Deliverable D7.8

Standardization Roadmap-v1

Editor(s):	Jesus Luna Garcia
Responsible Partner:	Robert Bosch GmbH (Bosch)
Status-Version:	Final
Date:	30.04.2022
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	Standardization Roadmap-v1
Due Date of Delivery to the EC	30.04.2022

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

Abstract:	This deliverable presents all the relevant activities performed in the context of standardization and standards observation during the first 18 months of the MEDINA project.
Keyword List:	Standardization, Cloud Security, EUCS, EU CSA
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	03.01.2022	First draft version	Bosch
v0.4	21.03.2022	Full draft ready	Bosch, TECNALIA, Fraunhofer
v0.5	08.04.2022	Revised draft with comments for authors	Bosch, TECNALIA, Fraunhofer
v0.7	13.04.2022	Sent for internal review	Bosch
v0.8	25.04.2022	Addressed all comments received in the internal QA review	Bosch
v1.0	30.04.2022	Ready for submission	TECNALIA

Table of Contents

List of Tables

List of Figures

Terms and abbreviations

AHWG	AdHoc Working Group
AISBL	Association Internationale Sans But Lucratif
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Conformance Assessment Body
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
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
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 presents MEDINA's standardization activities and associated main results, which took place during the reporting period (M1-M18). Documented activities include the methodological approach that has been developed by the consortium to guarantee the creation of efficient synergies with standardization bodies and good practices working groups. Furthermore, this deliverable also presents the results of MEDINA's activities related to standardization, including the adoption and influence of relevant works in the cloud cybersecurity certification field. Finally, we also report on the initial standardization roadmap which is being created by MEDINA to support sustainability of the produced project outcomes, and uptake of the EU Cybersecurity Certification Scheme for Cloud Services (EUCS).

1 Introduction

This section provides an overview of the content documented in this deliverable.

1.1 About this deliverable

The topic of standardization plays an important role in MEDINA, just as reflected by Task 7.4 which additionally contributes to the project's sustainability actions coordinated by WP7. On one hand, our project constantly surveys the standardization landscape (including industrial good practices) to facilitate early adopters, the integration of contributed frameworks into their own ecosystems. On the other hand, MEDINA is actively contributing to a selected group of standards as a mean to support the project's sustainability even after its lifetime. In this context, it is important to clarify our notion of "standardization", as 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., Cloud Security Alliance). In both cases fruitful/efficient synergies can only be built if the project develops the right approach for interacting with relevant SDOs and SSOs.

This deliverable covers the reporting period (M1-M18) and presents the methodological approach developed by MEDINA to internally leverage and influence relevant standards, and also industrial good practices. Furthermore, initial activities and results of applying the developed approach are also discussed. Finally, an initial version of MEDINA's proposed standardization roadmap is also discussed. Our roadmap aims to support sustainability of technical contributions from MEDINA, while at the same time supporting the EUCS uptake thanks to the activities in Task 7.4.

1.2 Document structure

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

- Section 2 reports on the methodological approach developed by MEDINA to adopt/influence both SDOs and SSOs.
- Section 3 presents the current activities of MEDINA withing selected standards and good practices.
- Section 4 discusses the initial version of MEDINA's standardization roadmap.
- Finally, Section 5 presents our conclusions and future work.

2 The Approach to Standardization in MEDINA

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.

2.1 Standardization Approach

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 in Figure 1 and are further explained in the rest of this section.

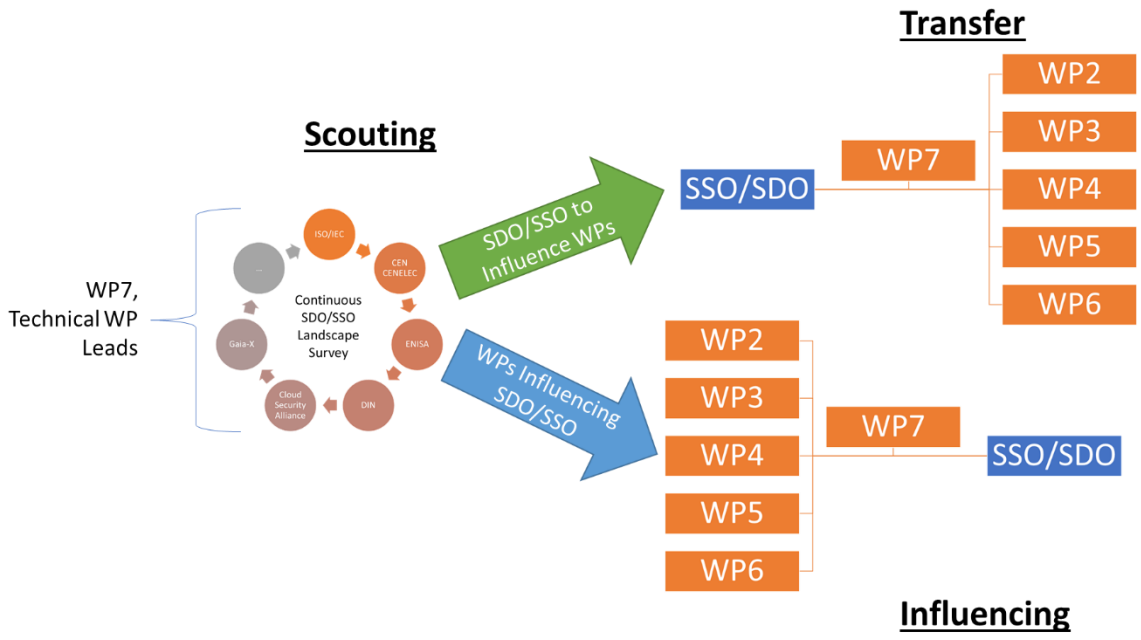

Figure 1. MEDINA's Approach to Standardization

2.2 Scouting - Identifying standardization activities relevant to MEDINA

A central role in our standardization approach relates to the continuous survey of the relevant SDO/SSO landscape i.e., the so-called "scouting" phase. During this stage all technical WPs participate, under the coordination of WP7, to bring their expertise related either to *(i)* the need for alignment with existing standards, or *(ii)* potential contributions to specific SDO/SSO initiatives.

The team in WP7 supports in coordination activities related to standardization in MEDINA, specifically for retrieving/summarizing identified standards from those SDO/SSO where a liaison exists (e.g., ENISA EUCS), evaluating the MEDINA-relevance of new works being discussed in standardization bodies (e.g., the revision to ISO/IEC 27017 presented in Section 3.3), and orchestrating the project's contributions to selected SDO/SSO initiatives.

Scouting is an essential activity in WP7-standardization because it makes more efficient the use of available MEDINA resources. Please take into account that "continuous cloud cybersecurity certification" is a novel topic in relevant SDO/SSO, and it is resulting in multiple workstreams (see as an example the thematic groups from ENISA EUCS in Section 3.1.2) which need to be prioritized in order to avoid scattering efforts.

Once the "scouting" has identified relevant SDO/SSO activities, with the support of MEDINA's WPs experts, then it must be collaboratively decided if the project should contribute (influence) or transfer standardization know-how to its technical activities. Both processes are presented in Section 2.3 and Section 2.4 respectively.

Finally, it is worth to notice that MEDINA's scouting activities play a relevant role in the creation of the project's standardization roadmap, which is presented in Section 4.

