standard obtained by the consortium shows that it provides requirements related to the secure authentication of users, delegation principles, roles definitions, and separation of duties related to the so-called extended vehicles as defined in this family of standards. Furthermore, basic communication workflows for authentication, authorization, and resource access are also defined. Finally, the standard provides an informative annex with a reference implementation based on OAuth 2.0 and OpenID Connect 1.0

Although a more detailed analysis should take place once the scope/applicability of EUCS is finalized, for the time being one could assume that Web Services in the scope of ISO 20078-2 might fall in the scope of EUCS if these are offered as cloud services. In the context of this working assumption, those ExVe web services could be automatically/continuously checked for EUCS compliance using the developed MEDINA framework and provided the adequate evidence collectors exists. Although from a pure technological perspective it is reasonable to assume applicability of MEDINA, more detailed analysis should take place about the actual mandate to EUCS-certify those services.

The latest revision of ISO 20078-3 dates from 2021, so our expectation is that for the next time it goes into maintenance mode, the topic of "continuous" (either related to EUCS or to ISO/IEC 27017 as presented in the Section 4.3.1), will be also part of the discussions within the corresponding ISO group.

4.3.3 Open Security Controls Assessment Language (NIST OSCAL)

An important initiative identified by our scouting approach relates to leveraging NIST OSCAL as a standardized machine-readable language to fully realize the potential of the MEDINA framework. OSCAL might create interoperability between different technology providers/CSP to transport relevant information for the continuous certification process as envisioned by MEDINA. Given the level of maturity achieved by OSCAL during the last few years (as evidenced by its leverage in relevant certification initiatives like FedRAMP[30]), MEDINA has devoted efforts to further analyse its potential from a standardization perspective[31]. This section presents a summary of MEDINA's standardization engagements related to OSCAL from two different perspectives: ETSI CYBER and EUROSCAL.

4.3.3.1 OSCAL Usage Guidelines (ETSI DTR/CYBER-0087)

OSCAL was first introduced into an ETSI technical report back in 2022 with a scope on cybersecurity controls for cyber defense [18], where a machine-readable representation of the defined controls was proposed using OSCAL. As mentioned on that ETSI report, the corresponding OSCAL representation was also made available online[32].

[29] Please refer to https://www.iso.org/standard/80185.html
[30] Please refer to https://www.fedramp.gov/blog/2021-07-20-FedRAMP-Releases-Updated-OSCAL-Templates-Tools/
[31] MEDINA's contributions to OSCAL have been also important to internationally disseminate our research, just as evidenced by the activities reported in D7.5 [21]
[32] Please refer to https://github.com/CISecurity/CISControls_OSCAL

Built on top of this previous OSCAL experience, ETSI went further and proposed work item DTR/CYBER-0087[33] with the goal of developing guidelines and good practices to extend the use of OSCAL in Europe. In this context, MEDINA was invited to contribute with use cases related to leveraging OSCAL in the context of EUCS. The provided contribution can be seen in *APPENDIX I: Contribution to ETSI DTR/CYBER-0087*, where usage of OSCAL is suggested not only for representing the EUCS' catalogue of requirements, but also for the actual (automated) compliance checks just as seen in Figure 16.

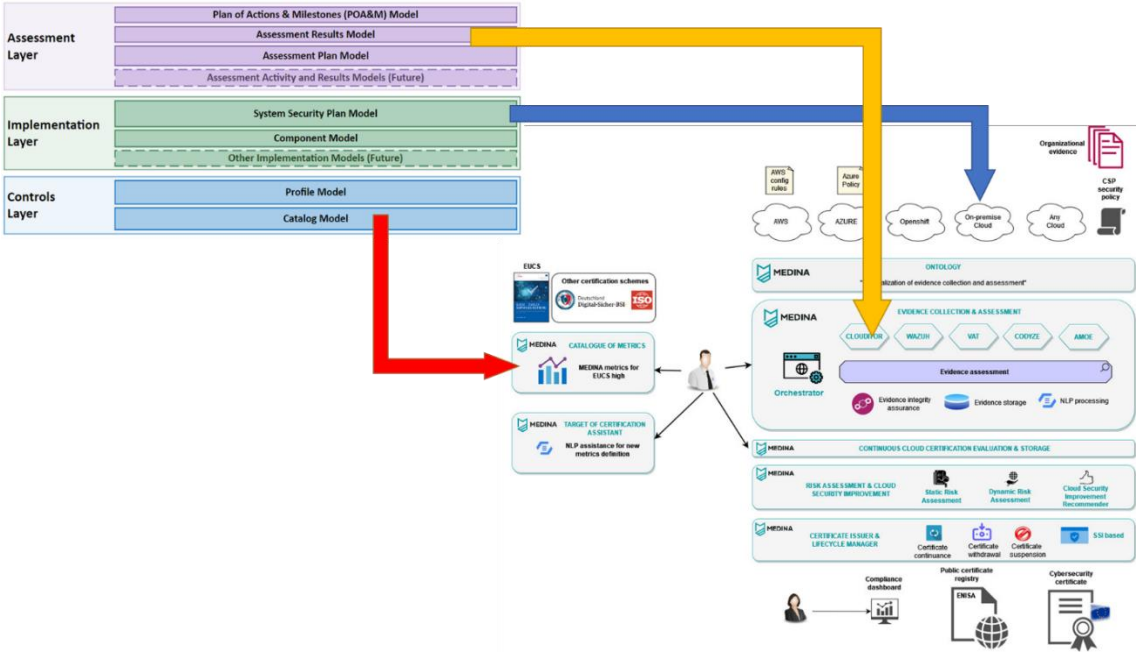

Figure 16. Leveraging OSCAL in EUCS using the MEDINA framework (ETSI TR 103 923 draft)

At the time of writing, further contributions are expected from MEDINA (and our ETSI CYBER liaison, Jesus Luna Garcia) by the end of 2023.

4.3.3.2 EUROSCAL

Essential in the sustainability plans of Bosch and TECNALIA for MEDINA is the so-called EUROSCAL initiative[34], which was born from our standardization efforts to promote the European use of NIST OSCAL (Open Security Controls Assessment Language) as a feasible solution for achieving interoperability and automating cloud security certification processes.

The proposal of MEDINA towards promoting the use of automation in EUCS relies on the creation of an open/community-driven initiative (EUROSCAL), where relevant European stakeholders will collaborate on a voluntary manner to exchange ideas and trigger spin-off activities towards adopting OSCAL. EUROSCAL is expected to become a central hub for learning the basics of OSCAL, and also to allow relevant stakeholders (including Regulators) realizing the potential of OSCAL for providing automation to cloud cybersecurity certification processes (in particular EUCS and other national schemes from Member States).

It is our belief in MEDINA that automation (through interoperability and standardization), will pave the road towards developing more efficient, objective, and trustworthy certification processes related to EUCS.

[33] Please refer to shortened link https://tinyurl.com/mvdetkbz
[34] Please refer to https://euroscal.eu/

During the course of MEDINA and based on our interaction with NIST, we identified a set of challenges where EUROSCAL could play a primary role. We refer in particular to the following:

- Lack of standardization in Control information: this not only hinders automation efforts, but also interoperability between the implementation of different tools. In MEDINA, this issue was found to limit our efforts to share information in the EUCS catalogue, and also while interacting with different CSPM (Cloud Security Posture Management tool) implementations.
- Interoperability in assessing Control implementations across multiple components: having a clear and transparent view on the implementation of Controls in complex cloud systems is essential for streamlining certification processes like those related to EUCS. The MEDINA framework relies on the notion of a "generic evidence collector" to automate the compliance checks in cloud services, and for this is needed to achieve interoperability in the way security configurations (implementation of Controls) are represented.
- Lack of support to multiple Regulatory frameworks: very often cloud services need to be compliant with different regulations and standards depending on different factors. Soon it will be common finding EU cloud service providers willing to demonstrate compliance with EUCS and one or more additional standards. The MEDINA framework has been designed to support more than only EUCS certifications, and therefore is strongly needed a mechanism to support multiple frameworks, in a machine-readable manner.
- Highly manual processes for reviewing documentation and assess Controls: certification processes have historically relied in manual processes involving all relevant parties. This is largely due to the complexity associated to defining and implementing security Controls, which is exacerbated in cloud services. This is a common challenge in MEDINA, where automated assessments need to rely on machine-readable schemas which can interoperate between the different components of the contributed framework.

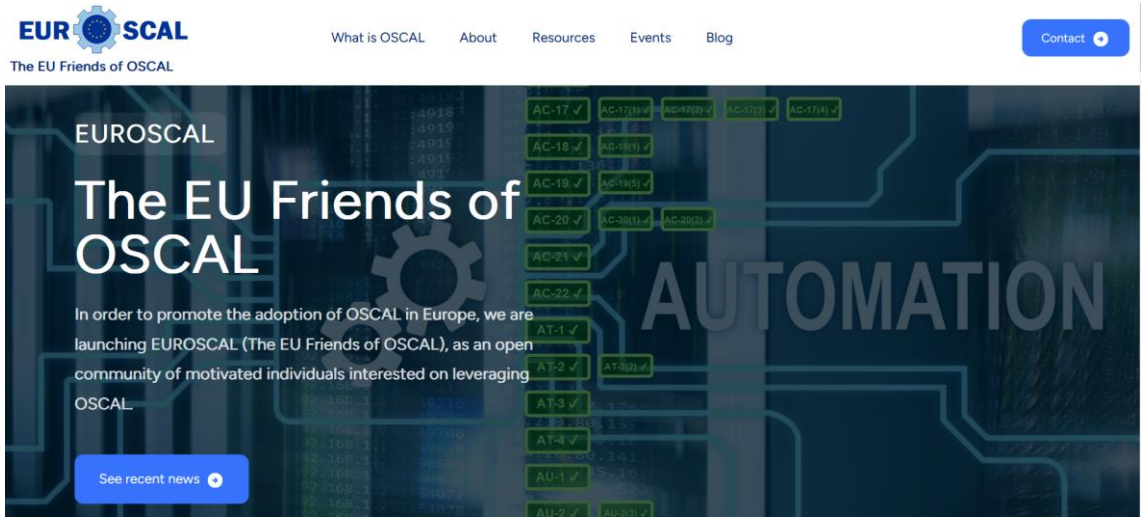

Figure 17. EUROSCAL landing page at www.euroscal.eu

At the time of writing the most relevant activities being discussed in the context of EUROSCAL include (i) continuous support to the standardization activities being led by ETSI CYBER (see previous section), (ii) support to the representation of the BSI C5[35] catalogue of controls in

[35] Please refer to https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

OSCAL format, and (iii) support leveraging OSCAL in the context of EUCS. These and other relevant topics are expected to continue developing even after the MEDINA project comes to an end. Finally, in the context of the Horizon EU COBALT project[36], actions related to EUROSCAL are being discussed and the option of setting it up as formal association (i.e., to comply with anti-trust compliance and address governance and IPR policies) will be further investigated.

4.3.4 The Gaia-X Initiative

Several members of the MEDINA consortium (i.e., Bosch, Fabasoft, FhG, HPE, TECNALIA and XLAB), are members of the so-called Gaia-X Association for Data and Cloud AISBL[37]. This association was founded with the goal of developing and operating the technical framework for the Gaia-X Federation services.

The German-funded Gaia-X Federation Services project was set up to design and implement an orchestration layer between the distributed, federated Clouds that comprise Gaia-X. The core functionalities of these Federation Services include integration, identity and authentication, security as well as compliance. Members of the consortium actively contributed to the design specification of the Continuous Automated Monitoring (CAM)[38] component. In this way, the research of MEDINA methodologies and techniques, such as the metric/evidence-based approach, were actively contributed to a de-facto industry standard. In turn to align with Gaia-X, the definition of the metric template used in the specification has been fully adopted by MEDINA.

Furthermore, Fraunhofer AISEC has been involved in the implementation of said specification in an open-source project[39], coordinated by the eco – Verband der Internetwirtschaft. Since the aim of the implementation task was to re-use existing open-source implementations in this field as much as possible, parts of the open-source components of MEDINA, such as the *Clouditor* component, have been integrated into the implementation of the CAM component, ensuring further reach of the MEDINA activities. Additionally, the MEDINA partner XLAB has been contracted for the implementation of the portal services of the Gaia-X federation services.

Also note that the Eclipse XFSC (Cross Federation Services Components) project[40] has adopted the development of Gaia-X federation services components.

4.3.5 Future Work on Automation for Compliance Monitoring

Like in the case of EUCS and metrics, there is still a long way to go before we can witness the use of automation in certification processes as envisioned by MEDINA. Undoubtedly, concrete steps have been taken by our project's standardization activities in the direction of automation, but much more is to be expected even after the finalization of MEDINA.

In the case of ISO/IEC 27017, one can still expect further discussions on the topic of continuous (automated) monitoring until the end of the revision period expected in 2024. As main proposer of that topic, MEDINA's Bosch partner will continue the corresponding contributions and discussions. A similar situation is to be expected with OSCAL and its EUROSCAL counterpart, where Bosch-led initiatives have been triggered and initial results are to be expected mid-2024. Related standardization activities in the upcoming Horizon Europe-funded COBALT project already consider support for such engagements.

[36] Please refer to https://horizon-cobalt.eu/
[37] Please refer to https://www.gaia-x.eu/who-we-are/association
[38] Please refer to https://www.gxfs.eu/download/1731/
[39] https://gitlab.com/gaia-x/data-infrastructure-federation-services/cam
[40] https://projects.eclipse.org/projects/technology.xfsc

Finally, depending on the future direction of EUCS and the referencing EU Directives and Acts, it is possible that future discussions within EU SDOs take place to decide on the applicability of "continuous" for purpose-specific cloud services including critical infrastructures and extended vehicles. This topic will be closely follow-up by interested MEDINA partners.

5 Conclusions

Standardization in MEDINA has played a central role both for supporting adoption of the overall framework (interoperability) and also for enabling sustainability of the project's key results. This deliverable presented the second (and final) iteration of MEDINA's report on standardization-related activities, which included a revised Roadmap with well-identified "pillars" designed to accelerate uptake of the developed framework. Activities and contributions to identified SDOs (including ENISA, ISO/IEC, NIST, and CEN CENELEC) have been reported by following the structure proposed by the referred Roadmap namely EUCS, metrics, and automation.

We have also identified and presented future work on the field of standardization which is expected to happen after the finalization of MEDINA. One of the main topics for the sustainability of the MEDINA results is to advance on the TRL of the developed outcomes towards a fruitful exploitation strategy. To this end, MEDINA partners have successfully achieved EU funding for the follow-up projects EMERALD and COBALT, and the DOME action:

- EMERALD (*Evidence Management for Continuous Certification as a Service in the Cloud*), led by TECNALIA, will start on 1st of November 2023. The EMERALD Certification as a Service solution leverages the H2020 project MEDINA's outcomes and advances them to TRL 7 in the EMERALD core. The core framework developers in MEDINA (TECNALIA, Fraunhofer, CNR, Fabasoft and NIXU) will participate in EMERALD where the MEDINA framework is expected to evolve and being exploited.
- COBALT (*Certification for Cybersecurity in EU ICT using Decentralized Digital Twinning*) will also start on November 2023 with the participation of Fraunhofer and Bosch. COBALT focuses on the continuous (automated) monitoring and certification of industrial AI systems, and quantum computing. The proposed framework will depart from core MEDINA functionalities (in particular the *Orchestrator*), and follow-up standardization engagements including its support to the European AI Act.
- DOME (*A Distributed Open Marketplace for Europe Cloud and Edge Services*) is a Digital Europe action in charge of developing a European Marketplace of Cloud and Edge Services. TECNALIA is leading the Certification task in DOME. It is planned that all the services to be endorsed in the DOME Market place support European certification schemes such as EUCS. DOME will serve as a new mechanism to gain users of the MEDINA framework, since the providers that want to include their services in DOME would need to be EUCS compliant. DOME started in January 2023 and since the beginning several partners have already expressed their interest in the MEDINA tools. In addition to Cloud Service providers, other stakeholders in the certification toolchain (e.g., Dekra) have requested information on the MEDINA framework and approach.

Before closing this report, we want to provide in Table 4 some final thoughts and recommendations targeting relevant stakeholders in the standardization field. Our goal is to incentivize an open dialogue towards the future adoption of MEDINA (and in general, towards the notion of "continuous/automated compliance monitoring") through well-focused standardization actions.