2.3 Influencing - MEDINA contributing to the development of Standards / Good Practices

Part of the project's sustainability depends on creating a "technical legacy" of its WP2-WP6 activities. From a WP7-standardization perspective, such legacy corresponds to what MEDINA can contribute to well-scoped SDO/SSO activities which have been identified during the scouting phase (see Section 2.2). It is well-known that standardization activities can have a very long timeline (sometimes lasting 20+ months until the final standard is released), therefore the importance of focusing only on those activities where MEDINA's impact can be maximized. Furthermore, if a standardization activity can expand beyond the project's lifetime then there must be a clear commitment from participating partners to continue their collaboration with their own resources at a given time. In some cases, this decision is directly related to the partners' exploitation plans, which are further discussed in D7.6 [1] and D7.7 [2].

In any case, and once WP7 identifies one or more relevant SDO/SSO initiatives, then it is time to orchestrate the actual technical contributions. From a high-level perspective, the "influencing" process consists of the following steps:

1. **Liaising with the corresponding SDO/SSO:** this is an essential step in order to guarantee that the project's contributions will be formally taken into account with the corresponding standardization body. In particular SSOs (e.g., Cloud Security Alliance) have an open (and cost-free) process for contributing to their initiatives, which facilitates for projects like MEDINA to provide contributions from different technical partners. The situation is different for many SDOs, where in order to contribute (and not only to participate as an Observer) it is necessary to become a (paid) member e.g.,

ISO/IEC and the German DIN. **During the reporting period, MEDINA partners (Bosch, TECNALIA, and FhG) created liaisons with ENISA (AdHoc WG on EUCS), Gaia-X, CEN CENELEC (CEN/CLC/JTC 13/WG 2), ISO/IEC (JTC1 SC27/WG1), German DIN (NA 043-01-27-01 AK), Cloud Security Alliance (Cloud Security Metrics WG), and NIST (OSCAL WG)**.

2. **Participating in related SDO/SSO activities:** once the liaison has been created by MEDINA, then it is time to start the actual work of participating in the corresponding SDO/SSO meetings in order to identify the topics/projects to contribute, and guarantee that established deadlines will be fulfilled.
3. **Orchestration of MEDINA contributions:** this is an interactive step, where WP7 coordinates with the technical WP2-WP6 to manage contributions on identified SDO/SSO activities. Depending on the organization, there might be substantial differences related to the way of writing and submitting feedback from MEDINA, but in any case, the WP7-standardization lead must carefully consider and follow the related guidelines.
4. **Positioning MEDINA contributions***:* submitting a contribution to the SDO/SSO does not mean that it will simply make it into the final published standard. The contribution must be well positioned using objective/sound arguments, to increase its chances of publication at the identified SDO/SSO. This is an interactive process where WP7 might need to come back to step (3) in order to refine the contribution as needed.

The described process has been leveraged by MEDINA, and ongoing contributions are presented in Section 3.

2.4 Transferring – Leveraging standard for scientific and technical activities in MEDINA

Complementary to MEDINA's process for influencing SDO/SSO, we can also find the WP7-standardization activity related to "bringing" standards to the technical activities from WP2-WP6. In a nutshell, it refers to transferring standards (e.g., machine-readable formats, good certification practices, assessment methodologies) so they can be leveraged or modelled by the technical MEDINA activities. This activity supports early adoption/interoperability of produced outcomes thanks to their alignment to existing standards, and also guarantees that MEDINA's framework follows the standard in the way it was meant to be.

During the reporting period we realized that this "transferring" activity was essential for the EUCS requirements and processes being implemented by the MEDINA framework, where the work created by ENISA was being directly leveraged by the technical WP2-WP6 activities. Thanks to this activity, the produced MEDINA framework is expected to have a major impact in future (commercial) products seeking also to implement EUCS. Relevant "transferring" activities are reported in the next section.

3 Report on MEDINA's Standardization / Best-Practices Activities

This section reports the consortium's activities with relevant SDO/SSO initiatives, which were selected based on the *Scouting* process described in the Section 2 and comprised both *Influencing* and *Transferring* tasks.

3.1 EU Cybersecurity Certification Scheme for Cloud Services (ENISA EUCS)

Probably the most relevant standardization activity from the MEDINA perspective is the one being led by ENISA on the topic of EUCS. MEDINA has both *Influenced* and *Transferred* know-how to ENISA EUCS, just as presented below.

3.1.1 Overview of ENISA AHWG

On March 2020, ENISA launched a so-called ad-hoc working group (AHWG) to support the European Commission (EC) in preparing the draft candidate cybersecurity certification scheme for cloud services[1].

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"[2].

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, two of them are part of the MEDINA project, namely Bosch (Dr. Jesus Luna Garcia) and TECNALIA (Dra. Leire Orue-Echevarria Arrieta).

The work in the AHWG of ENISA has been distributed in Thematic Groups (TG), which are dedicated sub-groups to work extensively and exclusively in one specific EUCS topic. Each TG was supported by a rapporteur (selected from the 20 experts), and at the time of writing are still meeting in a weekly manner since November 2020. Our project's engagement activities with those TG are reported next.

3.1.2 Contribution to Thematic Groups (TG)

ENISA defined *nine* TGs, out of which MEDINA actively contributed to *five* during the period covered by this deliverable. Those five specific TGs were selected based on the approach described in Section 2, and their relationship with our technical activities can be seen in Figure 2.

From a MEDINA's perspective, each contributed TG was classified either as *Foundational* or *Follow-up.* The former means that the TG outcome was part of the original EUCS draft from December 2020, whereas the latter refers to follow-up EUCS activities of the ENISA AHWG.

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

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

Notwithstanding its Foundational or Follow-up nature, the consortium actively engaged with the illustrated TGs just as explained in the rest of this section.

Figure 2. Contributed ENISA EUCS' Thematic Groups

3.1.2.1 TG1 – Assurance Levels

The aim of this group was to determine the different scope and dimensions needed to define the different assurance levels that the EU CSA requires. The two AHWG members of MEDINA participated in this group's discussions.

The EU CSA only states that there should be three levels of assurance (i.e. basic, substantial and high), but does not provide further details. It is up to the certification scheme under scope to determine how these levels will be characterized. In the case of the EUCS, the approach of "incremental dimensions" was selected. That is, assurance levels have dimensions where the security requisites are gradually incremented. MEDINA partners participated in the discussions, provided comments and alternative texts to the assurance level definitions, **in particular related to the notion of continuous (automated) monitoring for High Assurance**. That work was then leveraged into the activities of WP2-WP4 for topics like risk management (WP2), continuous collection of evidence (WP3), and conceptualization of operational effectiveness (WP4).

TG1 finished its activities in December 2021. For more information on EUCS-defined assurance levels (outcome of TG1) please refer to Appendix A.

3.1.2.2 TG2 – Security Controls

TG2 is the foundational group devoted to the definition of the categories, security controls, security requirements and their placement in one or another level of assurance. This activity is also fundamental for MEDINA, because it provides the actual set of technical and organizational measures (TOMs) for certifying a cloud service.

Taking as baseline existing schemes and control catalogues, the group met weekly to discuss the structure of the requirements, the requirements themselves, their scope, the wording and the assurance level. The MEDINA coordinator was also the rapporteur and led the discussions, in collaboration with the ENISA chair. In the context of TG2, MEDINA provided ENISA with the mapping of EUCS with other schemes, just as reported in D2.1 [3].