Table 4. Stakeholder recommendations related to standardization in MEDINA

Id	Recommendation	Target Stakeholder	Related MEDINA Roadmap Pillar	Additional Comments
R1	Incremental releases of EUCS benefit transparency and R&D	ENISA / European Commission	EUCS	Early dissemination / incremental releases of EUCS (e.g, first Basic, then Substantial, and finally High) would allow for more open dialogue with SDOs, and collaterally to speed up development of MEDINA framework.
R2	Cost-free access to EUCS1 and EUCS2	CEN CENELEC / European Commission	EUCS	Providing cost-free access to EUCS specifications (and in general to EU standards) would improve R&D+I around the proposed scheme.
R3	EUCS1 requirements are important, guidelines and training are essential	ENISA	EUCS	Major effort should be devoted to the development of EUCS1-guidelines and trainings, which will become of great aid for early adopters.
R4	EUCS guidance and metrics	ENISA	Metrics	ISO/IEC and NIST already acknowledged the importance of metrics for compliance. In parallel to the EUCS guidance, corresponding metrics should be elicited.
R5	Standardized metrics to improve certification	SDOs	Metrics	Having a standardized set of metrics for compliance, which is consistent among different SDOs would make certification processes more efficient and transparent.
R6	Automated monitoring is feasible, more practical experience is needed	CSP, CAB	Automation	Industry should start to acknowledge and embrace the role of automation in certification processes. Lots of EU-research has taken place on this topic, so it is time to take outcomes to practice.
R7	Automated monitoring is feasible, Regulators are essential for enablement	European Commission	Automation	Regulators' support is needed to take automation into certification processes. Without their support, frameworks like the one from MEDINA cannot be taken into real-world.

References

[1] MEDINA Consortium, "D7.8 Standardization Roadmap-v1," 2022.

[2] HSBooster.eu Consortium, "Horizon Standardization Booster," [Online]. Available: https://www.hsbooster.eu/. [Accessed 12 September 2023].

[3] StandICT.eu Consortium, "StandICT.eu," [Online]. Available: https://www.standict.eu/. [Accessed 12 September 2023].

[4] MEDINA Consortium, "D7.7 Exploitation and sustainability Report-v2," 2023.

[5] MEDINA Consortium, "D3.6 Tools and techniques for collecting evidence of technical and organisational measures-v3," 2023.

[6] MEDINA Consortium, "Blog - Third Expert Stakeholder Group meeting," 2 May 2023. [Online]. Available: https://medina-project.eu/blog/third-expert-stakeholder-group-meeting/.

[7] MEDINA Consortium, "Blog - StandICT.eu 2023 & MEDINA kick-off their collaboration," [Online]. Available: https://medina-project.eu/blog/standict-eu-2023-medina-kick-off-their-collaboration-with-an-mou-to-reinforce-european-standardisation-efforts-in-the-cloud-security-certification-field/. [Accessed 13 September 2022].

[8] MEDINA Consortium, "D4.5 Methodology and tools for risk-based assessment and security control reconfiguration - v2," 2023.

[9] HSBooster.eu Consortium, "HSBooster.eu Pool of Experts," [Online]. Available: https://www.hsbooster.eu/pool-of-experts/rusne-juozapaitiene. [Accessed 12 September 2023].

[10] Cisco Corporation, "Cisco Cloud Controls Framework," [Online]. Available: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html. [Accessed 13 September 2023].

[11] MEDINA Consortium, "D2.2 Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v2," 2023.

[12] National Institute of Standards and Technology, "OSCAL: the Open Security Controls Assessment Language," [Online]. Available: https://pages.nist.gov/OSCAL/. [Accessed 13 September 2023].

[13] ENISA, "From Candidate to Certification Scheme," [Online]. Available: https://www.enisa.europa.eu/topics/certification/from-candidate-to-certification-scheme. [Accessed 2 October 2023].

[14] MEDINA Consortium, "D3.3 Tools and techniques for the management of trustworthy evidence-v3," 2023.

[15] Cisco Systems, Inc., “Cisco Cloud Controls Framework,” 2022. [Online]. Available: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html. [Accessed January 2023].

[16] National Institute of Standards and Technology, “NIST 800-53 rev5 - Security and Privacy Controls for Information Systems and Organizations,” 2020.

[17] National Institute of Standards and Technology, “Performance Measurement Guide for Information Security,” 2008.

[18] European Telecommunications Standards Institute (ETSI), “Cyber Security (CYBER) - Critical Security Controls for Effective Cyber Defence - Part 4: Facilitation Mechanisms,” 2022.

[19] MEDINA Consortium, “D2.1 Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v1,” 2021.

[20] MEDINA Consortium, “D7.5 Dissemination and Communication Report-v2,” 2023.

APPENDIX A: The Approach to Standardization in MEDINA (excerpt as originally reported in D7.8)

Despite the evident benefits brought to research projects thanks to the adoption and influence on standards (including industrial good practices), previous experience has shown that unstructured approaches have a negative effect on both usage of resources and general uptake of generated outcomes. When technical work packages are not aware of relevant standards in their field, there is a high risk of lacking interoperability and therefore damaging their planned exploitation activities. Furthermore, if a project fails to timely identify and create synergies with relevant standardization activities, it is very unlikely that scientific and technical outcomes will influence the corresponding SDO or SSO.

Which are the elements to develop an efficient approach to standardization? When it is the right point in time for projects to start working on standardization activities? Despite there is no easy answer to these questions, this section will discuss the approach developed by MEDINA to maximize the benefits of standardization, in particular related to the topic of continuous certification.

MEDINA's standardization approach consists of three interrelated processes, namely:

1. **Scouting**, where project experts constantly survey the SDO/SSO landscape to identify relevant activities for MEDINA.
2. **Transfer**, where identified standards/good practices are analysed and leveraged into MEDINA's technical activities.
3. **Influencing**, where MEDINA actively engages in the development of identified standards/good practices.

These processes can be seen below.

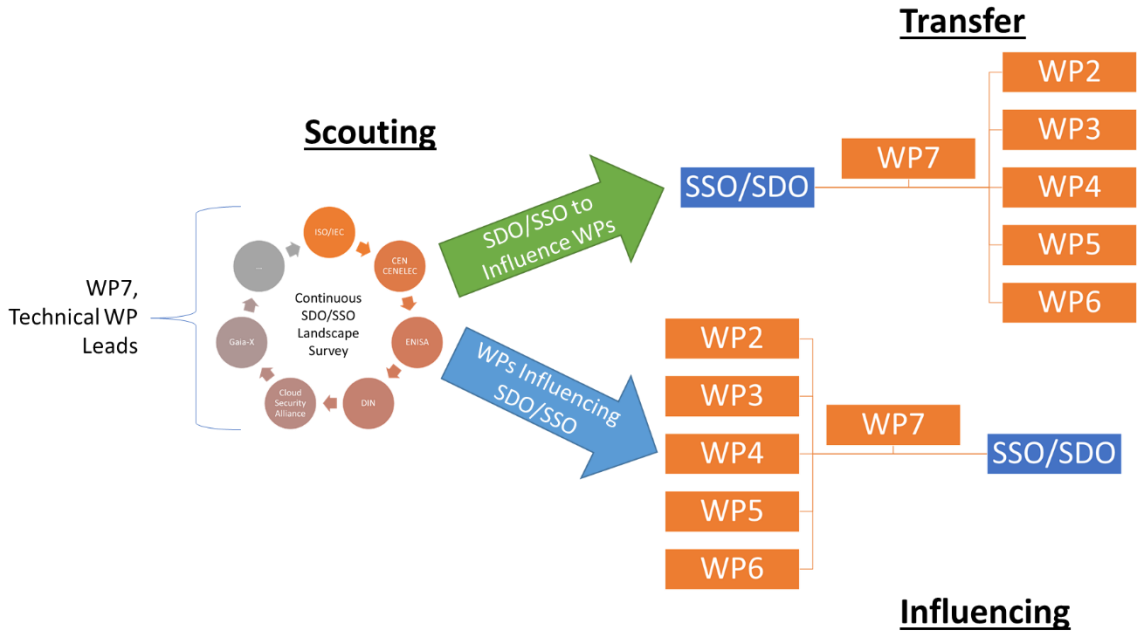

Figure 18. MEDINA's Approach to Standardization (D7.8)

APPENDIX B: Standardization Roadmap (excerpt as originally reported in D7.8)

The originally developed standardization Roadmap is shown in Table 5.

Table 5. MEDINA Roadmap (D7.8 [1])

Roadmap Topic	Prioritization	Rationale
Provide a catalogue of metrics as part of the implementation guidance for EUCS.	**High**	The notion of Metric is essential for triggering the different functionalities in the MEDINA framework, therefore its criticality from a project's perspective. We foresee most of our standardization activities going in the direction of contributing the developed catalogue (cf. D2.1 [19]) to relevant SSOs based on the presented strategy (cf. Section 2).
Support the notion of continuous (automated) assessments.	**High**	EUCS is the basis for MEDINA, not only due to the expected impact it will have in the EU CSP market, but also because it introduces the notion of continuous (automated) monitoring. In that sense, the project will continue its contributions both to ENISA and the technical specification being developed by CEN CENELEC.
Provide *implementation* guidance about EUCS requirements where some degree of automated monitoring is needed.	**Medium**	Guidance related to implementation of EUCS requirements is important for the uptake of this new certification scheme, although not critical for the adoption of MEDINA (at least not as the actual EUCS requirements are). Although the corresponding guidance will continue to be developed during the rest of the project's lifetime, its contribution to relevant SSO will be further discussed with ENISA.
Provide *audit/assessment* guidance related to EUCS requirements needing some degree of automated monitoring.	**Medium**	In analogy to the previous topic, the guidance related to audit/assessment for EUCS is also being developed by the project with the goal of contributing it to an SSO after discussing it with ENISA before the project's finalization.
Support development of machine-readable formats.	**Medium**	This topic is a consequence of the work being produced by the technical WPs in MEDINA, and despite it might greatly facilitate the adoption of the contributed framework, our belief is that it should not be a showstopper in the mid-term. Therefore, the proposal to continuously scout the relevant standardization landscape while continuing contributions to NIST.
Guidance on selecting tools/technologies for	**Low**	This guidance is important for early EUCS adopters, although our belief is that its development should be a consequence of

Roadmap Topic	Prioritization	Rationale
automated (continuous) monitoring.		MEDINA's exploitation activities (identification of potential market competitors).

APPENDIX C: Signed Memorandum of Understanding with StandICT.eu

Memorandum of Understanding (MoU)

This MoU is entered into by and between:

Trust-IT Srl (hereinafter also referred to as "Trust-IT"), an Italian company established in Via Francesco Redi 10 – 56124 Pisa (Italy), VAT number 01870130505, duly represented by its CEO, Ms Silvana Muscella

and

Fundación TECNALIA Research & Innovation (hereinafter also referred to as "TECNALIA"), a Spanish non-profit organization established in Parque Científico y Tecnológico de Bizkaia, Astondo Bidea, Edificio 700 – E-48.160 Derio (Bizkaia) Spain, duly represented by Mr. Joseba Mikel Laka Mugartza, Director of Digital.

hereafter individually referred to as "the Party" or, collectively, as "the Parties"

Whereas:

a) Trust-IT (www.trust-itservices.com) coordinates the StandICT.eu 2023 initiative (www.standict.eu), funded by the European Commission under the H2020 Framework Programme start date 1st September 2020 for a duration of 36 months.

b) StandICT.eu [2020-2023] is planning a series of Open Calls, for which technical topics will be discussed with as many competent interfaces as possible, to ensure they are relevant for the European community of ICT standardisation and so they can be included in the call topics.

c) TECNALIA is the coordinator of the MEDINA project "Security Framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme (https://medina-project.eu/) funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952633.

d) The MEDINA project has a holistic framework based on the following objectives:

- To provide Technical and Organizational Measures (TOMs) including associated quantitative/qualitative security metrics, machine-readable certification languages, and risk-based techniques to support security certification of cloud supply chains.
- To provide Security Validation Techniques, Processes and Tools, allowing cloud providers to gather trustworthy evidence of implemented TOMs, in accordance to defined assurance levels in the EU Cybersecurity Act.
- To implement and Integrate the Software Tools and Mechanisms to manage the life cycle of cloud security certifications, achieving the highest assurance

level defined by the EU Cybersecurity Act (e.g., continuous monitoring-based certification).

- To validate the outcomes in real use cases covering the three cloud service layers (IaaS, PaaS and SaaS).
- To raise the awareness on the benefits of the contributed framework in the context of the EU Cybersecurity Act, supporting activities related to European training, awareness and relevant standardization activities.

The Parties have agreed as follows:

Article 1 – Scope of the MoU –

- StandICT.eu 2023 may ensure these items are addressed on the call topic discussions in the forthcoming calls planned over the 36 months (2020-2023).
- Trust-IT will provide visibility to all outreach activities that MEDINA organises around efforts on the Cloud Cybersecurity and Cloud Certification, and contributions to ICT Standards (including, e.g. use cases and success stories) to its extensive network of stakeholder communities and through its main digital outlets.
- MEDINA will promote both the StandICT.eu Open Calls, as well as any other events/initiatives organised by StandICT.eu 2023, relative to its community of European organisations and specialists in Cloud Cybersecurity and Cloud Certification.
- The Parties may, with mutual consent, avail of each other's human resources to participate in any webinars or (virtual) events of mutual interest.
- The Parties may agree to co-organise events on topics of mutual interest.
- The Parties will cooperate on activities connected to the StandICT.eu 2023's "*EUOS – European Observatory for ICT Standardisation*", including the population of the StandICT.eu ICT Standards Repository and providing mutual support in creating synergies with other projects and initiatives active in the ICT standardization domain.
- In performing the activities envisaged by this MoU, each Party will bear its own costs and no remuneration, or reimbursement of costs is involved, on either side.

Article 2 – Non-favouritism

- This MoU, while being mutually beneficial for both StandICT.eu (via Trust-IT) and MEDINA (via TECNALIA) does not constitute an act of favouritism towards TECNALIA or its affiliates/partners, as the open calls that will be published on StandICT.eu will be evaluated by StandICT.eu's external evaluators, which will be checked for possible conflict of interest before being assigned the proposals submitted to the aforementioned open calls.

Article 3 – Confidentiality, Data Protection & Proprietary Rights

- It is understood that the Parties will not exchange any confidential information within the framework of this agreement. Should the exchange of confidential information become necessary or opportune, this will be the subject of a separate written agreement involving the other Partners of the MEDINA project.
- Any joint development made by the Parties as a direct consequence of this MoU will also be subject to the provisions of a separate written agreement to be executed by the Parties prior to the commencement of any such joint development work. The execution of this MoU shall in no way serve to create, on the part of either Party, a license to use, any proprietary rights of the other Party otherwise than explicitly stipulated herein.

Article 4 – Liability

- With respect to the information or data supplied by a Party to another Party under this MoU, the supplying Party shall be under no obligation or liability and no warranty or representation of any kind is made, given or to be implied as to the sufficiency, accuracy, or fitness for a particular purpose of such information or data or the absence of any infringement of any proprietary rights of third parties through the possession or use of such information or data. The recipient Party shall be entirely responsible for its use of such information or data and shall hold the other Party free and harmless and indemnify them for any loss or damage with regard thereto.

- No Party shall be responsible to the other Party for punitive damages, indirect or consequential loss or similar damage such as, but not limited to, loss of profit, loss of revenue or loss of contacts.

- The limitation of liability stated above shall not apply in (i) the case of damage caused by a proven wilful act of gross negligence, and (ii) in respect of any activity involving the wilful or grossly negligent misuse of anything protected by intellectual property rights of another Party and (iii) infringement of the confidentiality obligations of this agreement.

- Each Party shall be solely liable for any loss, damage, or injury to third parties in relation to its execution of this MoU.

Article 5 – Applicable law and Jurisdiction

- This MoU shall be governed by the laws of Belgium. All disputes arising in connection with the interpretation or implementation of this MoU shall be settled amicably.

- All disputes arising out of or in connection with this MoU which cannot be solved amicably within thirty (30) days, shall be finally settled under the courts of the city of Brussels.

Article 6 – Duration / Termination

The MoU will take effect after the signature of the two Parties and shall remain in force until the 31st of August 2023.

Each Party may terminate this MoU at any time by giving the other Party 30 days written notification (including motivation).

Signature page

For Trust-IT:

In its capacity as Coordinator of the StandICT.eu 2023 Project

Ms Silvana Muscella

Trust-IT S.r.l.
Via Francesco Redi, 10
56124 Pisa - Tel./Fax +39 050 28359
P.IVA 01870130505
www.trust-itservices.com

Date: 28/07/2022

For Fundación TECNALIA Research & Innovation:
In its capacity as Coordinator of the MEDINA Project

Mr. Joseba Mikel Laka Mugartza

Director of Digital

Date: 28/07/2022

APPENDIX D: TG2 Contribution Sample – CSEP Proof of Concept

The explanatory comments related to this document, authored by the MEDINA consortium, are summarized in the following table.