TG2 finished its activities in December 2021, although follow-up activities are taking place in the context of CEN CENELEC (cf. Section 3.2). The set of requirements elicited by TG2 are part of MEDINA's *Catalogue of Controls and Security Schemes* (please refer to D2.1).

3.1.2.3 TG3 – Assessment Methods

This foundational thematic group was devoted to the definition of the conformity assessment method(s) that will be used by EUCS. For the level of assurance basic, it was determined that an evidence-based self-assessment with a third party involved would be the appropriate one, while for the substantial and high levels of assurance a meta-methodology based on ISAE 3402[3] and ISO 17065[4] has been designed.

MEDINA participated in the weekly TG3 discussions, reviewing the generated methodological document thanks to the feedback being provided by our CAB partner NIXU. One of the main outcomes from TG3, which currently drives the MEDINA activities related to the certification lifecycle, are the management processes summarized in Figure 3. TG3 finished its activities in December 2021.

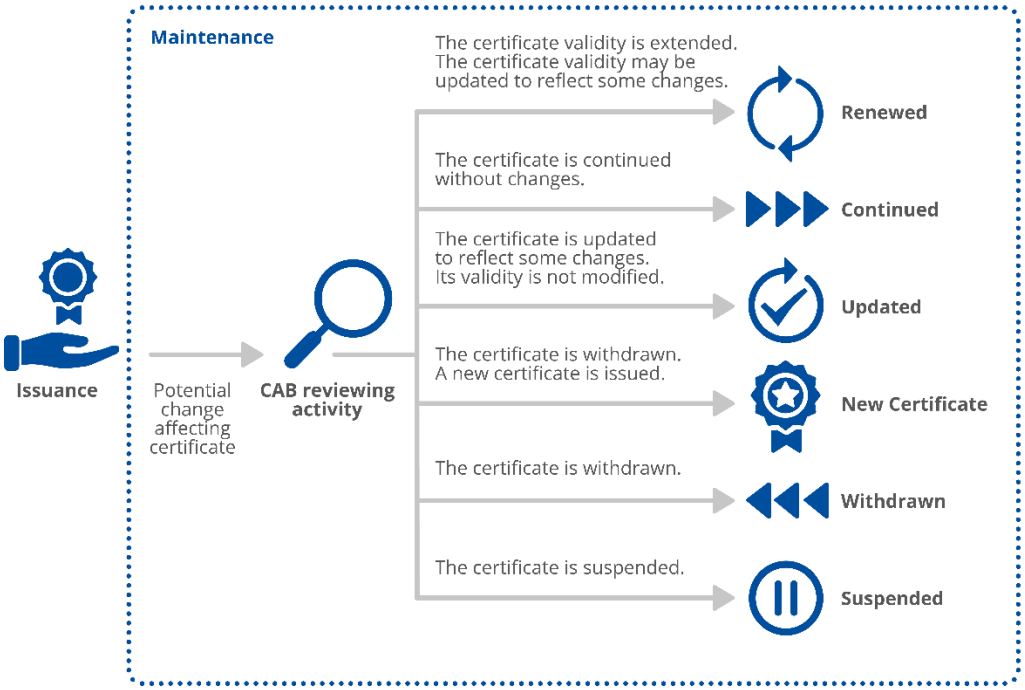

Figure 3. Processes related to the issuance and management of EUCS certificates[5]

[3] ISAE 3402 "Assurance Reports on Controls at a Service Organization"

[4] ISO 17065 "Conformity assessment — Requirements for bodies certifying products, processes and services"

[5] Based on ENISA EUCS draft from December 2020

3.1.2.4 TG8 – Guidance on Controls

After December 2021, ENISA organized a set of follow-up EUCS activities targeting both the standardization and uptake of the developed scheme. Guidance and good practices related to implementing and auditing the scheme are needed not only by EUCS, but also for supporting the adoption of the MEDINA framework. One of such follow-up activities related to TG9, which was born during the so-called experimentation stage (cf. Section 3.1.3) where it became clear from the comments of the participants, that guidance is needed to ensure the success of EUCS.

The MEDINA coordinator participated in the discussions of the TG8 approach, the depth level and the structure of the guidance to be developed. Furthermore, MEDINA has provided the reference implementations described in D3.1 [4] as potential input for the guidance of the controls of assurance level high (continuous monitoring). This is an ongoing activity, which is expected to finalize by the end of 2022.

3.1.2.5 TG9 –Questionnaire for Basic Assurance

Another EUCS *follow-up* activity which is tightly related to the technical tasks in MEDINA relates to the so-called self-assessment questionnaire (i.e., EUCS basic assurance). The goal of ENISA is to develop a methodology and questionnaire for guiding CSPs and CABs in aspects related to the achievement of a basic assurance EUCS certificate.

The work that partner TECNALIA is doing in WP3 with the questionnaires to assess the basic level of assurance (cf. D3.1 [4]) has been shared and discussed with ENISA. At the time of writing this deliverable, the MEDINA approach and questionnaires were being leveraged by the TG9 participants. The questionnaires that TECNALIA provided had approximately 500 questions as they were mostly a decomposition of the requirements, but included also the definition and identification of evidences (i.e., documents, logs or any kind of information that can potentially support a statement), which up until now had not been previously considered in-depth in past discussions. An excerpt of the developed MEDINA questionnaire, which was provided to TG9 can be seen in Appendix B.

The challenges and main effort expected to comply with the approach for the assessment of basic assurance level does not strive in the number of questions that CSPs need to complete, but in finding the right evidence that proves that that requirement is fully complied with. This lesson learned from MEDINA has been now also included in the questionnaires.

It is also worth to notice that the developed TG9 questionnaires are also being analysed for MEDINA's SATRA tool (cf., D2.6 [5] on static risk assessment), and similarly for the activities related to the assessment of organizational evidences (cf., D3.4 [6] on organizational measures). TG9 is an ongoing activity, which is expected to finalize by the end of 2022.

3.1.3 Contribution to ENISA EUCS Experimentation

During March 2021, a call for "EUCS experimentation" was released by ENISA with the goal of verifying the auditability and efficiency of the candidate draft scheme, where stakeholders were able to lead evaluation on specific parts of EUCS. The call was only open to members of the AHWG, and therefore to participate the team was supposed to apply only through a member of the AHWG. Furthermore, the team must be comprised of at least a CSP and a CAB. This "experimentation" allowed ENISA to get feedback on the draft candidate scheme and build guidance, and also allowed stakeholders taking a first step ahead on the future cloud certification scheme and gain maturity. A condition for the experimentation was to consider a real use case, based on an actual cloud service, and to include a return-on-experience phase to the ad hoc Working Group.

MEDINA considered this call for EUCS experimentation as a great opportunity to disseminate the project's activities, while at the same time contributing to the uptake of EUCS and the framework under development. In that context, MEDINA proposal targeted the experimentation of automated monitoring requirements extracted from the EUCS High Assurance. Participants on this ENISA POC were two cloud service providers (Fabasoft and Bosch), and one CAB (NIXU). As mentioned earlier in this chapter, Bosch is part of the ENISA AHWG.

Table 1 shows the original approach as proposed to ENISA for the POC.