Table 6. MEDINA comments related to "CSEP PoC"

Comment ID	Reference in document (Page Number)	Submitted Comment
D1	**2**	In the CSEP spec we ask about "security Objectives" as part of the security story. In practice, does it mean a preliminary mapping to the EUCS requirements? All security objectives from the "core EUCS requirements" are relevant for the described use case.
D2	**4**	What about the unique ID for the CSEP requirement? Is it self assigned or shall it follow some naming convention?
D3	**4**	An IoT firmware might not be considered "customer data", but it's a best guess from our side
D4	**5**	See comment D4 on usage of unique IDs

EUCS Profile Development (Proof of concept) “Cloud Services Supporting IoT Products”

Author

Jesus Luna Garcia (Jesus.lunagarcia@de.bosch.com)

Introduction

IoT has become a pervasive technology which is (literally) embedded in almost all aspects of our daily life. IoT enables existing market verticals (e.g., industrial technology), creates new ones (e.g., smart home automation), and even converges with others like Artificial Intelligence to breed new paradigms.

Despite there is no standardized system model for representing the architecture of IoT ecosystems, the elements show in Figure 1 can be typically found in real-world deployments:

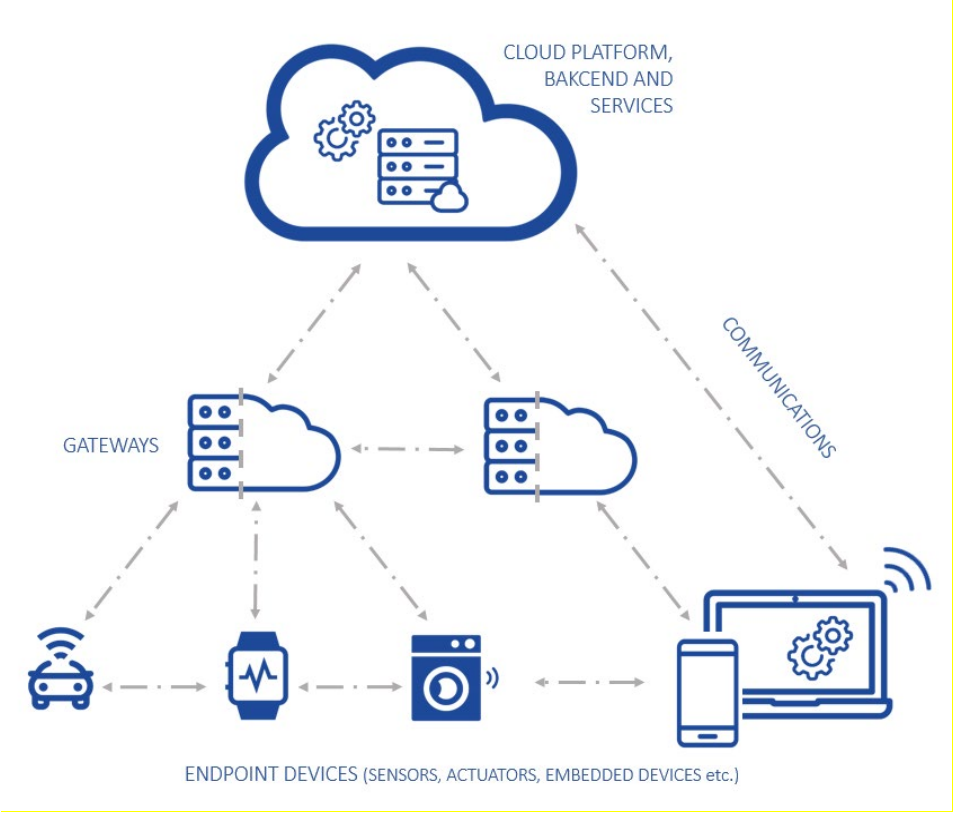

Figure 1 Architecture for IoT ecosystem with Cloud backends [1].

Citing from the ENISA report [1], “the cloud, in its different service and deployment models, is becoming the most accepted IoT backend to aggregate and process data from dispersed devices, and it also provides computing capabilities, storage, applications, services, etc. Due to this new paradigm IoT gives rise to, the cloud is consequently evolving towards different characteristics in the services they provide, in order to embrace IoT and adapt to this new environment with brand new needs and demands. While the physical infrastructure of the cloud did not change, the platform and software services that were

developed for enterprise IT management and mobility apps support became specific to IoT[1] creating a new model called "IoT Cloud". In short, this new model enables IoT developers to perform remotely tasks on IoT devices, such as to assess the status of their assets, review their specifications, configure or re-configure them, command or update them and extract any kind of statistics, values, and settings."

Security concerns associated with these new functionalities, raise the need for a CSEP covering the particularities of IoT Clouds.

Conformance Claims

This profile is conformant with EUCS core 10.2021, in particular related to assurance level XXXXXX.

Scope

The set of IoT Cloud assets to be covered by the proposed CSEP is based on the ENISA study [2] namely:

- Application services hosted in the cloud
- Database servers
- Decision systems
- Cloud platform (hyperscaler)
- Other supporting cloud services and resources (e.g., virtual networks, communication channels, and personnel).

Furthermore the proposed set of CSEP security requirements are derived from [1] and [3]

Security Story

Integration of cloud backends in IoT systems introduces new risks on the devices managed from the IoT cloud, in particular should the latter have been compromised. Security configurations in the cloud become even more critical in the case of IoT where such numerous and diverse devices are being monitored and managed.

Taking as baseline the analysis presented in ENISA's report on secure convergence of Cloud and IoT [1], we consider as relevant for the presented CSEP the following set of threats and security objectives:

Table 1. Security Threats and Security Objectives consider for the CSEP

Attack Scenario	Security Threat	Security Objective
Hosting the enemy (attacker interception/compromise of distributed IoT device's security patch)	• Outdated IoT devices • Heterogeneous protocols for communication • Insecure data flow from the Edge to the Cloud	• Secure communications, security stream analysis and security of data at rest • Addition of security elements to IoT environment • Automated, secure software updates • Automated security monitoring

[1] https://www.linkedin.com/pulse/from-cloud-iot-kaivan-karimi

Poisoned routes (compromised IoT device, allows unauthorized access and compromise of the cloud)	• Insecure data flow from the Edge to the Cloud • Real-time processing at the edge overshadows security	• Device virtualization to bring homogeneity • Secure communications, security stream analysis and security of data at rest • Physical and cyber security in edge devices • Strong authentication and authorization management for IoT devices • Automated security monitoring
Reaping the harvest (privilege escalation on IoT management console allows unauthorized access/controls of other devices)	• Security depends on the vertical that cloud is serving • Security relies much on the implementation from developers	• Adoption of baseline security measures • End-to-end security, through the whole environment • Secure DevOps • Strong authentication and authorization management for IoT devices • Automated security monitoring • Automated vulnerability scanning
Open House (insider compromises high-value IoT Cloud services like API Gateway)	• Security relies much on the implementation from • IoT developers • Insider	• Secure communications, security stream analysis and security of data at rest • End-to-end security, through the whole environment • Data at rest encryption • Employee security • Training and awareness • Separation of duties

Security Requirements

In Table 2 and Table 3 are shown the proposed set of (either extended or new) requirements for this CSEP candidate based on the EUCS document from November 2021. The proposed CSEP requirements are derived as security measures to accomplish the Security Objectives shown in Table 1.

New Requirements

Table 2. New CSEP Requirements - Categorization based on EUCS 11.2021

Existing Domain	Existing Category	Existing Objective	Existing Control ID	Existing Control	Existing Control Objective	Assurance Level	CSEP New Requirement (proposed)	Traceability / Rationale
A13	Development of Information Systems	Ensure information security in the development cycle of information systems	DEV-01	POLICIES FOR THE DEVELOPMENT AND PROCUREMENT OF INFORMATION SYSTEMS	Policies are defined to define technical and organisational measures for the development of the cloud service throughout its lifecycle	High	The CSP shall document custom changes made to any IoT device virtualization format or tool being used.	See "Device virtualization to bring homogeneity" in Table 1. Based CSA CCMv3.01
A13	Development of Information Systems	Ensure information security in the development cycle of information systems	DEV-03	SECURE DEVELOPMENT ENVIRONMENT	The development environment takes information security in consideration	High	The CSP shall implement a secure staging system for over-the-air updates to protect IoT devices from intrusion and malicious logic.	See "Automated, secure software updates" in Table 1. Based CSA IoT Security Controls Framework v2
A9	Cryptography and Key Management	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information	CKM-02	ENCRYPTION OF DATA IN TRANSIT	Cloud customer data communicated over public networks is protected in confidentiality, integrity, and authenticity.	High	The CSP shall apply integrity controls to IoT firmware files before transmitting them to edge devices.	See "Automated, secure software updates" in Table 1. Based CSA IoT Security Controls Framework v2

Extended Requirements

Table 3. Extended EUCS Requiremenst

EUCS Assurance Level	EUCS Requirement ID (current)	EUCS Requirement (current)	CSEP Extended Requirement (proposed)	Traceability / Rationale
High	DEV-01.3S	The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools.	The policies and procedures for IoT device virtualization shall use industry-recognized standard formats to ensure interoperability.	See “Device virtualization to bring homogeneity” in Table 1. Based CSA CCMv3.01

Bibliography

[1] ENISA, "Towards secure convergence of Cloud and IoT," 17 September 2018. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot. [Accessed 19 11 2021].

[2] ENISA, "Baseline Security Recommendations for IoT," 20 November 2017. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. [Accessed 19 11 2021].

[3] CSA, "CSA IoT Security Controls Framework v2," 28 01 2021. [Online]. Available: https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/. [Accessed 19 11 2021].

APPENDIX E: TG8 Contribution Sample – EUCS Guidance for Category CKM

MEDINA's feedback to this document is summarized in the following table.

Table 7. MEDINA feedback submitted to ENISA Ad Hoc WG EUCS TG8 (excerpt)

Comment ID	Reference in document (Page Number)	Submitted Comment
E1	**6**	Some years ago, while writing the EU guidelines for Cloud Security SLAs, we were asked to include EU-specific references to "whitelisted" crypto algorithms. Probably these are now ETSI / CEN CENELEC/BSI specs.
E2	**6**	The table with the explanation of these icons is missing in this document.
E3	**6**	Do you mean "specific aspects related to this requirement"?
E4	**7**	Based on previous experiences there was a clear guideline on referring to EU-recommendations/standards/specs. Consider providing the very specific name of the documents, to avoid ambiguities.
E5	**7**	Does the document mean "review" in the sense of an "audit"?
E6	**7**	Please refer to E4.
E7	**7**	What do you mean with "clues"?
E8	**8**	I don't see why this paragraph is needed, furthermore it might cause confusions with topics like "VPC" (see AWS) which are not really falling into this concept.
E9	**8**	I'm not sure about this, because that's the reason behind concepts like network peering between clouds, or other mechanisms (e.g., ExpressRoute) which provide for this kind of access control.
E10	**8**	Consider proof reading to split in smaller sentences. Also, for clarity you might want to consider providing illustrative examples. E.g., is inter-region considered in this definition?
E11	**8**	Given the nature of this guidance, would it be worth to add an example? Something this XYZ hash function is well suited for XYZ risk level.
E12	**8**	Consider answering the question, protected against what?

Comment ID	Reference in document (Page Number)	Submitted Comment
E13	**8**	What about CSP-data moving across public networks? Please clarify.
E14	**9**	Please be more specific on the sentence.
E15	**9**	Up this this point, most of the provided guidance goes in the direction of “confidentiality”, but what about “integrity” and “authenticity” as mentioned on the Requirement?
E16	**9**	Here you can discuss about the usage of cryptographic (VPN) tunnels, but also consider highlighting that the usage of crypto does not excludes leveraging other security mechanisms like strong authentication.
E17	**9**	We agree on the provided guidance, but only in cases related to public networks e.g., inter-region. It does not apply to a CSP backbone if it’s maintained within their private network boundaries.
E18	**10**	What is the difference between that concept and the previous bullet (Encrypt the data)?
E19	**10**	Access controls refers to authorization, whereas passwords/2FA is about authentication. For the former consider concepts like ACLs, RBAC, etc.
E20	**10**	The provided statement applies to most (if not all) of the EUCS1 requirements.
E21	**10**	What is the threat vector in this case whereas HW-level encryption provided by the CSP isn’t enough? Even if the CSC encrypts at rest, the data is “cleartext” while being processed by the DBMS or Web App. Also, why CSC-guidance is needed? Is this for the CSP to document then as CUEC?
E22	**10**	Add some guidance about timeliness related to the updates, so CSC can have time to migrate (if needed) to the new crypto schemes. Consider providing examples whereas not all layers of storage might be encrypted (HW -> Virtual Bucket -> DBMS)
E23	**10**	Given the associated threat model for BYOK, I would suggest moving to CS-High.
E24	**11**	See comment D4 about EU-specific guidance, otherwise also add reference to the well-known FIPS standard.

Comment ID	Reference in document (Page Number)	Submitted Comment
E25	**11**	Proof read this sentence.
E26	**11**	Consider providing illustrative examples of both kinds of crypto modules.
E27	**11**	Add guidance on what a “Trusted PKI” means? Is it Qualified PKI, is it PKI from the hyperscaler?
E28	**12**	Is key escrow allowed?
E29	**12**	Is this residual risk supposed to be documented / notified to the CSC? Also, what about processes for key rotation? What about PKI-specific process for managing certificates (even wildcard certificates)? Does the same guidelines apply for encryption keys issues to Technical Accounts (App Key, or Service Principal keys)?
E30	**13**	There are many HSM-as-a-Service (e.g., KeyVaults) solutions offered by hyperscalers, what about these? Those are particularly attractive for small SaaS.
E31	**13**	Be careful with this statement, because there are also attack scenarios against the HSM.
E32	**14**	What do you mean with “equivalent”? The requirement also opens the possibility for software modules, so these should be also explained in the guidance.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCS GUIDANCE

Guidance on the requirements on controls for cloud Services (Sample – Category “CKM”)

DECEMBER 2022

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
Table text	Table text	Table text	Table text
Table text	Table text	Table text	Table text

1. CRYPTOGRAPHY AND KEY MANAGEMENT

1.1 KEY CONCEPTS

1.1.1 Cryptography

Cryptography is the practice of securely communicating information in the presence of third parties or on an insecure communication channel through the use of codes, ciphers, and other techniques to protect the confidentiality, integrity, and authenticity of the information. It involves the use of mathematical algorithms and protocols to secure communication channels, protect data from unauthorized access, and verify the identity of an entity. Cryptography is used in a wide range of applications, including online communication, banking and financial transactions, and data storage. It is an essential tool for protecting sensitive information and maintaining the privacy and security of individuals and organizations.

Cryptography is used to perform or support the fundamental security services listed below such as

- Confidentiality – Assurance that information is not disclosed to unauthorized users. Cryptography can render information unreadable except to those whom have authorization to read it. To provide confidentiality, encryption must be performed with a cryptographic algorithm in such a way that an unauthorized party is unable to access the private key or access the information without first applying the correct keys.
- Data Integrity – Assurance is needed that data is not modified in an unauthorized manner since its creation, transmittal or storage. Cryptographic mechanisms such as digital signatures can be used to detect both deliberate and accidental modifications.
- Authentication – Cryptography can provide two types of authentication services, integrity authentication and source authentication through digital signatures and several key-agreement techniques.
- Authorization – Permission for access or to perform a specific access can be supported through the use of a cryptographic service that is used to provide a key to allow access.
- Non-Repudiation – When non-repudiation is required, digital signature keys and certificates are created via cryptography that are bound to the name of the certificate subject. For example, this would be used for obtaining a digital signature that would carry the same legal weight as a handwritten signature

1.1.2 Cryptographic mechanisms

1.1.2.1 Encryption

This is the process of converting plaintext into ciphertext, which is a form of text that cannot be understood without the appropriate decryption key. Encryption helps to protect the confidentiality of data by making it unreadable to anyone who does not have the decryption key.

1.1.2.2 Decryption

This is the process of converting ciphertext back into plaintext using the appropriate decryption key. Decryption allows authorized users to read and access the original, unencrypted data.

1.1.2.3 Key

a secret piece of information that is used in conjunction with a cipher to encrypt and decrypt data.

1.1.2.4 Hash function

a mathematical function that takes an input (or "message") and produces a fixed-size output (or "hash value") that is unique to the input. Hash functions are often used to verify the integrity of data by comparing the computed hash value to a previously stored hash value.

Digital signature: a mathematical technique used to verify the authenticity of a digital message or document. A digital signature is created using the sender's private key and can be verified using the sender's public key.

1.1.3 Key Management

Kerckhoffs's principle is one of the basic principles of modern cryptography. The principle goes as follows: A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

Since all the strength of the cryptography rests on the secrecy of the key, this principle emphasizes the importance to properly manage cryptographic keys.