Table 1. MEDINA approach to ENISA Experimentation

Stage	Explanation	Comment
1	Selection of EUCS requirements	The requirements will be extracted from EUCS High Assurance (Annex A), where the keyword "automated monitoring" has been used. Our aim is to evaluate for • Bosch: 5 different EUCS requirements, from at least 3 different Azure services. • Fabasoft: 5 different EUCS requirements for the Fabasoft Cloud.
2	Selection of automated monitoring policies (Bosch only)	The automated monitoring policies (for the Azure platform) will be selected as they correspond to a set of chosen EUCS requirements. Such policies will come from the custom catalogue of Azure.
3	Experiment the EUCS concept of *operational effectiveness* for automated monitoring requirements	Bosch: will deploy its selected policies in the Microsoft Azure platform for a period 90 days corresponding to the EUCS notion of *operational effectiveness*. In the scope of this experiment will be a specific Bosch PaaS solution deployed in Microsoft Azure. Fabasoft: will apply the selected requirements to current implementations that are monitored with app.telemetry[6] for other standards, like BSI C5: 2020, for a period of time corresponding to the EUCS notion of *operational effectiveness*.
4	Document results, observations and challenges	A report will be produced to compile the lessons learned, results, and foreseen challenges related to the real-world usage of the experimented EUCS requirements. The report will be also contributed by NIXU, in order to provide the perspectives of both CSP and CAB.

The final report delivered to ENISA by the MEDINA team can be found in Appendix C. This experience was also integrated into the technical activities for developing the MEDINA framework, in particular related to the evidence collectors and the definition of operational effectiveness which is in the scope of WP4.

[6] https://www.fabasoft.com/en/products/fabasoft-apptelemetry

3.2 CEN CENELEC's Technical Specification for EUCS

As part of ENISA's mandate to establish EUCS, there is the need for an EU standard developing organization (SDO) to create a so-called "technical specification" (TS). This specification is basically a formal standard containing the EUCS requirements which were published by ENISA in draft form last December 2020. The technical specification must follow the processes of the target SDO, which in this case is CEN CENELEC[7], the European Committee for Electrotechnical Standardization. At the time of writing this report, CEN CENELEC JTC 13 WG2 (Management Systems and Controls Sets) had taken over that responsibility by establishing the project "Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services (EUCS 1)". Starting November 2021, **MEDINA (represented by partner Bosch) has been designated by ENISA as technical expert for supporting the development of the technical specification in the EUCS 1 project from CEN CENELEC**.

The timeline of the EUCS 1 project is 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

As observed, this activity extends beyond MEDINA's lifetime, nevertheless participation of selected partners is part of the project's sustainability activities to be presented in D7.9 [7]. Although for the time being this activity has been delayed due to organizational issue within CEN CENELEC, it is our expectation that most of the standardization efforts in MEDINA will be devoted to the successful publication of the EUCS TS. More details on MEDINA's standardization roadmap can be found in Section 4.

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

As stated in its public abstract[8] "ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services."

A notable difference between EUCS and the current version of ISO/IEC 27017, is that the latter does not contain any reference to the topic of continuous (automated) monitoring as required by the MEDINA framework. However, a new project proposal for revising ISO/IEC 27017 was created in April 2021 and approved as "design specification" early 2022, where it is mentioned[9] "consider other documents relevant to information security controls applicable to cloud services, to determine which control topics and issues that might need to be considered in ISO/IEC 27017, e.g. **German C5, EUCS and SECNUM**. During the revision experts are invited to submit contributions from these and other sources.".

[7] https://www.cencenelec.eu/
[8] https://www.iso.org/standard/43757.html
[9] Please notice that the cited document is internal to ISO/IEC, therefore it cannot be referenced/attached as appendix to this public deliverable.

A corresponding call for expert contributions was issued by ISO/IEC JTC1/SC 27/WG 1 on March 2022 to start shaping the revised ISO/IEC 27017 standard. MEDINA, represented by Bosch in the respective ISO/IEC committee, is already aligning with ENISA to **shape the contributions on topics like continuous (automated) monitoring in order to propose an EUCS-like approach**. If successful, the addition of these novel concepts/requirements in ISO/IEC 27017 has the potential to increase the impact of the MEDINA framework beyond its EU-scope.

Although the revision of ISO/IEC 27017 is planned to finalize late in 2023. MEDINA's contributions (and planned sustainability actions) will be reported in D7.9 [7].

3.4 Open Security Controls Assessment Language (NIST OSCAL)

A topic identified by MEDINA's scouting approach (cf. Section 2) relates to leveraging standardized machine-readable languages in order to fully realize the potential of the framework under development. Such a language would have the potential to create interoperability between different technology providers/CSP, and at the same time conveying relevant information of the continuous certification process as envisioned by the MEDINA architecture (cf. D5.2 [8]). To the best of our knowledge, NIST OSCAL[10] is nowadays the most mature candidate (from a standardization perspective) in this specific field[11] just as evidenced by its leverage in relevant certification initiatives like FedRAMP[12].

Almost since the beginning of MEDINA, the consortium has been actively involved in the development of NIST OSCAL. This experience has been also integrated in the ENISA EUCS Experimentation (cf., Section 3.1.3), just as seen in the report documented in Appendix C. At the time of writing, **MEDINA is supporting the discussions between NIST and ENISA in order to further experiment with OSCAL**. This activity is also supported by the proofs of concept developed in the technical WPs of the MEDINA project, which started with the representation of EUCS in OSCAL format just as summarized in the following table.

Table 2. Contribution to NIST OSCAL related to EUCS

OSCAL	EUCS	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

[10] Please refer to https://pages.nist.gov/OSCAL/

[11] It is also worth to notice that a founding member of NIST OSCAL (Dr. Michaela Iorga) is part of MEDINA's Expert Stakeholder Group.

[12] https://www.fedramp.gov/blog/2021-07-20-FedRAMP-Releases-Updated-OSCAL-Templates-Tools/

OSCAL	EUCS	Examples
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.

The resulting OSCAL representation of the EUCS requirements will be made available on the MEDINA code repositories during the execution of the project. The consortium has been also using this standardization activity to participate in NIST-organized workshops with the goal of disseminating MEDINA's activities to US-based audiences (see D7.4 [9]).

3.5 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[13]. This association was founded with the goal of developing and operating the technical framework for the Gaia-X Federation services.

In the timeframe of March 2020 to December 2021, Gaia-X had a dedicated group on Compliance, where MEDINA partners Bosch, Fabasoft, FhG and TECNALIA were very active. The WG Compliance met on a weekly basis to discuss the certification schemes that should be relevant for Gaia-X, as well as to discuss the different assurance levels that could be considered in Gaia-X for the labelling framework.

In addition, 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)[14] 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 is currently involved in the implementation of said specification in an open-source project[15] currently coordinated by the eco – Verband der Internetwirtschaft. Since the aim of the implementation task is to re-use existing open-source implementations of this field as much as possible, parts of the open-source components of MEDINA, such as the

[13] https://www.gaia-x.eu/who-we-are/association
[14] https://www.gxfs.eu/download/1731/
[15] https://gitlab.com/gaia-x/data-infrastructure-federation-services/cam

Clouditor component, are currently being 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.

Gaia-X is not only significant for MEDINA from a standardization perspective, but it is a central concept for the joint exploitation strategy as discussed in D7.6 [1].

3.6 Security Metrics and Cloud Controls Matrix (Cloud Security Alliance)

While MEDINA has a strong focus on the European approach using the EUCS, it aims to be as compatible to other international standards as possible (cf. Section 3.4). In particular, activities from the Cloud Security Alliance[16] have a strong international relevance for CSPs and thus are also of importance for MEDINA. Dedicated persons from the MEDINA project, such as Christian Banse of Fraunhofer AISEC are part of different working groups within the Cloud Security Alliance, namely the Cloud Controls Matrix v4 (CCMv4) working group as well as a newly established working group on Continuous Audit Metrics. An initial report[17] related to the latter working group has been actively supported by MEDINA, and the developed metrics are being analysed by the corresponding technical WP.