The key management refers to the processes and systems used to generate, distribute, store, and protect keys. Effective key management is essential for ensuring the security and integrity of encrypted data.

1.1.4 Risks related to key management

There are many threats that can result in a key being compromised – often it's impossible to even know the key has been compromised until it has been exploited by the attacker, which makes the threats all the more dangerous. Here are some of the major threats that could be considered:

- **Weak keys**: A key is essentially just a random number – the longer and more random it is, the more difficult it is to crack. It is important to define an appropriate key strength for the value of the data it is protecting and the period of time for which it needs to be protected. As well as generate keys using a high-quality (ideally certified) random number generator (RNG), ideally collecting entropy from a suitable hardware noise source. There are many instances where poor RNG implementation has resulted in key vulnerabilities.
- **Incorrect use of keys**: The use of a key which was not generated for the specific purpose for which it is used may not provide the expected or required level of protection.
- **Re-use of keys**: Improper re-use of keys in certain circumstances can make it easier for an attacker to crack the key.
- **Non-rotation of keys**: If a key is over-used (e.g. used to encrypt too much data), then it makes the key more vulnerable to cracking and cryptanalysis; it also means that a high volume of data could be exposed in the event of key compromise. A key rotation (i.e. update / renewal) at appropriate intervals, is a way to avoid this.
- **Inappropriate storage of keys**: If keys are stored alongside the data that they protect (e.g. on a server, database, etc.), any exfiltration of the protected data likely compromise the key also.
- **Inadequate protection of keys**: Key is used to protect data, but they also need protection, if keys are easily accessible to an attacker all the data protected by these are not protected anymore. There have been a number of vulnerabilities that could expose cryptographic keys in server memory including Heartbleed, Flip Feng Shui and Meltdown/Spectre.

- **Insecure movement of keys**: It is often necessary to move a key between systems. If keys are transported in a unsecure manner, the leak of keys may lead to lost of confidentiality of data protected by these keys.
- **Non-destruction of keys**: If keys are not destroyed (i.e. securely deleted, leaving no trace) once they have expired, unless explicitly required for later use (e.g. to decrypt data), this increase the risk of accidental compromise at some future date.
- **Lack of resilience**: Not only must the confidentiality and integrity of keys be protected, but also their availability. If a key is not available when required, or worse still lost due to some fault, accident or disaster with no backup available, then the data it is protecting may also be inaccessible / lost.
- **Lack of audit logging**: If the key lifecycle is not fully recorded or logged, it will be more difficult to identify when a compromise has happened and any subsequent forensic investigation will be hampered.
- **Manual key management processes**: The use of manual key management processes, using paper or inappropriate tools such as spreadsheets and accompanied by manual key ceremonies, can easily result in human errors that often go unnoticed and may leave keys highly vulnerable.

1.1.5 Data Classification Schemes

There are different classification schemes that can be used, depending on the needs of an organization and the type of data being classified. Some common classification schemes include:

- **Confidentiality**: This classification scheme is based on the sensitivity of the data and the potential impact on the organization if it were to be disclosed. Data is typically classified as public, internal, confidential, or secret based on its level of sensitivity.
- **Accessibility**: This classification scheme is based on the need to access the data and the level of authorization required to do so. Data is typically classified as public, restricted, or private based on the level of access required.
- **Integrity**: This classification scheme is based on the importance of the data and the potential impact on the organization if it were to be compromised or altered. Data is typically classified as low, medium, or high based on its level of importance.
- **Availability**: This classification scheme is based on the need to access the data and the potential impact on the organization if it were not available. Data is typically classified as high, medium, or low based on the level of availability required.

Data classification schemes help organizations to establish clear policies and procedures for managing and protecting their data, and to ensure that the appropriate level of security is applied to different types of data based on their sensitivity and importance.

1.1.6 Legal and regulatory obligations and requirements related to cryptography

There are a number of legal and regulatory obligations and requirements related to cryptography that may vary depending on the jurisdiction in which the CSP is located. Some common considerations include:

- **Export controls**: Many countries have laws and regulations that restrict the export of certain cryptographic technologies. These laws may apply to both the export of hardware and software containing cryptographic functionality, as well as to the provision of related services.
- **Intellectual property**: There may also be intellectual property considerations related to the use of cryptographic technologies, such as patents or trademarks. It is important to ensure that any cryptographic technologies you use do not infringe on the intellectual property rights of others.

- **Law enforcement**: Some jurisdictions may have laws that allow law enforcement agencies to request access to encrypted data or to require that companies provide assistance in decrypting data. It is important to understand any legal obligations CSP may have in this regard, as well as any potential limitations on your ability to protect the privacy of CSP's customers or users.
  This kind of enforcement could have a structural impact with the obligation to implement key escrow for example.
- **Producing license**: In some country sellers, manufacturers of cryptography products or cryptography service provider must obtain a license before distributing

1.2 REFERENCES

1.2.1 External references Related to requirements

Reference	Description	Note
[OWASP]	Key Management Cheat Sheet	
[ISO27002]	[ISO27002] defines several controls related to identity, authentication and access control management, which are referred to in the description of the controls.	
[ISO19790]	ISO/IEC 19790:2012 defines the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems.	
[ISO24759]	ISO/IEC 24759:2017 specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012.	

1.3 SECURITY CONTROLS

1.3.1 CKM-01 Policies for the Use of Cryptography and Key Management

1.3.1.1 Involved actors

Actors					
					

1.3.1.2 Objective

Policies and procedures for cryptography and key management related to the cloud service, including technical and organisational safeguards, are documented, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.

1.3.1.3 Requirement and recommendation

Level	Requirements	Recommendations
Basic	**The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management related to the cloud service, according to ISP-02, in which at least the following aspects are described:**	**The key requirements for the definition, communication and distribution of policies and procedures are defined in ISP-02.** **About the specific aspects to be covered in the policies:** • **Cryptographic mechanisms and communication protocols could be**

	• **Usage of strong cryptographic mechanisms and secure communication protocols;** • **Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys;** • **Consideration of relevant legal and regulatory obligations and requirements.**	**considered as strong and secure if its usage is recommended by a recognized organization as a NCCA (i.e. BSI, ANSSI, etc…) or independent, non-governmental international organization/agency (i.e. ISO, NIST, etc…).** **The length of the key used is also an important factor to determine the robustness of encryption. Therefore the length of the key used should respect the criteria described in the above mentioned recommendation in order to consider that the cryptographic mechanism used is strong.** **It is also important to regularly update and review the cryptographic mechanisms as well as key sizes being used to ensure that they are still considered strong. A mechanism considered strong at one time may no longer be so at another.** • **The secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys refers to key management concept. Section 8.24, "Use of Cryptography", of the ISO27002 gives clues on how to achieve this kind of implementation.** • **There are a number of legal and regulatory obligations and requirements related to cryptography that may vary depending on the jurisdiction in which the CSP is located. Some common considerations are described in key concepts section.**
Substantial	The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management related to the cloud service, according to ISP-02, in which at least the following aspects are described: • Usage of strong cryptographic mechanisms and secure communication protocols, **corresponding to the state of the art**; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; • Consideration of relevant legal and regulatory obligations and requirements. • **Risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption.**	**There are two main additions for CS-Substantial which are:** • **The introduction of the notion of "state-of-the-art" for the strong mechanism and secure protocol. This will be defined in a dedicated cryptography guidance, to be worked on with the ECCG. Note that the state of the art to be considered may not be the same at all levels. At level Substantial, state of the art may be mostly about using proper algorithms, whereas at High, it should include resistance against state of-the-art crypto attacks. Some recent document produced in cooperation with ENISA and currently use for personal data protection, can give some clue about "state of the art algorithm" pending the publication of the ECCG guidance.[1]** • **The obligation to have a data classification scheme and to perform risk-based provisions for the use of encryption which allow the CSP to determine how a**

[1] https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/?tx_reintdownloadmanager_reintdlm%5Bdownloaduid%5D=10505&cHash=f39d74868a8b38e98e6cc09b0ab16f6f

		particular data should be protected. The protections for a data classified as "confidential" could be different than the protections for a data classified as "secret".
High	The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management related to the cloud service, according to ISP-02, in which at least the following aspects are described: • Usage of strong cryptographic mechanisms and secure communication protocols, corresponding to the state of the art; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; • Consideration of relevant legal and regulatory obligations and requirements. • Risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption	**The requirement is unchanged from CS-Substantial.**

1.3.2 CKM-02 Encryption of Data in motion

1.3.2.1 Involved actors

Actors					
					

1.3.2.2 Objective

CSC data transmission and CSP remote access over public networks both to, or by, the CSP is protected in confidentiality, integrity, and authenticity.

1.3.2.3 Requirement and recommendation

Level	Requirements	Recommendations
Basic	**The CSP shall select and implement strong cryptographic mechanisms for the transmission of CSC data both to, or by, the CSP over public networks, in order to protect the confidentiality, integrity and authenticity of data.**	**A private network is a network wherein restrictions are established to promote a secured environment. CSP private network will be all the communication network which is fully under its control.** **Contrary, a public network will be network which are not under the CSP control, on when the CSP could not setup access control.** **Typically when data transit from the CSP to CSCs, they leave the private network of the CSP or the CSCs and transiting over "Internet", which is a public network, to reach the target.** **Since data are transiting over a network which can be "access by anyone", they need to be protected.** **At this level the data to be protected is only CSC data.**

		Cryptographic mechanisms and communication protocol could be considered as strong and secure if its usage is recommended by a recognized organization as a NCCA (i.e. BSI, ANSSI, etc…) or independent, non-governmental international organization/agency (i.e. ISO, NIST, etc…). **The length of the key used is also an important factor to determine the robustness of encryption. Therefore the length of the key used should respect the criteria described in the above mentioned recommendation in order to consider that the cryptographic mechanism used is strong.** **It is also important to regularly update and review the cryptographic mechanisms as well as key sizes being used to ensure that they are still considered strong. A mechanism considered strong at one time may no longer be so at another.**
	The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.	
Substantial	The CSP shall select and implement strong cryptographic mechanisms for the transmission of CSC data both to, or by, the CSP over public networks, in order to protect the confidentiality, integrity and authenticity of data.	**The requirement is unchanged from CS-Basic.**
	The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.	**The requirement is unchanged from CS-Basic.**
High	The CSP shall select and implement strong cryptographic mechanisms for the transmission of **all** data both to, or by, the CSP over public networks, in order to protect the confidentiality, integrity and authenticity of data.	**At this level not only the CSC data should be protected but all the data coming from or going to the CSP.**
	The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.	**The requirement is unchanged from CS-Substantial.**

1.3.3 CKM-03 Encryption of Data at Rest

1.3.3.1 Involved actors

Actors					
					

1.3.3.2 Objective

The CSP has established procedures and technical safeguards to prevent the disclosure of CSC data during storage.

1.3.3.3 Requirement and recommendation

Level	Requirements	Recommendations

Basic	**The CSP shall select and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.**	**The key requirements for the definition, communication and distribution of policies and procedures are defined and shall be documented according to ISP-02.** **There are several ways to protect the confidentiality of data during storage:** • **Encrypt the data: One of the most effective ways to protect the confidentiality of data is to encrypt it.** • **Use secure storage solutions: There are various storage solutions available that are designed to protect the confidentiality of data. These can include hardware-based storage solutions such as encrypted hard drives and solid-state drives.** • **Implement access controls: It's important to limit access to data to only those who need it. This can be done through the use of access controls, such as passwords and two-factor authentication.** **Depending on the type of service offered by a CSP, the approach of protecting data at rest and the split of responsibility for protecting data are not the same.** **CSPs that offer SaaS have greater control over encryption of CSC data than CSPs that offer IaaS only. SaaS providers could encrypt data from CSPs at the database level, application level, or file system level, whereas IaaS providers could only perform full disk encryption. In the latter case, CSC remains responsible for encrypting data at the database or application level.**
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	
Substantial	The CSP shall select and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	**The requirement is unchanged from CS-Basic.**
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	**The requirement is unchanged from CS-Basic.**
	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be established in accordance with applicable legal and regulatory obligations and requirements and contractually agreed with the CSC.	**There are a number of legal and regulatory obligations and requirements related to cryptography that may vary depending on the jurisdiction in which the CSP is located. Some common considerations are described in key concepts section.** **In order to enable public cloud users to maintain control of the cryptographic keys used in the cloud to keep their data secured, innovative solutions have been developed as the Bring your own key (BYOK) concept. BYOK enables public cloud users to generate their own high quality master key locally on-premises, and securely transfer the key to**

		their CSP to protect their data across cloud deployments. If this kind of solution or any equivalent exist a procedure should frame it.
High	The CSP shall select and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	**The requirement is unchanged from CS-Substantial.**
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	**The requirement is unchanged from CS-Substantial.**
	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be established in accordance with applicable legal and regulatory obligations and requirements and contractually agreed with the CSC.	**The requirement is unchanged from CS-Substantial.**

1.3.4 CKM-04 Secure Key Management

1.3.4.1 Involved actors

Actors					
					

1.3.4.2 Objective

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys that are used to provide the cloud service.

1.3.4.3 Requirement and recommendation

Level	Requirements	Recommendations
Basic	**Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects:** • **Generation of keys for different cryptographic systems and applications;** • **Issuing and obtaining public-key certificates;** • **Provisioning and activation of the keys;** • **Secure storage of keys including description of how authorised users get access;** • **Changing or updating cryptographic keys including policies defining under which conditions and in which**	**The key requirements for the definition, communication and distribution of policies and procedures are defined in ISP-02.** **About the specific aspects to be covered in the policies:** • **Cryptographic keys should be generated within cryptographic module with at least an ISO/IEC 19790:2012 and ISO/IEC 24759:2017 compliance. For explanatory purposes, consider the cryptographic module in which a key is generated to be the key-generating module. Any random value required by the key-generating module shall be generated within that module; that is, the Random Bit Generator that generates the random value shall be implemented within cryptographic module with at least an ISO/IEC 19790:2012 and ISO/IEC 24759:2017 compliance that generates the key. Hardware cryptographic modules are preferred over software cryptographic modules for protection.** • **Issuing and obtaining public-key certificates should be manage by a Trusted PKI.**

	manner the changes or updates are to be realised; • **Handling of compromised keys; and** • **Withdrawal and deletion of keys;**	• **The generated keys shall be transported (when necessary) using secure channels and should be used by their associated cryptographic algorithm within at least an ISO/IEC 19790:2012 and ISO/IEC 24759:2017 compliant cryptographic modules.** • **The CSP should ensure that when keys are stored they are :** ○ **protected on both volatile and persistent memory, ideally processed within secure cryptographic modules.** ○ **never stored in plaintext format.** ○ **are stored in cryptographic vault, such as a hardware security module (HSM) or isolated cryptographic service.** ○ **encrypt using Key Encryption Keys (KEKs) prior to the export of the key material, if they are stored in offline devices/databases. KEK length (and algorithm) should be equivalent to or greater in strength than the keys being protected.** ○ **Protected against integrity tampering.** • **A compromise-recovery plan is essential for restoring cryptographic security services in the event of a key compromise. A compromise-recovery plan shall be documented and easily accessible. The compromise-recovery plan should contain:** ○ **The identification and contact info of the personnel to notify.** ○ **The identification and contact info of the personnel to perform the recovery actions.** ○ **The re-key method.** ○ **An inventory of all cryptographic keys and their use (e.g., the location of all certificates in a system).** ○ **The education of all appropriate personnel on the recovery procedures.** ○ **An identification and contact info of all personnel needed to support the recovery procedures.** ○ **Policies that key-revocation checking be enforced (to minimize the effect of a compromise).** ○ **The monitoring of the re-keying operations (to ensure that all required operations are performed for all affected keys).** ○ **Any other recovery procedures, which may include:** ○ **Physical inspection of the equipment.** ○ **Identification of all information that may be compromised as a result of the incident.** ○ **Identification of all signatures that may be invalid, due to the compromise of a signing key.** ○ **Distribution of new keying material, if required.** • **If keys are not destroyed (i.e. securely deleted, leaving no trace) once they have expired, unless explicitly required for later use (e.g. to decrypt data), this increases the risk of accidental compromise at some future date**
Substantial	Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects:	**The requirement is unchanged from CS-Basic.**

	• Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes or updates are to be realised; • Handling of compromised keys; and • Withdrawal and deletion of keys;	
	For the secure storage of keys, the key management system shall be separated from the application and middleware levels.	**The CSP could consider use HSM.** **A hardware security module (HSM) is a physical computing device that protects digital key management and key exchange, and performs encryption operations for digital signatures, authentication and other cryptographic functions. It can be thought of as a "trusted" network computer for performing cryptographic operations. A HSM is secure because it:** **○ Is built on top of well-tested, lab certified hardware.** **○ Has a security-focused OS.** **○ Has limited access via a network interface controlled by internal rules.** **○ Actively hides and protects cryptographic material.** **HSMs may have tamper evidence features such as visible signs of tampering, tamper resistance where tampering makes the HSM inoperable, or tamper responsiveness such as deleting keys upon tamper detection. Many HSM systems have secure backup systems, which allows keys to be backed up and stored on a computer disk or externally using a secure portable device. HSMs are usually certified to internationally recognized standards, such as Common Criteria (e.g. using Protection Profile EN 419 221-5, "Cryptographic Module for Trust Services") or FIPS 140 (currently the 3rd version, often referred to as FIPS 140-3) to provide users with independent assurance that the design and implementation of the product and cryptographic algorithms are sound.** **The best way of protecting cryptographic material is using a hardware component that is designed for this purpose. Hardware security modules (HSM, TPM, etc.) usually offer both key storage and cryptographic operation acceleration in the same module.** **All cryptographic work should be done in the vault (such as key access, encryption, decryption, signing, etc).**
	If pre-shared keys are used, the specific provisions relating to the secure use of this procedure shall be specified separately.	