[16] https://cloudsecurityalliance.org/
[17] https://cloudsecurityalliance.org/artifacts/the-continuous-audit-metrics-catalog/

4 Standardization Roadmap (First Iteration)

This section elaborates on the first version of MEDINA's standardization roadmap, which is our "guiding light" both for (i) the standardization activities taking place within the project, and also for (ii) our expert opinion on the core topics where SDO/SSO engagement is needed for sustaining MEDINA's framework and EUCS.

The section starts with a description of the proposed approach for creating the standardization roadmap, followed by a presentation of the identified topics, and their synergies within the SDO/SSO community.

4.1 Methodological Approach

In order to develop MEDINA's standardization roadmap, the consortium has followed a methodological approach consisting of the activities listed below:

1. The starting point for the roadmap are the project's scouting activities presented in Section 2.2, which provide the consortium with a landscape overview of SDO/SSO activities associated with the MEDINA framework.
2. The information provided by our scouting activities is then complemented by our interactions with the expert SDO/SSO community. We refer in particular to our ESG[18] members where the following key representatives have been engaged:
    a. Dr. Eric Vetillard (ENISA[19], EUCS lead).
    b. Dr. Michaela Iorga (NIST[20], OSCAL lead).
    c. Mrs. Meghan Herster (Oracle, ISO/IEC 27017 lead).
    d. Dr. Clemens Doubrava/Dr. Patrick Grete (BSI[21], C5 lead)
3. Finally, for MEDINA is also essential the results coming from our empirical validation of the developed framework (cf. Work Package 6), where input from practitioners is then used to refine both scouting and ESG feedback.

Needless to say, that the presented approach is not a one-time-activity, but an iterative task which refines the roadmap during the execution of the project. Finally, it is also worth mentioning that the standardization roadmap plays an essential role in the project's sustainability which is expected to last even after MEDINA has finalized.

Next, we present our initial set of standardization topics, as identified for our roadmap based on the approach described in the previous paragraphs.

4.2 Topics for Standardization

Departing from the approach described above, the consortium identified a set of standardization topics which have the potential to increase the impact of MEDINA's outcomes, while at the same time supporting the uptake of EUCS. These topics are summarized in Table 3. Furthermore, the roadmap was also presented to ENISA in the context of the performed EUCS experimentation (see Section 3.1.3).

[18] Expert Stakeholder Group
[19] European Union Agency for Cybersecurity
[20] US National Institute for Standards and Technology
[21] Bundesamt für Sicherheit in der Informationstechnik

Table 3. Topics for Standardization Roadmap

Topic	Description/Comments	MEDINA Contribution/Action Item
Provide *implementation* guidance about EUCS requirements where some degree of automated monitoring is needed.	Close examination of the "Continuous (Automated) Monitoring" definition in the core EUCS document opens questions related to aspects like frequency for gathering compliance data, reference to use for comparing gathered data, and so forth. More detailed/concrete implementation guidance is needed for CSPs aiming to achieve continuous monitoring. As needed, we even suggest referencing technologies like Cloud Security Posture Management systems, which can greatly support implementation of continuous monitoring.	MEDINA is creating the so-called TOM Implementation Guidance (see D2.1 [3]), which is part of the framework component "Catalogue of Controls & Security Schemes". This implementation guidance is well suited for SSO where *recommended* good practices are in scope. An initial assessment has identified Cloud Security Alliance[22] as a potential target for this roadmap's topic, although further discussion with ENISA is also planned.
Provide *audit/assessment* guidance related to EUCS requirements needing some degree of automated monitoring.	In analogy to the previous topic, we also suggest developing concrete guidance for auditors working on continuous monitoring. Such guidance should tackle aspects like identification of deviations on the continuous monitoring systems, definition of operational effectiveness in the automated monitoring context, and so forth. Such guidance must also provide information about what CABs are expected to do with data coming from the CSPs' continuous monitoring systems. For example, to guide	The project is contributing with a thoughtful analysis of evidence management for continuous/automated monitoring. Associated tools and techniques will be also part of the MEDINA framework. Developed good practices (as documented in D3.1 [4], D3.2 [10], D3.3 [11], D3.4 [6], D3.5 [12] and D3.6 [13]), for automated management of technical and organizational measures, will be contributed to SSOs like Cloud Security Alliance[22] and even ISACA[23]. In both cases, the topic of automated audit has taken great importance during the last few years.

[22] Online https://cloudsecurityalliance.org/
[23] Online https://www.isaca.org/

Topic	Description/Comments	MEDINA Contribution/Action Item
	CABs (and CSPs) on actions to take with "compliance fluctuations" identified during the audit period.	
Provide a catalogue of metrics as part of the implementation guidance for EUCS.	The MEDINA team sees the need for a catalogue of metrics to be released as part of the implementation guidance related to continuous monitoring. Such catalogue will reduce the subjectivity of both CSPs and CABs while implementing/assessing a requirement related to continuous monitoring. For our team, the proposed Metrics Catalogue is seen as a necessary requirement for guiding CABs in assessing operational effectiveness and understanding the definition of target values defined by CSPs. The lack of such catalogue might result in partial implementations/assessments of "complex" EUCS requirements.	This very important topic is being directly tackled by MEDINA as presented in D2.1 [3]. The elicited set of metrics might not be in the scope of an SDO for taking over, mainly because of its non-prescriptive nature, so an SSO seems to be also the target audience for this outcome. Besides the discussions with Cloud Security Alliance, it is our belief that ENISA could also profit from publishing such catalogue. Other important aspects of the MEDINA metrics (e.g., the corresponding machine-readable format) are in the focus on the standardization roadmap topic presented below.
Guidance on selecting tools/technologies for automated (continuous) monitoring.	Stakeholders in EUCS, in particular CSPs and CABs, need further guidance on the tools/technologies implied as required for leveraging automated (continuous monitoring). Such tools/technologies can become a security risk by themselves if they cannot provide the required assurance to stakeholders e.g., if a tool has known vulnerabilities.	The proposed guidance is expected to be a result of the validation activities in MEDINA, where the project leverages commercial tools (i.e., the so-called Cloud Security Posture Management[24]) for integration into the overall framework. While keeping MEDINA's technology-neutral approach, we aim to discuss with SSOs the developed good practices which can be then profited by early MEDINA/EUCS-adopters.