High	Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes or updates are to be realised; • Handling of compromised keys; and • Withdrawal and deletion of keys;	**The requirement is unchanged from CS-Substantial.**
	For the secure storage of keys, the key management system shall be separated from the application and middleware levels.	**The requirement is unchanged from CS-Substantial.**
	For the secure storage of keys and other secrets used for the administration tasks, the CSP shall use a suitable software or hardware security container.	**The CSP should use an HSM or equivalent.**
	If pre-shared keys are used, the specific provisions relating to the secure use of this procedure shall be specified separately.	**The requirement is unchanged from CS-Substantial.**

1.4 TERMINOLOGY

Term	Definition
data at rest	structure, or group of structures, dedicated to the centralized accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function. Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building
data in motion	data being transferred from one location to another Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device).
policy	intentions and direction of an organization, as formally expressed by its top management
procedure	specified way to carry out an activity or a process Note 1 to entry: Procedures can be documented or not.
state-of-the-art	developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the "generally acknowledged state of the art".
strong	not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built [SOURCE: From ISO/IEC 19790:2012, 3.123]

Term	Definition
authentication	provision of assurance that a claimed characteristic of an entity is correct. [SOURCE: ISO/IEC 27000:2018, 3.5]
authenticity	property that an entity is what it claims to be Note 1 to entry: Authenticity is judged on the basis of evidence. [SOURCE: ISO/IEC 27000:2018, 3.6, modified — Note 1 to entry has been added.]
authorised	To be explicitly allowed. ISO/IEC/IEEE 8802-11:2022(en), 3.1.21
compromised keys	Cryptographic key that is no longer able to ensure the security need for which it is used.
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes [SOURCE: ISO/IEC/IEEE 27000:2018]
cryptographic keys	A parameter that determines the operation of a cryptographic function such as a) The transformation from plain text to cipher text and vice versa b) Synchronized generation of keying material c) Digital signature computation or validation.

	ISO/IEC/IEEE 8802-1AE:2020(en), 3.9
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext (3.1), i.e. to hide the information content of the data [SOURCE: ISO/IEC 18033-1:2015, 2.21]
Data integrity	property that data has not been altered or destroyed in an unauthorized manner [SOURCE: ISO/IEC 9797-1:2011, 3.4]
pre-shared keys	shared key that is established prior to the initiation of the function that requires its use ISO/IEC 14776-454:2018(en), 3.1.110
private keys	private key which defines the private signature transformation [SOURCE:ISO/IEC 9798-1]
public-key certificates	public key information of an entity signed by the certification authority and thereby rendered unforgeable [SOURCE:ISO/IEC 9798-1]

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

APPENDIX F: Contribution to EUCS1 on Continuous Automated Monitoring

MEDINA

Continuous Monitoring in EUCS1 6th WD

Presenter: Jesus Luna Garcia

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

1

Some facts

MEDINA

- Current definition in EUCS1:

120 Continuous monitoring

121 The requirements related to continuous monitoring that typically mention "monitor automatically " in their
122 text, is about gather data by non-human means. These requirements can be supplemented by continuous
123 auditing, because technologies have not reached an adequate level of maturity. The introduction of automated
124 monitoring requirements is intended to utilize the available technology.

- Automated Monitoring referred in 34 out of 427 **CS-High** requirements (< 8%)

2

Excerpt from EUCS1

EUCS1 ReqID	Text
OIS-02.4H	The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
ISP-03.5H	The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.
HR-03.4H	All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.
HR-04.3H	The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program.
HR-05.2H	The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure.
HR-06.2H	The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptation shall be automatically monitored.
HR-06.3H	The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptation shall be automatically monitored.
HR-06.5H	The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptation shall be automatically monitored.

3

Excerpt from EUCS1 (cont'd)

EUCS1 ReqID	Text
AM-01.4H	The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.
AM-03.4H	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.
AM-04.1H	The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored.
PS-02.8H	The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored.
OPS-02.2H	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards.
OPS-05.3H	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.
OPS-07.2H	In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP.
OPS-09.2H	When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup.
OPS-12.1H	The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation.
OPS-12.2H	The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H).
OPS-13.1H	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data.
OPS-18.6H	The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC.
OPS-21.1H	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements.

4

Excerpt from EUCS1 (cont'd)

EUCS1 ReqID	Text
IAM-03.1H	The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons.
IAM-03.2H	The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application
IAM-03.5H	The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application.
IAM-03.6H	The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant.
CCM-04.1H	The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored.
CCM-05.1H	The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights.
PM-04.7H	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling).
PM-04.8H	The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action.
IM-02.5H	The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures.

5

Excerpt from EUCS1 (cont'd)

EUCS1 ReqID	Text
CO-03.5H	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions.
CO-03.6H	The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP's subject matter experts for immediate assessment and action.
INQ-03.4H	The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.
PSS-04.2H	An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails.

6

Discussion: Continuous Monitoring versus Automated Monitoring

MEDINA

- Continuous Monitoring does not always imply Automated Monitoring:

> *If you want to monitor the perimeter of your facility, you can place a (human) guard every few meters around your fence who observe the environment. If the guards are there 24/7, you have continuous monitoring without automation. It is obvious that this approach does not scale, and the larger and more complex the facility grows, the less (economically) feasible the guard approach gets. You might then want to replace the guards by cameras and have a control center where humans observe the perimeter on a screen – this would be the first step towards automation (even if it doesn't go very far in this direction). But also this semi-automated approach might not scale, and eventually you will end up with an image processing system that automatically creates alerts and notifies a security officer. This would then be automated monitoring (but not yet fully automated, since there is still a human in the loop).*

7

Discussion: Continuous Monitoring versus Automated Monitoring

MEDINA

- The complexity expected from cloud services in the scope of CS-High, might result in the impossibility to implement "continuous monitoring" without automation.
  - Reminder: CS-High is *"intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources"*

8

Are we there yet?

MEDINA

- C5:2020 proposes 53 controls (out of 121) where continuous auditing with automation is considered feasible for cloud services.
  - EUCS1 approach is more conservative in this respect ☺
- Automation explicitly mentioned in NIST SP 800-53 (e.g. AC-2.1) and FedRAMP (see Flaw Remediation in continuous monitoring strategy)
- For "cloud native requirements", we have found good coverage (> 70%) in available CSPM technology like:
  - Defender for Cloud (Azure), Security Command Center (GCP), SecurityHub (AWS)
  - 3rd party (e.g., PrismaCloud),
  - OSS (e.g., Fraunhofer Clouditor)
  - Strong (MEDINA) collaboration with Azure and GCP product groups to further align CSPM capabilities

Automated Monitoring in EUCS1

MEDINA

- *Automated monitoring* in EUCS1 was conceived as a first step to the ultimate goal of enabling *continuous auditing* with automation.
- This is aligned with C5:2020 vision of "Continuous Auditing":

> • Notes on Continuous Auditing:
> The C5 criteria include guidance on how Cloud Service Providers can take actions towards continuous monitoring, including independent third-party audits, by automating their procedures and measures. This guidance should enable Cloud Service Providers to assess the general feasibility and effort implications of a continuous third-party audit.

Original Definition (EUCS Draft)

Continuous monitoring

The requirements related to continuous monitoring typically mention "automated monitoring" or "automatically monitor" in their text. The intended meaning of "monitor automatically" is:

1. *Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;*
2. *Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS;*
3. *Report deviations to subject matter experts who can analyse the deviations in a timely manner;*
4. *If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and*
5. *If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.*

These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity. Nevertheless, the introduction of continuous auditing, at least for level CS-High, remains a mid- or long-term objective, and the introduction of automated monitoring requirements in at least some areas is a first step in that direction, which can be met with the technology available today.

ENISA may develop, in collaboration with the ECCG, further guidance about suitable implementations of monitoring.

11

Proposal (1)

Continuous monitoring

The requirements related to continuous monitoring typically mention "automatically monitor" in their text. The intended meaning of "automatically monitor" in EUCS is:

1. *Gather data to analyse some aspects of the activity being monitored at discrete intervals and at a sufficient frequency;*
2. *Compare the gathered data to a reference for determining conformity to the related EUCS requirement;*
3. *Report deviations to subject matter experts who can analyse the deviations in a timely manner;*
4. *If the deviation indicates a nonconformity, then initiate the corresponding EUCS process.*

The definition of continuous monitoring and its associated EUCS requirements rely on technologies which have reached an adequate level of maturity. Nevertheless, the automation of procedures and measures for continuous auditing (at least for level CS-High), remains a mid- or long-term objective. The provided definition and requirements associated to continuous monitoring in EUCS are a first step in that direction.

ENISA may develop, in collaboration with the ECCG, further guidance about suitable implementations of continuous monitoring.

12

Proposal (2)

Line 120 - 124

Automated ~~Continuous~~ *monitoring*

The requirements referring to ***~~continuous monitoring that typically mention~~*** *"* ***~~monitor~~*** *automatically* ***monitor****" in their text, are about gathering data by non-human means.* ***Automated monitoring should be distinguished from continuous monitoring, as the latter can also be done without automation, i.e. by human means. In the future t****hese requirements can become the foundation for* ***~~continuous~~*** ***automated*** *auditing, but* ***at this moment*** *technologies have not reached the level of maturity needed for achieving that goal.* ***Automatically monitor therefore is a first step to the ultimate goal of enabling continuous automated auditing.*** *The introduction of automated monitoring requirements is intended to utilize the available technology.*

Line 103 – 105

CS-High requirements add further details or constraints in bold text. Some are also related to ***~~continuous~~*** ***automated*** *monitoring, or to additional testing and review requirements, contributing to an increase in confidence in the security of the service.*

13

The role of guidance

- Guidance will be provided in relationship to the 34 referred "automated monitoring" requirements from EUCS1.
  - Focus on current technology
  - Profit from relevant sources including practical experience with C5:2020 for continuous auditing, outcomes from H2020 MEDINA, and peer-discussions with CSPs and CABs.

14

15

APPENDIX G: Contribution to NIST SP 800-55 Rev. 2

1 Foreword

We welcome the opportunity to provide feedback to NIST SP 800-55r2, which we contribute on behalf of the EU-funded MEDINA project (https://medina-project.eu/). MEDINA is an EU funded-research initiative working in the areas of (cloud) security metrics, automation and certification. Its main goal is to create a security framework for achieving a continuous audit-based certification in compliance with the upcoming EU Certification Scheme for Cloud Services (EUCS, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme).

Main topics in MEDINA relate to (cyber-)security metrics and standardization, which have resulted in active engagements with European and International initiatives like ISO/IEC 27017 and NIST OSCAL. In this context, our project has developed the below documented feedback related to the initial working draft of NIST SP 800-55 Rev. 2. The provided feedback collects years-long experience of the industrial and academic participants in the project team which includes cloud service providers, audit firms, and technology centres.

Most of the feedback provided below is presented in a summarized manner, and focuses on introducing key ideas, however we will be glad to further elaborate our contributions in subsequent review rounds depending on the Editors' timeline.

For further questions related to the provided comments, please do not hesitate in contacting us at jesus.lunagarcia@de.bosch.com

2 Comments On Initial Working Draft

The feedback related to the referred draft can be found in Table 1 below.

Furthermore, we provide next our responses to the three "additional questions for reviewers":

CIOs and CISOs: What measurement and metrics guidance would benefit your program?

We would welcome an update to the catalogue of metrics and measurements from SP800-55r1 (Appendix A). Such uniform "baseline" enables the rapid adoption of the proposed metrics framework, while also allows for benchmarking / comparisons inter-/intra-organizations. Without such candidate measures, we run the risk of maintaining the status-quo where this topic has become highly subjective depending on how each organization interprets what "a good metric / measurement" means. Ideally, the "candidate measures" should become prescriptive part of international standards.

Furthermore, we would also appreciate further guidance on the topic of automation with respect to the "life-cycle" of the metrics / measurement program. Which stages of the process are possible to automate? Which standards become relevant?

NB: In the current draft of SP800-55v2, we have noticed that "Appendix A. Candidate Measures" has been removed. Please re-consider this decision, and also provide relevant updates, given the valuable information provided there.

How to best communicate information security measurement needs up and down the organizational structure?

In our experience, the need for security metrics has started to get better understood by organizations worldwide. The notion of "if you cannot measure, you cannot improve it" is taking a concrete shape when referring to certifications and GRC processes in general. Furthermore, it is getting common for organization to "benchmark" with respect to their peers based on commonly agreed metrics and maturity model frameworks. Few years ago, data collection was a challenge for implementing a sound metrics and measurements framework in the organization. However, nowadays we see the availability of data sources (e.g., cloud-based) which allow the rapid adoption of measurement systems that facilitate the active engagement of managerial.

The notion of aggregation / disaggregation of metrics is essential to efficiently communicate these within the organization. Despite the concept of aggregation / disaggregating has existed for years on this field, the lack of standardized approaches has proved as a show-stopper for leveraging the true potential of metrics and measurements.

Based on our practical experience and strongly dependant to the goals of the organization's metrics framework, communicating bottom-up becomes more efficient through KRI (Key Risk Indicators) or maturity models which allow identifying *areas of opportunity*. Literature on this topic is widely available, although (once again) the lack of standardized approaches is evident.

Communicating top-down the outcomes of a metrics and measurements program becomes more efficient through KPIs (Key Performance Indicators) which could be modelled as security postures. These, when drilled down by the experts, provide rich information to improve organization-wide GRC topics and align to the expectation from managerial.

Examples: What kinds of measures and metrics examples or templates could this publication provide that would be helpful in your work?

We strongly support the standardization of both baseline metrics and associated machine-readable templates which can be then leveraged by the respective stakeholders. Please consider updating the "Annex A. Candidate Measures" with related works like the following:

- CIS Critical Security Controls, Measures and Metrics (link)
- ISO/IEC 27004 "Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation"
- EU-MEDINA's catalogue of technical and organizational metrics (link).

About the MEDINA metrics, one must notice that they have been created for the specific purposes of assessing compliance with respect to the upcoming EU Certification Scheme for Cloud Services.

Machine-readable templates for representing metrics and measurements surely will benefit their management, interoperability and implementation. From our previous works, we have seen promising approaches in the following works:

- NIST OSCAL (link)
- NIST 500-307 “Cloud Computing Service Description” (also published as ISO/IEC 19086-2)

It is also worth mentioning that the previously referred ISO/IEC 27004 and MEDINA’s own catalogue of metrics, define simplified templates for cybersecurity metrics which also allow for rapid automation.