[24] Cloud Security Posture Management (CSPM) refers to those tools used to automatically assess if the configuration of commercial cloud services (mainly IaaS and PaaS) is compliant with specific target values. More information https://www.techtarget.com/searchsecurity/definition/Cloud-Security-Posture-Management-CSPM

Topic	Description/Comments	MEDINA Contribution/Action Item
	Furthermore, it is necessary to discuss if the tool/technology itself must be also EUCS certified (if cloud-based) or should provide any other kind of assurance/certification. This might introduce additional complexities (e.g., compositional certification aspects) to the already challenging EUCS High.	At this stage we have identified both Cloud Security Alliance and ISACA as potential target SSO groups for this topic.
Support development of machine-readable formats.	Despite a machine-readable language is not required by EUCS, this is the basis for rolling out continuous (automated) monitoring. For example, providing the EUCS catalogue in a standardized machine-readable format, will benefit automation and adoption by CSPs. However, the machine-readable format should go beyond the representation of EUCS requirements, so it should also cover other elements like automated assessments. Only then, it might be possible to establish a functional ecosystem for continuous audit-based certification as envisioned by MEDINA.	The project is already collaborating with US NIST on their OSCAL initiative (see Section 3.4), which is by far the most promising alternative for a machine-readable language as envisioned by MEDINA. Furthermore, OSCAL is already showing its potential within SSOs like ISO/IEC SC27 where machine-readable representations of well-known catalogues like ISO/IEC 27001 are already being created.
Support the notion of continuous (automated) assessments.	Of utter importance for MEDINA is the adoption of the continuous/automated notion in standardized cloud security requirements. Such concept needs to be extended in EUCS, while in parallel should be also integrated into other well-known security control frameworks.	MEDINA contributes with the empirical validation of EUCS requirements related to continuous (automated) monitoring, which will be then used as initial experience to extend the coverage in the final catalogue being built by CEN CENELEC (see Section 3.2). This notion will be also brought to ISO/IEC (see Section 3.3).

4.3 Next Steps

As seen in the previous section, all the topics in MEDINA's standardization roadmap are already underway in the project's technical WPs. Also, Section 3 already presented the SDO/SSO activities of MEDINA which directly relate to the proposed roadmap. At the time of writing this deliverable, the MEDINA team agrees on the following prioritization of standardization efforts derived from the roadmap:

Table 4. MEDINA Roadmap - Next Steps

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 [3]) 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 (cf. Section 3.1) and the technical specification being developed by CEN CENELEC (cf. Section 3.2).
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

Roadmap Topic	Prioritization	Rationale
		relevant standardization landscape while continuing contributions to NIST (cf. Section 3.4).
Guidance on selecting tools/technologies for automated (continuous) monitoring.	**Low**	This guidance is important for early EUCS adopters, although our belief is that its development should be a consequence of MEDINA's exploitation activities (identification of potential market competitors).

5 Conclusions

This deliverable has reported on MEDINA's standardization activities which have taken place during the first half of the project's lifetime. The performed activities included a presentation of the designed approach towards identifying/contributing to relevant SDO/SSO, and a report on the actual activities performed by MEDINA on this specific topic. Our approach is allowing the project to create an impact on activities which are considered as critical for the uptake of our framework e.g., EUCS and CEN CENELEC.

Furthermore, this deliverable also presented the first version of MEDINA's standardization roadmap, which allows the consortium to structure and plan our activities taking place during the second half of the project's lifetime. The topics in the standardization roadmap have been prioritized to maximize the impact of the foreseen framework, while optimizing the usage of standardization resources.

The next (and final) version of this deliverable (D7.9 [7]) will report the latest version of the presented roadmap, including an update on the performed SDO/SSO activities, and the devised standardization activities which are considered essential for the project's sustainability.

6 References

[1] MEDINA Consortium, “D7.6 Exploitation and sustainability Report-v1,” 2022.

[2] MEDINA Consortium, “D7.7 Exploitation and sustainability Report-v2,” 2023.

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

[4] MEDINA Consortium, “D3.1 Tools and techniques for the management of trustworthy evidence-v1,” 2021.

[5] MEDINA Consortium, “D2.6 Risk-based techniques and tools for Cloud Security Certification-v1,” 2022.

[6] MEDINA Consortium, “D3.4 Tools and techniques for collecting evidence of technical and organisational measures-v1,” 2021.

[7] MEDINA Consortium, “D7.9 Standardization Roadmap-v2,” 2023.

[8] MEDINA Consortium, "D5.2 MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v2," 2022.

[9] MEDINA Consortium, “D7.4 Dissemination and Communication Report-v1,” 2022.

[10] MEDINA Consortium, “D3.2 Tools and techniques for the management of trustworthy evidence-v2,” 2022.

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

[12] MEDINA Consortium, “D3.5 Tools and techniques for collecting evidence of technical and organisational measures-v2,” 2022.

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

APPENDIX A: Assurance Levels in EUCS (Draft November 2020)

Level	Basic	Substantial	High
Intention	Provide limited assurance through a review by an independent third party that the cloud service is built and operated with procedures and mechanisms to meet the corresponding security requirements at a level intended to minimize the known basic risks of incidents and cyberattacks.	Provide reasonable assurance through evaluation by an independent third party that the cloud service is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The CSP has assessed those risks and implemented suitable controls that, if operating effectively, minimize those risks and meet the corresponding security requirements throughout a specified period.	Provide reasonable assurance through evaluation by an independent auditor that the cloud service is built and operated with procedures and mechanisms to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources. The CSP has assessed those risks and implemented suitable controls that operated effectively to minimize those risks and meet the corresponding security requirements throughout a specified period. Security controls are monitored for continuous operation in accordance with their design; they are reviewed, and pen tested to validate their actual ability to prevent or detect security breaches.
Intention rationale	Scope, depth and rigour of the evaluation level is limited to procedures and mechanisms for those security requirements that shall minimize basis risks only.	Scope, depth and rigour of this evaluation level requires the cloud service provider to apply a risk-based approach for the suitable design and implementation of controls that meet the corresponding security requirements. The systematic risk assessment approach and the operating effectiveness (consistent application) of controls throughout a specified period is evaluated by an independent auditor,	Scope, depth and rigour of this evaluation level extends the previous level by additional procedures to be performed for automated controls. Automated monitoring is applied by the CSP to identify exceptions in the application of controls (*e.g.* changes to the configuration) and initiate corrective actions. Reviews and pen tests are performed by the independent auditor or a third party engaged by the CSP with the objective to identify vulnerabilities that allow to circumvent, override or breach controls.

Level	Basic	Substantial	High
		including for the initial conformity assessment.	
Suitability	This level is suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems.	This level is suitable for cloud services that are designed to meet typical security requirements on services for business-critical data and systems.	This level is suitable for cloud services that are designed to meet specific (exceeding assurance level 'substantial') security requirements for mission critical data and systems.
Suitability rationale	This level provides limited assurance that baseline procedures and mechanisms are in place to address security risks and threats in potentially low impact information systems (e.g.: Web site hosting public information). It is typically not suited for Platform or Infrastructure capabilities, used by a large number of services. built on top and that require an elevated level of security. This level demonstrates a willingness to address security, including the application of security guidance from subservice providers.	This level provides reasonable assurance that a set of more stringent security controls is designed and operated to address security risks and threats in potentially moderate impact information systems to protect business critical information (e.g.: Confidential business data, email, CRM – customer relation management systems, personal information). It is suitable for all capabilities types. This level demonstrates a robust and mature holistic security management to provide secure services.	This level provides reasonable assurance that a set of even more stringent security controls is designed and operated to address security risks and threats in potentially high impact information systems to protect mission critical information (e.g. highly confidential business data, patents). The costly and rigorous evaluation process reflects the intention to minimize the risks in using the cloud service.
Attacker profile	Single person with limited skills repeating a known attack with limited resources, not including the ability to perform social engineering attacks.	Small team of persons with hacking abilities and access to a wide range of known hacking techniques, including social engineering, but with limited resources, in particular to launch wide attacks or to discover	Team of highly skilled persons with access to significant resources to design and perform attacks, get insider attacks, discover or buy access to previously unknown vulnerabilities.

Level	Basic	Substantial	High
		previously unknown vulnerabilities.	
Attacker profile rationale	Today, this is about removing low-lying fruits and ensuring that cloud services, including simple ones, are designed with security in mind. The objective is to remove the possibility to fall victim to trivial attacks. When such certification becomes mainstream, the requirements should be revised upwards.	This is the "standard" attacker, corresponding to most real-life attacks used to disclose information, steal resources, deny service, or tamper with a service. Their main characteristics come from the definition of the level: "known attacks" and "limited resources". Note that this definition is quite ambitious and allows the use of attacks that leverage several vulnerabilities.	This is the sophisticated attacker, against which detection and mitigation is more efficient than resistance. At this level, it may be difficult to define precisely a way to analyse that the objective has been met, in particular because there is an expectation to minimize risks through various mitigation methods.
Scope	As defined by the service description and the controls pertaining to this level, including processes and the software (understood as result of a development process) underlying the service. .	As defined by the service description and the controls pertaining to this level, including processes and the software (understood as result of a development process) underlying the service. Operating effectiveness of the controls shall be demonstrated.	As defined by the service description and the controls pertaining to this level, including processes and the software (understood as result of a development process) underlying the service. Operating effectiveness of the controls shall be demonstrated. (including automated monitoring if required by the control definition).
Scope rationale	This may need to be rephrased, depending on the relationship between "controls" and "requirements". Here, the idea would be to include all controls in their general form, but without the more detailed requirements	We refer to the same controls from the Basic assurance level, but with the stronger refinements or enhancements (e.g., (mandated techniques, thresholds, *etc*.).	We refer to the same controls from the Substantial assurance level, but with the higher refinements or enhancements. Enhancements often included additional constraints, references to state-of-the-art requirements, and automated monitoring of some controls.

Level	Basic	Substantial	High
	that may be added for higher levels.	Requirements must include a limited pen testing using known attacks.	
Depth	Inspection solely, based on a check for completeness and coherence of the provided documentation on processes and design intended to confirm the fulfilment of technical and organizational measures, and interactions between the auditor and the CSP at the beginning and at the conclusion of the inspection. A report following defined procedures is generated by the inspection body. Once a year, a documentation update is provided for third-party review of the continued development and operation of the service.	Additional to the requirements of the Basic level: On-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified policies and procedures, and an additional focus on development activities, for instance on the functional tests performed. On the initial assessment and once a year, the operating effectiveness of the security controls, *i.e.* their operation as designed, needs to be demonstrated over the previous period.	Additional to the requirements of the Substantial level, specific requirements on the monitoring and testing of the controls, i.e. their operation as intended to protect from attacks or detect them, needs to be demonstrated. Different measures may be used, such as technical reviews, and penetration testing shall be performed by qualified personnel, following a multi-year plan that needs to be validated in the audit.
Depth rationale	The inspection focuses on completeness, coherence and plausibility of the documentation. It needs to be an efficient process that mostly focuses on the existence of processes, and of a secure by design approach, to demonstrate the proper design and existence	The full audit aims at providing reasonable assurance that the security controls are properly designed and operate effectively, *I,e,* as designed, over a period of time.	The audit aims at providing the same reasonable assurance as for the Substantial level. The main addition in depth come from additional requirements for level Substantial such as automated monitoring and penetration testing, which are intended to demonstrate that the controls remain effective under strenuous conditions.

Level	Basic	Substantial	High
	of security measures to protect the cloud service.		
Rigour	The assessment is performed by the CSP and driven by a standardised checklist. An accredited third-party then audits the assessment report and its supporting documentation.	The assessment is performed by an accredited third-party, and it is driven by a risk analysis performed by the CSP, which is in the audit scope.	The assessment is performed as for the Substantial level, but the CAB needs to be authorized by the NCCA to it has the required competencies to audit the specific requirements of the Substantial level. More rigour is expected in the definition and application of policies, usually as defined in requirements specific to the controls (*e.g.* the need to demonstrate the coverage of functional tests used in development). A specifically accredited and authorized CAB needs to be involved in the performance of vulnerability identification and penetration testing activities.
Rigour rationale	The assessment follows all items in a checklist suited to the targeted cloud service, and its results are reviewed by an accredited third-party.	A full audit is performed by an independent third-party, and the checklist approach is replaced by a more rigorous risk-based approach, allowing the auditor to identify controls that require specific attention.	The rigour remains mostly the same as for level Substantial as it corresponds to typical audit conditions. Nevertheless, specific requirements explicitly increase the level of rigour on some controls by requiring additional deliverables from the CSP. The addition of testing by a CAB provides an additional level of rigour around the critical activities of vulnerability identification and penetration testing

APPENDIX B: Basic EUCS Questionnaire Contribution (excerpt)

ReqID	Requirement	Level	Question ID	Statement/Questions	Answer	Evidence
OPS-01.1	The CSP shall document and implement procedures to plan for capacities and resources (personnel and IT resources), which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload	Basic	Q1-OPS-01.1	Does the CSP document procedures to plan for capacities and resources (personnel and IT resources)?		- Capacity plan - Specific capacity procedures
			Q2-OPS-01.1	Do procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload?		- Capacity plan (encompasses future capacity requirements) - Specific capacity procedures
			Q3-OPS-01.1	Does the CSP implement procedures to plan for capacities and resources (personnel and IT resources)?		- Capacity plan audit
OPS-01.2	The CSP shall meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of capacity bottlenecks or personnel and IT resources outages	Basic	Q1-OPS-01.2	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of capacity bottlenecks?		- Monitoring reports - Non-conformities to the contract (if there are non-compliances)
			Q2-OPS-01.2	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of IT resources outages?		- Monitoring reports - Non-conformities to the contract/SLA (if there are non-compliances)
OPS-01.3	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning	High				
OPS-02.1	The CSP shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement	Basic	Q1-OPS-02.1	Does the CSP define technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?		- Multidimensional QoS prediction methods

			Q2-OPS-02.1	Does the CSP implement technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	- Service level agreement - SLA compliance report
			Q3-OPS-02.1	Does the CSP define organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	- Multi-dimensional QoS measures
			Q4-OPS-02.1	Does the CSP implement organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	- Service level agreement - SLA compliance report
OPS-02.2	The CSP shall make available to the cloud customer the relevant information regarding capacity and availability on a self-service portal	High			
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1	High			
OPS-03.1	The CSP shall enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs	Basic	Q1-OPS-03.1	Does the CSP enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs?	- Contract - SLA - Privileges to use the monitoring and control tools

APPENDIX C: Report to ENISA on EUCS Experimentation

This report discusses lessons learned related to the experimentation performed by the MEDINA team on the topic of continuous (automated) monitoring, just as required by the High Assurance baseline of the draft version of the European Cybersecurity Certification Scheme for Cloud Service (EUCS). Besides the reported process and obtained results, we also provide a set of recommendations to relevant stakeholders (in particular Cloud Service Providers and Auditors) with the goal of supporting the uptake of EUCS for High Assurance.