Table 1. EU-MEDINA Project feedback to NIST SP 800-55r2

Line Number	Clause /Subclause	Paragraph /Figure /Table	Type of Comment[1]	Comments	Proposed Change
251	Terminology		Te	We recommend referring to either ISO/IEC 19086-2 (also published as NIST SP 500-307) for standardized terminology related to Metric, Measurement, Measurement Result, and Unit.	Consider the provided references in order to align with related terminology found in international standards.
395	Measurement Quality		Te	Related to this topic, we recommend to briefly present the S.M.A.R.T. nature of the metrics in order to introduce the need for quality in the measurement process. Standardized measurements greatly benefit quality, and for this reason we suggest considering some of the concepts already introduced in ISO/IEC 19086-2 e.g., its definition of Metric model (8.1.5). Because it is common to use measurement results as compliance evidence, it is also advisable to introduce the need for protecting the collected data which was used for the measurement. In general, consider adding some of the notions already introduced by ISO/IEC 27004 (8.4).	Please consider some of the existing notions in both ISO/IEC 19086-2 and ISO/IEC 27004.
405	Trends and Historical Information		Te	We are not so sure that this Subsection fits into the topic of fundamental concepts related to measures. We would recommend moving it as part of the actual processes described in Chapter 4. That said, the analysis of trends	Consider moving this section to Chapter 4. Also, consider discussing the topic of trends and historical information in the context of the goals pursued by the

[1] Te = Technical, Ge = General, Ed = Editorial

				and historical information depends on the organization's goals. If the metrics and measurements are leveraged in the context of cybersecurity compliance, then trends are more difficult to identify, whereas historical information takes more importance due to associated conformance assessment processes.	organization (see e.g., ISO/IEC 27004 8.6 – 8.7).
416	Automation of Data Collection		Te	During the development of this SP, we recommend discussing standardized mechanisms which would benefit the automation of data collection. Some initial experiences exists with NIST OSCAL for this purpose, which might be worth considering.	In future review rounds, consider the discussion of NIST OSCAL and its role in the topic of metrics and measurements.
457	Information Security Measures Fundamentals		Ed	The title of Chapter 3 is the same of Chapter 2.	Please revise.
496	Governance and Compliance		Te	It is a common practice to align internal cybersecurity governance frameworks (including standards) to external ones, in order to facilitate processes like certifications and access to market. That said, we do not see that external cybersecurity goals are "opposed" to internal ones. Relevant (external) regulations, standards and even good practices are taken into account to populate the content of internal ISMS and other GRC-related processes. Metrics and measurement are not an exception, and internal governance frameworks also rely on (standardized) processes to elicit and leverage these in the organization. Although their main purpose (from an internal GRC	The ISO/IEC 27004 discussion on performance and effectiveness measures (7.2 – 7.3) might also provide related inputs for this topic.

				perspective) relates to “measuring” compliance, developed metrics/measurements can also apply to other cybersecurity areas of the organization like CTI or security monitoring. In our experience, what is really important in order to align both external and internal objectives is to leverage in the organization existing standards. In the case of metrics & measurements, we see the need for standardized catalogues of “baseline” cybersecurity metrics / measurements, including templates and schemes for managing them. Take into account that from an enterprise GRC-perspective, our goals are quite aligned to external entities which are based on similar standards like NIST SP 800-53 or ISO/IEC 27001.	
541	Measures prioritization and selection		Te	Based on our field experience, despite a mature metrics and measurement framework enables the improvement of implemented controls (line 546), we have realized that this comes after “performance” measures can be implemented. This follows the principle “if you cannot measure, you cannot improve it”. Furthermore, prioritizing the implementation of “applicable” metrics allows organizations to realize a series of challenges which experience can be then re-used for implementing more complex metrics. These “low hanging fruits” relate to measurements for which data sources and processes already exist (lines 548 and 549 respectively). A more complex topic related to assigning weights to measurements (and their related metrics), because the	Providing real-world examples about weighting scales might be highly appreciated by interested readers. Combining weights, with the existing qualitative/quantitative nature of metrics might add further complexity to the overall process. Even a “simplistic” weight system (e.g., high, medium, low), might be a good start for many organizations. We also recommend revisiting ISO/IEC 27004 on clause 8.3.4 for additional

				criteria will strongly depend on the organizations' goal. For example, if the goal is to measure "compliance" then more weight will be assigned to those metrics derived from regulatory Controls (e.g., NIST 800-53 or ISO/IEC 27001). However, if the goal is to measure "attack surface" then more weight will be given to metrics and measurements related to vulnerability management. Unfortunately, given the lack of standardized / baseline metrics (and measurements), at the state of practice their elicitation process is highly subjective. This adds more complexity to the prioritization and selection process, where lack of consensus related to "important metrics" might appear.	information on the topic of prioritizing the implementation of measurements. Please consider updating the current Appendix A. Candidate Measures.
595	Defining evaluation methods		Te	The scope of this section is not very clear to us, because it seems to mix the topic of "measurement methods" (e.g., component testing) with the actual metric (e.g., incident response volume), and the goal of obtained measurement results (e.g., monitoring for anomalies, KPIs, and so forth). It is our belief that topics like "Indicators" are better suited for Sect. 3.5.3, where performance targets can be defined as KPIs or any other type of "Metric + Target Value" form. Also, we suggest devoting this section to answer the question "what should I do with the obtained measurement results?". Topics like metrics' computation and aggregation could fit on this section as well e.g., leveraging maturity models.	Please consider clarifying upfront the scope of this section.

				In any case, the actual "evaluation method" to adopt by the organization will strongly depend on the pursued goals. For regulatory compliance, you might want to take into account that evaluation of KPIs should follow questions related to the effectiveness of the ISMS (e.g., for ISO/IEC 27001). This might imply "transforming" typical assessors' checklists into measurable indicators, where further guidance on SP800-55r2 would be welcomed.	
701	Data collection and reporting		Te	Despite the evident benefits of automation, it is true that "continuous monitoring" can also be manually performed by assessors. The scope of "continuous" should be clarified (automated / manual / both) in this section. Automation is more efficient when relying on standardized interfaces which ease interoperability. We recommend referring to NIST OSCAL for this purpose. We also acknowledge that not all metrics (nor their underlying measurements) can be fully automated, and therefore need manual intervention for data gathering. Manual data collection brings the challenges of objectiveness and assurance, which add further complexity when creating aggregated indicators which can be then visualized to provide a "big picture" of e.g., the organization's security posture. Work on this area has been developed by the EU-funded MEDINA project, which can be considered for inputs.	Please consider referring to the automation of metrics for compliance which is being documented by the EU-funded MEDINA project.

				Finally, given the importance of the “reporting” topic, we strongly suggest discussing it in a different section.	

APPENDIX H1: Contribution to ISO/IEC 27017 on Automated Configuration Monitoring

Template for comments and secretariat observations

Date: 06.03.2023	Document: **N 3404**	Project: ISO/IEC WD 27017

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
JL1	42	5.9	Guidance for cloud services - CSP	Te	For CSC to realize in a concrete manner their shared responsibility related to the security controls relevant to the cloud service asset, it is needed for the CSP to provide suitable information in the inventory system. Note: Alternatively, the proposed change can be applied to the CSP guidance table under “5.13 Labelling of Information” because part of the mentioned “service functionality” are the referred security features.	Please change the CSP guidance by adding the following item to the list: *— the security features on responsibility of the CSC to implement.*	
JL2	44	5.9	Other information for cloud services	Te	Usually, CSP add security-relevant information to cloud service assets in the form of standard templates like those referred in ISO/IEC 27002:2022 “8.9 Configuration Management”. Note: Alternatively, the proposed change can be applied to the other information paragraph under “5.13 Labelling of Information” because part of the mentioned “service functionality” are the referred security features.	Please add the following text as an additional paragraph under “Other information for cloud services”: *Standardized templates (see 8.9) can be used by the CSP to document in the inventory the shared responsibility model associated to the cloud service asset. These templates can be then applied by CSC as part of their shared responsibility.*	
JL3	734	8.9	Guidance for cloud services - CSC	Te	To be more precise we recommend reformulating both the paragraph preceding the bullet list, and also item (c) of the CSC guidance.	Consider changing “*The cloud service customer should define and implement processes and tools for the cloud service considering*:” to “*The cloud service customer should define and implement* ***configuration management*** *processes and tools for the cloud service considering*:”. Also for please consider reformulating item *“c) to* ***continuously monitor*** *whether the* ***provided standard templates*** *satisfy the security policy and requirements of the cloud service customer;”*	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Template for comments and secretariat observations

Date: 06.03.2023	Document: **N 3404**	Project: ISO/IEC WD 27017

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
JL4	734	8.9	Guidance for cloud services - CSP	Ed	The second paragraph on the guidance provides information which is redundant with the rest of the text. Also, the third paragraph in this CSP guidance seems to erroneously refer to the CSC.	Please consider removing the paragraph *"The cloud service provider should provide documented information to customers for the secure configuration for the use of the cloud service."* In the third paragraph change the reference from CSC to CSP i.e., *"The **cloud service provider** should provide capability and/or information about:"*	
JL5	734	8.9	Guidance for cloud services - CSP	Te	As referred in ISO/IEC 27002 (8.9) and also on the CSC guidance of 27017, the use of "standard templates" is central for configuration management. Therefore, the provided CSP guidance should explicitly refer to these.	Please consider adding the following item to the capability / information that should be provided by the CSP: *C) standard templates of offered cloud services, provided in standardized machine-readable formats (e.g., OSCAL), which can be consumed by configuration monitoring tools (8.9).*	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

APPENDIX H2: Contribution to ISO/IEC 27017 on Automated Monitoring Annex

Template for comments and secretariat observations

Date: 30.06.2023	Document: **N 3518**	Project: ISO/IEC WD 27017

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
DE1	612	8.9	Other Information for Cloud Services	Te	The provided Guidance for CSC and CSP (see table in line 612) refers to the notion of monitoring for the purposes of Configuration Management. We recommend further information to be provided in Annex C (in analogy to line 657 under "8.16 Monitoring Activities").	Please add "**Other Information for Cloud Services** For more information on the monitoring of cloud services for the purposes of configuration management, see Annex C."	
DE2	745	CLD.5.38	Guidance for Cloud Services – Cloud service customer	Te	The provided guidance for CSC states "The cloud service customer can use frameworks established by third parties or independent bodies to verify that no necessary information security capabilities of the cloud service provider have been omitted." Being the CSP the authoritative source of information related to information security capabilities related to offered cloud services, we recommend using 3rd party information just for the sake of completeness and not verifiability.	Please change the referred paragraph to "The cloud service customer can use frameworks established by third parties or independent bodies **to complement** the cloud service provider information on available security capabilities."	
DE3	745	CLD.5.38	Guidance for Cloud Services – Cloud service provider	Te	We recommend adding the following topics related to shared responsibility: • In cloud computing, the CSP also shares information security risks with its CSC. These should be documented and associated to recommended controls on CSC responsibility to implement. • CSP can support their CSC in analyzing fulfilment of the defined shared responsibilities (usually in form of security recommendations/allocated controls).	Please change: "The cloud service provider should define and document the allocation of information security roles and responsibilities, and agree with its cloud service customers, its cloud service providers, and its suppliers." To: "The cloud service provider should define and document the allocation of information security roles, **risks** and responsibilities, and agree with its cloud service customers, its cloud service providers, and its suppliers. **If the cloud service provider shares risks with the cloud service customer, the shared risks should be allocated to recommended**	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
						information security controls on responsibility of the cloud service customer to implement. **The cloud service provider should support cloud service customers to regularly analyse fulfilment of provided security recommendations and allocated controls, and take measures to encourage compliance based on the defined shared responsibility model.**"	
DE4	838	C.1	Monitoring of Cloud Services	Te	It is on the opinion of this expert that the referred Annex C contains information which is relevant not only for the security monitoring of cloud services (8.16), but also for monitoring in the context of configuration management (8.9). **Therefore, it is suggested to keep Annex C (although by considering the proposed changes).**	Please change the Annex C text as referred on the note below.	

NOTE: the following is the proposed text for Annex C (Informative) – Monitoring of Cloud Services

Cloud computing, amongst others, introduces changes in the way that security monitoring (see 8.16) and configuration management (see 8.9) are conducted. In traditional computing, those monitoring activities involved installing agents on specific equipment, collecting, reviewing, and evaluating logs for sources of potential issues. These tasks could be performed manually (especially in the case of SMEs) or automatically through software tools. Although these tasks could be performed through a third party (e.g. IT Services supplier), the same process was followed.

In cloud computing, there is a specific degree of transparency of the systems and a specific degree of monitoring that can be performed by the cloud service customer (depending on the service model, this could range from insubstantial – SaaS – to increased – IaaS). The cloud service customer and the cloud service provider have specific roles and responsibilities regarding monitoring, either for the detection of security-relevant events or for configuration management purposes. For example, when a cloud service customer uses SaaS, they have a limited number of security monitoring functions that can be implemented, and they are only related to the internal functions of the software (e.g. in a CRM application they may see business related information submitted by the personnel of the organization). In contrast, consider the example of an IaaS cloud service customer who leverages specific tools (where a broader number of functions are implemented) to continuously monitor if the standard configuration templates offered by the cloud service provider satisfy a security policy. In both examples, the cloud service customer has no monitoring capabilities on the infrastructure (logical or hardware) that supports the provision of the cloud service. In these cases, the cloud service customer (depending also on the agreed upon terms of service) will have to content with the information shared by the cloud service provider (see CLD.5.38).

Cloud monitoring for configuration management purposes is expected to rely on "automated monitoring" or "monitoring with automation" i.e., gathering and pre-processing data by non-human means. Automated monitoring should be distinguished from continuous monitoring. The latter refers to monitoring for an enduring period of time that can be applied both with or without automation.

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Template for comments and secretariat observations

Date: 30.06.2023	Document: **N 3518**	Project: ISO/IEC WD 27017

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					The introduction of automated monitoring for configuration management activities can leverage available technology (e.g., Cloud Security Posture Management – CSPM) and machine-readable languages (e.g, Open Security Controls Assessment Language - OSCAL) able to manage the complexity and scale of cloud services. In the mid term, “automated monitoring” might facilitate processes and practices of auditing cloud services. Since audit is a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled, the limitation of available information, mandates that the audit plans and relevant risk treatment options are adapted and supported with available tools (e.g. for the above mentioned SaaS example and for the criterion related to access control, an auditor would need to collect and evaluate evidence for the access control within the SaaS application and for the rest the collected evidence could be just the relevant Terms and Conditions of the service). Different service models introduce a difference in the responsibilities and abilities for monitoring and auditing between the cloud service customer and the cloud service provider, with SaaS being the most limited for the cloud service customer and the most extensive for the cloud service provider. In conclusion, for the cloud service customer, within the project of cloud computing transition, an adaption of the monitoring and configuration management procedures should be implemented and supported by automated monitoring. For the cloud service provider, on the other hand, monitoring and configuration management should cover their own needs for the effective and efficient operation of the relevant services as well as make provisions for the needs for information of the cloud service customer.		

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

APPENDIX I: Contribution to ETSI DTR/CYBER-0087

The explanatory comments related to this document, authored by the MEDINA consortium, are summarized in the following table.

Table 8. MEDINA comments related to "ETSI DTR/CYBER-0087"

Comment ID	Reference in document (Page Number)	Submitted Comment
I1	**4**	In our opinion the value proposition of this document should be clearly stated so it is built as guidelines for OSCAL. Then both OSCAL and this document become complementary. E.g., these guidelines can extend specific aspects of OSCAL, or present how to leverage it for specific purposes. This would also avoid overlapping with the OSCAL reference maintained by NIST.
I2	**4**	With “platform” do you mean OSCAL? Please clarify and user homogenously in the document.
I3	**4**	“Automation” does not seem to be the right term, because although OSCAL benefits automation, it can also be used to represent manual assessments. Another option would be “[…] challenges around the machine-readable representation of security controls […]”
I4	**5**	Please refer to I2.
I5	**5**	Please add reference to the MEDINA project together with [i.2]
I6	**5**	Proof-read the introductory chapter
I7	**6**	Clarify upfront who the target audience is.
I8	**6**	To which version of OSCAL is the document referring?
I9	**7**	For citing MEDINA, please use https://medina-project.eu/
I10	**9**	As a suggestion, for readability purposes it might be better the bottom-up explanation of the OSCAL models (i.e., starting with the Catalogue).
I11	**9**	Something copy+paste error seems to be in Section 4.2.2
I12	**9**	Please refer to I10 while presenting OSCAL
I13	**9**	Sanity check that all acronyms have been added to Sect 3.3
I14	**10**	Please refer to I10 while presenting OSCAL.
I15	**18**	Appendix 2 seems to be missing.

ETSI TR 103 923 V0.0.2 (2022-12)

Cyber Security (CYBER);
Open Security Controls Assessment Language Use Guidelines

Reference
RTR/CYBER-0087

Keywords
cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
Executive summary 4
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
4 OSCAL Concepts 8
4.1 OSCAL Introduction 8
4.2 Layers and models 8
4.2.1 Assessment Layer 9
4.2.2 Implementation Layer 9
4.2.3 Controls Layer 9
4.3 Identifier use 10
4.3.1 Identifier Type 10
4.3.1.1 Machine-Oriented 10
4.3.1.2 Human-Oriented 10
4.3.2 Uniqueness 10
4.3.3 Scope 11
4.3.4 OSCAL identifier defining model 11
4.3.4 Consistency 12
4.4 Processing specifications 13
4.5 Well-formed data formats 13
4.6 Discovery and availability 13
5 OSCAL encoding using Control Mappings 13
5.1 Control mappings 13
5.2 Conversion techniques 14
Annex A: Examples of OSCAL Content 15
A.1 OSCAL Format for the European cybersecurity scheme for cloud services (EUCS) 15
A.2 OSCAL Format for the Critical Security Controls 18
Annex: Bibliography 18
History 19

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides OSCAL guidelines based largely on the NIST OSCAL on-line reference site [i.1] [i.2] to provide a definitive international standards publication to advance use of the platform to address a number of challenges around the automation of security controls and security control assessments, especially pursuant to European Union legislative instruments. [i.n1] [i.n2] [i.n3] [i.n4] [i.n5] [i.n6] [i.n7]

- Control Information Lacks Standardization
- Assessing Control Implementations Across Multiple Components
- Supporting Multiple Regulatory Frameworks Simultaneously
- Documentation Reviews and Control Assessments are Largely Manual Processes

The goals are to: 1) drive a large decrease in the paperwork burden for both information security professionals and vendors, 2) normalize the representation of security control catalogues, regulatory frameworks, and system information using precise, machine-readable formats, 3) allow the sharing of control implementation and assessment information across communities, and 4) enable the creation of innovative solutions which rely on automation for managing compliance, risk and governance in organizations.

Introduction

The Open Security Controls Assessment Language (OSCAL) is a standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls. [i.1] Traditionally, security controls and control baselines are represented in proprietary formats, requiring data conversion and manual effort to describe their implementation and assessment. The goal of OSCAL is to move the security controls and control baselines from a text-based and manual approach (using word processors or spreadsheets) to a set of standardized and machine-readable formats. With systems security information represented in OSCAL, security professionals will be able to automate security assessments for diverse information systems, therefore paving the road towards continuous audit-based certification processes. [i.2]

To address information security and privacy risks, the implementation of selected controls needs to be verified and shown to be effective. To provide assurance of a system's security and privacy posture, the control implementation of a system must be both correctly described, assessed, and authorized. The standardized formats provided by OSCAL help to streamline and standardize the processes of documenting, implementing and assessing security controls. The automation enabled by the OSCAL formats reduces complexity, decreases implementation costs, and enables the simultaneous, continuous assessment of a system's security posture against multiple sets of requirements.

The rapidly increasing array of European Union legislative instruments combined with the imposition of extremely complex specifications for controls and certification requirements provide a compelling value proposition for application of the Open Security Controls Assessment Language (OSCAL) to automate implementations while achieving interoperability. [i.n1] [i.n2] [i.n3] [i.n4] [i.n5] [i.n6] [i.n7]

1 Scope

The present document provides use guidelines for the Open Security Controls Assessment Language (OSCAL) that enables extensible and verifiable interoperability among tools and portability of OSCAL content for the array of diverse cyber security controls which exist among different industry sectors, standards bodies, and countries. The guidelines build on the NIST OSCAL Project material and are fully aligned with that work and undertaken to encourage widespread global use, including open control specifications for meeting normative requirements with automated cybersecurity tools. [i.n1] [i.n2] [i.n3] [i.n4] [i.n5] [i.n6] [i.n7]

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST, “OSCAL Model Reference.”

NOTE: Available at https://pages.nist.gov/OSCAL/reference/.

[i.2] NIST, “OSCAL Concepts.”

NOTE: Available at https://pages.nist.gov/OSCAL/concepts/

[i.3] OSCAL XML Reference Index

NOTE: Available https://pages.nist.gov/OSCAL/reference/latest/complete/xml-index/#/@id

[i.4] OSCAL JSON Reference Index

NOTE: Available https://pages.nist.gov/OSCAL/reference/latest/complete/json-index/#/id

[i.n1] 2020/0359 (COD), Directive (EU) 2022/… of the European Parliament and of the Council of … on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.html.

[i.n2] 2020/0365 (COD), COM(2020) 829 Final, Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities, https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf

[i.n3] 2022/0272 (COD), COM(2022) 454 final, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

[i.n4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), ELI: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[i.n5] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance), ELI: https://eur-lex.europa.eu/eli/dir/2015/1535/oj

[i.n6] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (Text with EEA relevance), ELI: https://eur-lex.europa.eu/eli/reg/2012/1025/2015-10-07

[i.n7] 2022/0021 (COD), COM(2022) 32 final, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022PC0032

[i.y] ETSI Security Conference 2022, H2020 Project MEDINA.

NOTE: Available at https://docbox.etsi.org/Workshop/2022/10ETSISECURITYCONFERENCE/10_SECURITY_RESEARCH/FABASOFT_FANTA.pdf

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

machine-oriented identifier: a persistent identity for an entity within the OSCAL models, which can be used in other locations within related OSCAL models to reference the associated entity, and implemented using a Universally Unique Identifier (UUID) as defined by RFC 4122.

OSCAL baseline: defines a specific set of selected security control requirements from one or more control catalogs for use in managing risks in an information system.

OSCAL control: a requirement or guideline, which when implemented will reduce an aspect of risk related to an information system and its information.

OSCAL control catalog: an organized collection of controls

3.2 Symbols

For the purposes of the present document, the following apply:

NONE

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

NIST	National Institute for Standards and Technology
OSCAL	Open Security Controls Assessment Language
POA&M	Plan of Action and Milestones

4 OSCAL Concepts

4.1 OSCAL Introduction

The Open Security Controls Assessment Language (OSCAL) is a standardized, data-centric framework developed by NIST that can be applied to an information system for documenting and assessing its security controls. Today, security controls and control baselines are represented in proprietary formats, requiring data conversion and manual effort to describe their implementation, assessment and resulting security posture. An important goal of OSCAL is to move the security controls and control baselines from a text-based and manual approach (using word processors or spreadsheets) to a set of standardized and machine-readable formats. With systems security information represented in OSCAL, security professionals will be able to automate security assessments for diverse information systems, therefore paving the road towards continuous audit-based certification processes.

OSCAL addresses a number of challenges around security controls and security control assessment.

- Control Information Lacks Standardization
- Assessing Control Implementations Across Multiple Components
- Supporting Multiple Regulatory Frameworks Simultaneously
- Documentation Reviews and Control Assessments are Largely Manual Processes

The OSCAL project is working to address the following goals.

- Decrease Paperwork
- Improve System Security Assessments
- Enable Continuous Assessment

Design Principles

- Interoperable Data Formats
- Be Relevant Now, Enable a Better Future

4.2 Layers and models

The OSCAL architecture is organized in a stack of *layers*. Each lower layer in the stack provides information structures that are referenced and used by each higher layer. Each layer is composed of one or more *models*, which represent a information structure supporting a specific operational purpose. Each model in OSCAL is intended to build on the information provided by the model(s) in the lower layers. Figure x, below, depicts each layer and the corresponding model(s) for each layer. Each OSCAL model is represented in multiple, machine-readable *formats* (e.g., XML, JSON, YAML), which provide a serialization and encoding mechanism for representing and exchanging OSCAL data, also referred to as *OSCAL content*.

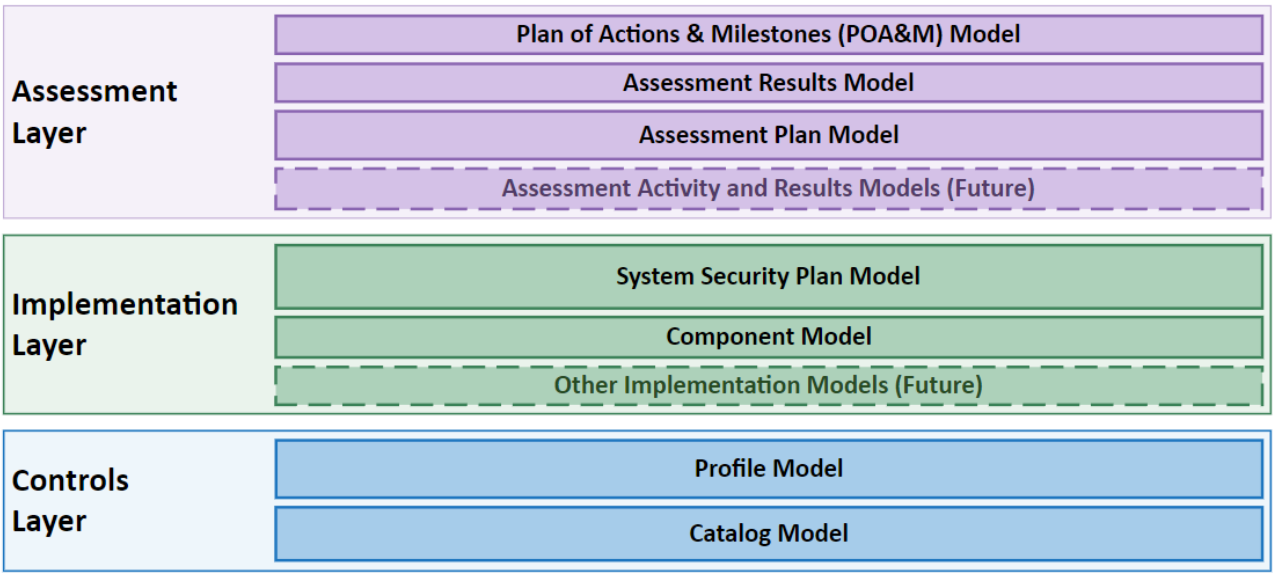

Figure x, OSCAL architecture

4.2.1 Assessment Layer

The OSCAL assessment layer provides models for describing how an assessment is planned, performed, and how the results of assessment activities are reported. The OSCAL assessment layer consists of the following models. The Assessment Results and POA&M models are designed to enable easy flow of risk information from the results to the POA&M. These models are intended to be used in the context of a specific system. The assessment results are further intended to be used in the context of a specific assessment plan.

Assessment Plan Model. The Assessment Plan model represents information related to the planning of a periodic or continuous assessment of a specific system. Ref. https://pages.nist.gov/OSCAL/concepts/layer/assessment/assessment-plan/

Assessment Results Model. The Assessment Results model represents information related to the findings of a periodic or continuous assessment of a specific system. Ref. https://pages.nist.gov/OSCAL/concepts/layer/assessment/assessment-results/

Plan of Action and Milestones Model. The Plan of Action and Milestones (POA&M) model represents the known risks for a specific system, as well as the identified deviations, remediation plan, and disposition status of each risk. Ref. https://pages.nist.gov/OSCAL/concepts/layer/assessment/poam/

4.2.2 Implementation Layer

The OSCAL implementation layer provides models for describing how controls are implemented in a specific system or in distributed component that can be incorporated into a system. The OSCAL implementation layer consists of the following models. The component definition and SSP models are designed to work together. As specific components are selected for use within a system, the content of the relevant component definition files can be used to populate the use of these components within the SSP model. The SSP model can also be used to represent systems that do not define information at the granularity of a specific component, where component definitions do not exist.

Component Definition Model. The Component Definition model allows for the definition of a set of components that each provide a description of the controls supported by a specific implementation of a hardware, software, or service; or by a given policy, process, procedure, or compliance artifact (e.g., validation). These are intended to be produced by the maintainer of the hardware, software, or service; or by the author of a given policy, process, procedure, or compliance artifact. Consumers of these assets are then able to use this information to document the implementation of a given asset in the implementing information system's System Security Plan (SSP). Ref. https://pages.nist.gov/OSCAL/concepts/layer/implementation/component-definition/

System Security Plan Model. The System Security Plan model allows the security implementation of an information system to be defined using an OSCAL profile (or baseline) as the basis for the system's control implementation. OSCAL-based SSPs are expressed in machine-readable formats that can be easily imported into a tool, allowing for increased automation of SSP validation and system assessment. An OSCAL SSP can also be transformed from the machine-readable form to a human-readable version. Ref. https://pages.nist.gov/OSCAL/concepts/layer/implementation/ssp/

4.2.3 Controls Layer

The OSCAL control layer consists of the following models. In OSCAL, profiles are generalized to be applicable to any set of information presented in catalog form. Thus, the idea of tailoring in application can be applied not only to security guidelines in general, but also in mixed environments that have to address requirements in more than one catalog at a time.

Catalog Model. The Catalog Model provides a structured, machine-readable representation of a catalog of controls. The OSCAL catalog model can be represented in XML, JSON, and YAML formats. It is important to note that the OSCAL catalog model is not a catalog document format, since the introductory prose included in many control catalogs is not present (or supported) in the OSCAL catalog model. Instead, the OSCAL catalog formats provide a robust syntax for representing collections of controls, including control statements, assessment objectives, and other control details. This structured form of a control catalog allows control information to be easily imported, exported, indexed, and searched by applications. Controls must also be encoded in a standard machine-readable form. The OSCAL model gives the designers of catalogs great flexibility in the details of how controls are defined, with their constituent parts. Ref. https://pages.nist.gov/OSCAL/concepts/layer/control/catalog/

Profile Model. The Profile Model provides a structured, machine-readable representation of a baseline. As the starting point for defining an organization's security mission and security posture, a baseline must be defined by any organization undertaking a risk-based security program or security assessment, typically by selecting and adapting controls from an authoritative catalog of controls, or from another baseline that has already been defined and described. The OSCAL profile model allows for selecting security controls from catalogs using a number of different mechanisms, as well as for tailoring those controls (e.g., assigning parameter values, modifying requirements). An OSCAL profile can select controls from more than one catalog, allowing an organization to have a single profile that references controls from several catalogs. OSCAL profiles can also be based on other OSCAL profiles, allowing baselines to be established as customizations of other baselines. This technical capability reflects the real-world use case for organizations and programs who need to do this. Ref. https://pages.nist.gov/OSCAL/concepts/layer/control/profile/

4.3 Identifier use

4.3.1 Identifier Type

By design, OSCAL supports machine-oriented and human-oriented identifiers. The OSCAL models dictate which are used for different data items.

4.3.1.1 Machine-Oriented

Machine-oriented identifiers provide a persistent identity for an entity within the OSCAL models, which can be used in other locations within related OSCAL models to reference the associated entity. These identifiers are intended to be auto-generated by tools when the entity is initially created. In OSCAL, a machine-oriented identifier is implemented using a Universally Unique Identifier (UUID) as defined by RFC 4122. A UUID is represented in OSCAL using the UUID datatype. UUIDs were chosen because:

- Programming interfaces exist in most programming environments to generate a UUID
- UUIDs can be issued without a central authority
- UUIDs are represented in 128 bits, providing for a large address space with low risk of identifier collisions for randomly generated values

The opaque nature of UUIDs, which consist of a series of hexadecimal characters, makes them less than ideal for wildcard matching scenarios. Thus, their use in OSCAL is intended for identification only where an exact match is required. Where wildcard matching is needed, the other data elements associated with the entity should be evaluated for a match instead.

The OSCAL XML Reference Index and OSCAL JSON Reference Index provide a listing of UUIDs in the core OSCAL models. References to these identifiers typically follow a naming convention of the object type followed by “-uuid”. For example, see the XML reference index for location-uuid (or location-uuids in the JSON reference index). [i.3] [i.4]

4.3.1.2 Human-Oriented

A human-oriented identifier incorporates semantic that support readability and processing by humans. OSCAL implements human-oriented identifiers as token data types, which are non-colonized names. For example, control identifiers in a catalog may use a nomenclature that is familiar to the intended audience, allowing them to quickly determine what security control is being referred to, simply by its identifier value.

The OSCAL XML Reference Index [i.3] and OSCAL JSON Reference Index [i.4] provide a comprehensive listing of the human-oriented IDs in the core OSCAL models. References to these IDs are typically named according to the referenced object type (e.g., control) followed by “-id”, as seen here in the XML Reference Index (and likewise JSON Reference Index in the JSON reference index).

4.3.2 Uniqueness

OSCAL identifier uniqueness is categorized as locally-unique or globally-unique. As implied by the category name, locally-unique identifiers must be unique within the current document, whereas globally-unique identifiers are guaranteed to be unique across all other identifiers. OSCAL’s machine-oriented UUID identifiers are always globally-unique. Human-oriented identifiers must be defined and managed organizationally and are more susceptible to identifier duplication or collisions. Thus, human-oriented identifiers are less likely or cannot be guaranteed to be globally-unique.

4.3.3 Scope

Identifiers that are only intended for use within the same OSCAL instance are categorized as instance scope. However, since OSCAL supports composition relationships, there are many cases where identifiers in a source OSCAL instance need to be referenced from other OSCAL instances. These are considered cross-instance scoped identifier references. Figure y below illustrates how the core OSCAL models relationships are established through import and link mechanisms, enabling cross-instance references.

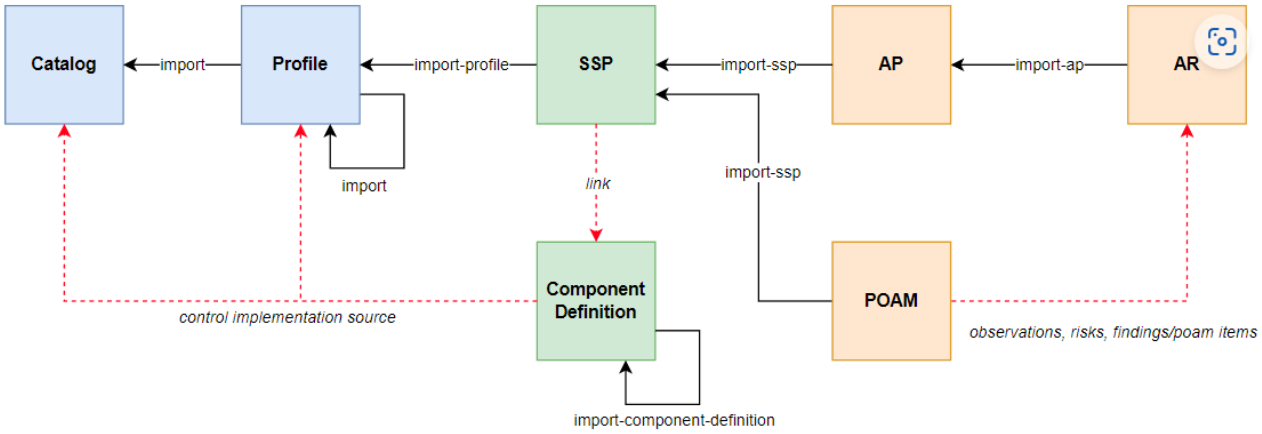

Figure y, OSCAL model relationships

Note: The solid black arrows depict relationships implemented via the import mechanism (e.g., import, import-profile, import-component-definition, import-ssp, and import-ap), whereas the dashed red line arrows illustrate relationships established through links.

The following import types are supported:

- import - see XML index or JSON index [i.3] [i.4]
- import-component-definition - see XML index or JSON index [i.3] [i.4]
- import-profile - see XML index or JSON index [i.3] [i.4]
- import-ssp - see XML index or JSON index [i.3] [i.4]
- import-ap - see XML index or JSON index [i.3] [i.4]

When implementing cross-instance references, identifier must be referenced in the context of the containing resource. The appropriate import attribute should be used (similar to a namespacing) to deconflict identifiers with the same values in the associated OSCAL instances. This is particularly important for human-oriented identifiers that may not be globally unique but still require cross-instance scoping. For example, this technique allows for the same control IDs to be used and referenced in a profile and its imported catalog(s) without conflict.

4.3.4 OSCAL identifier defining model

Catalog Identifiers

Identifiers defined in a catalog may be referenced locally or from an importing profile (see Fig. y). Additionally, identifiers defined in a catalog may be referenced in other upstream OSCAL instances in a hierarchical set of associated OSCAL documents (e.g., SSPs, assessment plans, assessment results, and POA&Ms). The table below provides a listing of the core OSCAL catalog model identifiers.

Defining Model	Identifier Type	Identifiers
Catalog	Machine-Oriented	XML Index | JSON Index
Catalog	Human-Oriented	XML Index | JSON Index

Profile Identifiers

Identifiers defined in a profile may be referenced locally or from an importing profile or SSP (see Fig. y). Component definitions can reference these identifiers through its control-implementation - source reference to the profile. Other upstream OSCAL models, including assessment plans, assessment results, and POA&Ms can also reference these profile identifiers via the hierarchical set of associated OSCAL documents. The table below provides a listing of the core OSCAL profile model identifiers.

Defining Model	Identifier Type	Identifiers
Profile	Machine-Oriented	XML Index | JSON Index
Profile	Human-Oriented	XML Index | JSON Index

Component Definition Identifiers
Identifiers defined in a component definition may be referenced locally or from an importing component definition instance (see Fig. y). SSPs may also reference identifiers from a component definitions through its implementation of links for a given component. Other upstream OSCAL models, including assessment plans, assessment results, and POA&Ms can also reference these component definition indirectly (e.g., via reference to an SSP component that has a link to a component definition). The table below provides a listing of the core OSCAL component definition model identifiers.

Defining Model	Identifier Type	Identifiers
Component Definition	Machine-Oriented	XML Index | JSON Index
Component Definition	Human-Oriented	XML Index | JSON Index

SSP Identifiers
Identifiers defined in an SSP may be referenced locally or from an importing AP or POA&M (see Fig. y). SSP identifiers can also be referenced from the AR through its hierarchical relationship with AP. The table below provides a listing of the core OSCAL SSP model identifiers.

Defining Model	Identifier Type	Identifiers
SSP	Machine-Oriented	XML Index | JSON Index
SSP	Human-Oriented	XML Index | JSON Index

AP Identifiers
Identifiers defined in an AP may be referenced locally or from an importing AR (see Fig. y). The table below provides a listing of the core OSCAL AP model identifiers.

Defining Model	Identifier Type	Identifiers
AP	Machine-Oriented	XML Index | JSON Index
AP	Human-Oriented	XML Index | JSON Index

AR Identifiers
Identifiers defined in an AR may be referenced locally (see Fig. y). However, observations, risks, and findings may also be referenced implicitly in the POA&M. The table below provides a listing of the core OSCAL AR model identifiers.

Defining Model	Identifier Type	Identifiers
AP	Machine-Oriented	XML Index | JSON Index
AP	Human-Oriented	XML Index | JSON Index

POA&M Identifiers
Identifiers defined in a POA&M are only referenced locally (see Fig. y). The table below provides a listing of the core OSCAL POA&M model identifiers.

Defining Model	Identifier Type	Identifiers
POA&M	Machine-Oriented	XML Index | JSON Index
POA&M	Human-Oriented	XML Index | JSON Index

4.3.4 Consistency

Identifier (value) must be managed across revisions of the same document. In general, OSCAL identifiers have per-subject consistency. They should only be changed if the underlying identified subject has changed in a significant way that no longer represents the same identified subject.

4.4 Processing specifications

OSCAL data is intended to be processed in many ways for many different purposes. The specifications here describe normative processes, in the sense that all OSCAL processors that perform these operations should produce the same outputs from the same inputs under the same configuration. However, users and developers should find many ways to take advantage of data encoded in OSCAL, even beyond what is considered here.

> **Profile Resolution Specification**. The Profile Resolution Specification provides the standardized process for transforming an OSCAL Profile into an OSCAL Catalog. Ref. https://pages.nist.gov/OSCAL/concepts/processing/profile-resolution/

[TBD]

4.5 Well-formed data formats

It is important that OSCAL tool developers know how to use, and build, software that can confirm that JSON-, XML-, or YAML-based OSCAL document instances are well-formed and valid. Being able to validate documents against externally-specified schemas (mutually and generally understood) is a foundation of robust, secure data interchange and interoperability. Generally, both "well-formedness" and "validity" of OSCAL instance data determine if a conformant OSCAL application can process such data. In this way, "well-formedness" and "validity" define the boundary between what can be considered OSCAL data and what cannot. The degree to which an application can support well-formed, valid OSCAL data defines how conformant the application is.

[TBD]

4.6 Discovery and availability

OSCAL expressions are typically published at a permanent URI.

[TBD] Ref. https://github.com/usnistgov/OSCAL

5 OSCAL encoding using Control Mappings

5.1 Control mappings

An array of different cyber security control frameworks exist. Many have been identified and mapped to the Critical Security Controls using XML structures that lend themselves to transformation into OSCAL. The Control Frameworks identified an mapped include the following.

- American Institute of CPAs (AICPA)Service Organization Control (SOC) 2 Controls
- Australian Signals Directorate (ASD) Essential Eight Controls
- Australian Signals Directorate (ASD) Top 37 Controls
- CIS Cyber Risk Profile v1.2 Controls
- CISA Cybersecurity Performance Goals (CPGs)
- Cloud Security Alliance Cloud Controls Matrix (CSA CCM) Controls
- GSM Association (GSMA) FS.31 Mobile Network Baseline Security Controls
- Health Insurance Portability and Accountability Act (HIPAA) Checklist Controls
- ISO/IEC 27001:2013 Controls
- ISO/IEC 27001:2022 Controls
- ISO/IEC 27002:2022 Controls
- Information Systems Audit and Control Association (ISACA) COBIT 19 Controls
- MITRE ATT&CK v8.2 adversary tactics and techniques knowledge base
- Microsoft Azure Security Benchmark v3 Controls
- NIST Cybersecurity Framework (CSF) v1.1 Controls
- NIST Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations 800-171 Rev 2 Controls
- NIST Risk Management Framework SP 800-53 Rev 5 Moderate and Low Baselines Controls
- New York State Department of Financial Services (23 NYCRR Part 500) Controls
- New Zealand Information Security Manual (NZISM) v3.5 Controls

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) Controls
- Payment Card Industry (PCI) Data Security Standard v4.0 Controls
- U.S. Criminal Justice Information Services (CJIS) Controls
- U.S. Federal Financial Institutions Examination Council - Cybersecurity Assessment Tool (FFIEC CAT) Controls
- UK National Cyber Security Centre (NCSC) Cyber Assessment v3.1 Controls
- UK National Cyber Security Centre (NCSC) Cyber Essentials Controls
- USDOD Cybersecurity Maturity Model Certification (CMMC) v2.0 Controls

5.2 Conversion techniques

[TBD] Ref. https://pages.nist.gov/OSCAL/concepts/relations-to-other/#niso-jats—nlm-bits-xml-encoding-for-publication-of-journals-and-books

Annex A:
Examples of OSCAL Content

A.1 OSCAL Format for the Draft[1] European Cybersecurity Scheme for Cloud Services (EUCS)

In the context of the cybersecurity certification schemes proposed by the EU Cybersecurity Act (EUCSA), ENISA (EU Agency for Cybersecurity) has setup an AdHoc Working Group to prepare the candidate scheme for cloud services (EUCS – EU Cybersecurity Certification Scheme for Cloud Services) [link]. This novel EUCS introduces the notion of continuous (automated) monitoring for checking compliance with some of the proposed cybersecurity requirements (in particular a subset from EUCS's high assurance baseline). Acknowledging the technical and organizational challenges associated with the notion of "EUCS-continuous" (link), the EU-funded MEDINA project proposes a framework to achieve automated audit-based certification aligned to the underlying EUCS principles. As part of the proposed framework, MEDINA investigates the usage of OSCAL for automatizing different processes related to EUCS, just as seen in the figure below.

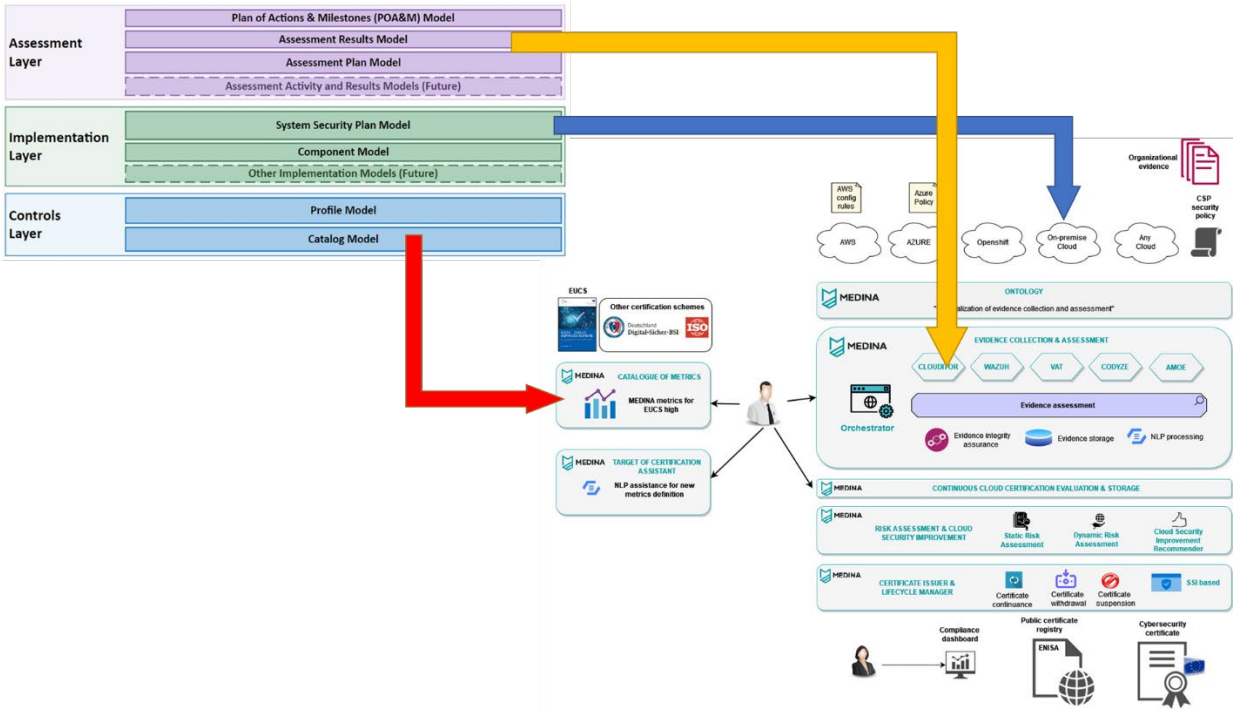

Figure X, Leveraging OSCAL in the MEDINA framework.

As a initial proof of concept, MEDINA has developed a mapping to represent the EUCS catalogue of requirements by leveraging OSCAL's Catalog Model[2]. This proof of concept was developed by applying the JSON scheme of OSCAL, where the draft EUCS catalog from ENISA is modelled as a hierarchy comprising the following eight levels:

1. Domain
2. Category
3. Objective
4. Control ID
5. Control
6. Control Objective

[1] As published by ENISA on December-2020 and available online https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[2] At the time of writing, an ongoing proof of concept was being developed for leveraging OSCAL's Assessment Result Model to provide interoperability between different implementations of Cloud Security Posture Management systems (CSPM). Further updates will be presented in future versions of this document.

7. Requirement ID
8. Requirement

The OSCAL scheme is implemented within a `Catalog` element, which contains an UUID and other applicable metadata as seen below:

```
{
  "catalog": {
    "uuid":"93a38765-4930-451a-9b74-9dba729bea84",
    "metadata":{
      "title":"OSCAL TEST",
      "last-modified":"2021-06-10T08:18:37.432+02:00",
      "version":"FPD",
      "oscal-version":"1.0.0"
    },
```

In the next step the EUCS' Domain and Category are created with the attribute "`title`". Also, by using the "`parts`" and "`prose`" elements the Objective can be presented as follows:

```
"groups": [
        {
          "id":"a7",
          "title":"A7 Operational Security",

          "parts":[
            {
              "name":"objective",
              "prose": "Ensure proper and regular operation, including appropriate measures for planning and
monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities,
malfunctions and failures"

            }
          ],
```

The EUCS Control itelf is represented as a "`title`" element, and finally the Control identifier becomes an OSCAL "`id`" with its respective "`properties`".

```
"controls": [
            {
              "id":"ops-02",
              "title": "CAPACITY MANAGEMENT - MONITORING",

              "properties":[
                {
                  "name":"label",
                  "value":"OPS-02"
                }
              ],
```

To complete the EUCS Control definition, the Control Objective must be added within "`parts`" and presented as "`prose`". Requirements and Control IDs are implemented as a nested "`parts`" element within the EUCS Control. In a similar manner, the Requirement ID is specified with "`properties`" and the Requirement itself as "`prose`".

```
"parts": [
                {
                  "id":"ops_02_obj",
                  "name":"control-objective",
                  "prose": "The capacities of critical resources such as personnel and IT resources are monitored."
                },
                {
```

```
                "id":"ops-02_smt",
                "name":"statement",
                "parts": [
                  {
                    "id":"ops-02_smt.3",
                    "name":"item",
                    "properties": [
                      {
                        "name":"label",
                        "value":"OPS-02.3"
                      }
                    ],
                    "prose": "The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1"

                  }
                ]
              }
            ]
          },
```


The above preented mapping from EUCS to OSCAL is summarized in the following table:

OSCAL Catalog Model	EUCS Element	Examples
Groups/ID	Domain	A7
Groups/title	Category	A7 Operational Security
Groups/parts/prose(objective)	Objective	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Groups/Controls/properties/value(label)	Control ID	OPS-02
Groups/Controls/title	Control	CAPACITY MANAGEMENT - MONITORING
Groups/Controls/parts/prose/(control-objective)	Control Objective	The capacities of critical resources such as personnel and IT resources are monitored.
Groups/Controls/parts/parts/properties/value(label)	Requirement ID	OPS-02.3
Groups/Controls/parts/parts/prose(item)	Requirement	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1

A.2 OSCAL Format for the Critical Security Controls

[TBD]

Annex: Bibliography

-

History

Document history		
V0.0.1	September 2022	Initial Draft
V0.0.2	December 2022	Early Draft