MEDINA

ENISA EUCS Experimentation with Automated Monitoring Requirements

(Technical Report)

Editor(s):	Jesus Luna Garcia
Responsible Partner:	Robert Bosch GmbH
Status-Version:	1.0
Date:	01.09.2021
Distribution level:	Restricted (ENISA)

Project Number:	952633
Project Title:	MEDINA

Title of Technical Report:	ENISA EUCS Experimentation with Automated Monitoring Requirements

Workpackage responsible for the Deliverable:	WP6, WP7
Editor(s):	Jesus Luna Garcia, Bosch
Contributor(s):	Thomas Ruebsamen, Bosch Valentin Acker, Bosch Björn Fanta, Fabasoft Tatu Suhonen, Nixu Jarkko Majava, Nixu
Reviewer(s):	N/A
Approved by:	All Partners
Recommended/mandatory readers:	N/A

Keyword List:	ENISA, EUCS, OSCAL, Automated Monitoring
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	05.08.2021	First draft version	Bosch
V0.5	30.08.2021	Full draft	Bosch, Nixu, Fabasoft
V1.0	03.09.2021	First version	Bosch

Table of contents

List of tables

List of figures

Terms and abbreviations

API	Application Programming Interface
CAB	Conformance Assessment Body
CISO	Chief Information Security Officer
CSA or EU CSA	EU Cybersecurity Act
CSP	Cloud Service Provider
EC	European Commission
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
ICO	Internal Control Owner
IoT	Internet of Things
KPI	Key Performance Indicator
NLP	Natural Language Processing
PII	Personally Identifiable Information
SaaS	Software as a Service
TOM	Technical and Organizational Measure

Executive Summary

This report summarizes the process and results of the experimentation performed by the MEDINA team on the topic of continuous (automated) monitoring in EUCS. Furthermore, we also provide a set of recommendations based on our practical experience, which aim to facilitate the adoption of continuous monitoring requirements in the scope of this EUCS proof of concept.

1 Introduction

The novel EU Cybersecurity Certification Scheme for Cloud Services (EUCS) introduces the notion of continuous (automated) monitoring, for selected high-assurance requirements, in the following manner:

> *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 scheme;*
> 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 High, remains a mid- or long-term objective, and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.*

The EU MEDINA consortium acknowledges the technological and organizational challenges associated with the implementation of continuous monitoring as envisioned by EUCS, and therefore experimented with a set of applicable requirements to provide ENISA with relevant feedback.

This report presents the performed experimentation, discusses obtained results, introduces and MEDINA's recommendations for facilitating the adoption of this novel approach.

The rest of this document is organized as follows: Section 2 provides high-level background on the EU MEDINA project, Section 3 describes the objectives and approach of the performed experimentation, Section 4 presents the obtained results, Section 5 discusses the CAB's perspective, and Section 6 provider the MEDINA team's recommendations to ENISA.

2 Background: EU-funded MEDINA Project

Cloud computing brings evident benefits to both private and public sector in Europe, however its whole potential has not yet been released partially because the EU customers' perceived lack of security and transparency in this technology. Cloud service providers (CSPs) usually rely on security certifications as a mean to improve transparency and trustworthiness, however European CSPs still face multiple challenges for certifying their services (e.g., fragmentation in the certification market, and lack of mutual recognition).

In an effort to solve some of the challenges depicted above, the EU Cybersecurity Act (EU CSA, approved in June 2019) in its Title III gives ENISA the mandate of defining and implementing a European security certification scheme for ICT products, processes and services. Being cloud computing one of the identified EU CSA priorities, Articles 54 (j) and 57 (9) propose the possibility of deploying a high-assurance, evidence-based and continuous certification of European cloud providers. In this context, the EU Cybersecurity Act (EU CSA) proposes improving customer's trust in the European ICT market through a **European certification scheme for cloud services (EUCS)**. The EUCS introduces novel concepts including:

- Three different levels of assurance (Basic, Substantial, and High),
- Composition of certifications for the cloud supply chain,
- Automated/continuous monitoring for high assurance certification.

Such novelties in EUCS convey new technological challenges for cloud service providers, which need to be solved for fully achieving the expected benefits (including those for cloud customers). In this context, the main objective of the MEDINA European research project is to **provide a holistic framework that enhances cloud customers' control and trust in consumed cloud services**, by supporting CSPs (IaaS, PaaS and SaaS providers) towards the successful achievement of a continuous certification aligned to the EUCS. The proposed framework will be comprised of tools, techniques, and processes supporting the continuous auditing and certification of cloud services where security and accountability are measurable by design. As the MEDINA framework is leveraged into a cloud supply chain, it will support continuously assessing the efficiency and efficacy of security measures to ultimately achieve and maintain a certification.

The rest of this section further elaborates on the MEDINA approach as required in the context of the performed ENISA experimentation.

2.1 Metrics Catalogue

The current EUCS draft[1] provides an organized set of security requirements, mostly based on international standards, which shall we leveraged to certify cloud services. Despite such comprehensive set of requirements, EUCS does not define the concrete metrics which can be used to (automatically) assess them. The lack of standard EUCS-metrics can become a problem for future adopters (including auditors), which might be leveraging their own custom metrics for assessing the EUCS requirements in an automated manner. MEDINA is defining a catalogue of metrics associated to technical and organizational measures (TOMs) in EUCS. The metrics repository in MEDINA covers topics such as those related to system security and integrity, operational security, business continuity and incident management.

2.2 Security Controls

MEDINA proposes a risk-based, tool-supported methodology for the selection of EUCS-complementary controls and associated TOMs based on the CSP's risk appetite. Such controls

[1] Please refer to https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

and requirements shall address the concrete needs of a CSP, by also taking into consideration the targeted EUCS assurance level.

2.3 Certification Language

In practice, all security control frameworks (EUCS included) are defined in natural language, which at some point need to be "translated" into a machine-readable representation for purposes related to managing the security life cycle of cloud services. A machine-readable representation of frameworks like EUCS should facilitate the elicitation of metrics and controls as referred in the previous sections. MEDINA proposes to transform the natural-language specification of control frameworks like EUCS into a machine-readable expression, by using NLP. The expected outcome should comprise aspects like scope of the certification, assurance level and conformity assessment method.

2.4 Evidence Collection and Continuous Audit

Essential for achieving continuous audit-based certification is the collection of actual, technical evidence related to the automated monitoring (EUCS). From a technical point of view, one could distinguish between tools and methodologies to address this at code level and at service level. The topic of managing digital evidence related to EUCS will become critical once CSPs start applying for a high-assurance certificate.

MEDINA aims to develop a framework for managing digital evidence related to EUCS. Collected evidences need to be continuously evaluated, so risks are also continuously monitored and updated. Collected evidence in MEDINA will explore leveraging DLT / blockchain techniques for implementing accountable tracking.

2.5 Standardization Roadmap

Standardization is a necessary milestone to guarantee both market adoption and future governance of EUCS. Despite EU/international standardization initiatives can take a long time to provide concrete results, it is required to develop a strategic roadmap (1-3 years vision) which prioritizes the MEDINA's framework components. MEDINA will drive efforts to influence relevant standards bodies (such as ETSI, ISO, BSI, or US NIST), on the basis of the project results. Whenever applicable, the project will promote the adoption of existing or emerging standards to its own R&D activities.

3 Description of Experimentation

In this section we describe the objective and overall approach for performing the referred EUCS experimentation.

3.1 Objective

The main goal of the presented EUCS experimentation is creating a proof of concept (PoC) related to the *automated monitoring requirements from the EUCS High Assurance baseline*. It is worth to notice that such PoC is not a formal feasibility analysis of the referred EUCS requirements, but a first step in providing practical experience with its implementation.

Furthermore, because the PoC was fully carried over in the context of MEDINA, we want to acknowledge the following conditions related to its execution:

- No additional funding was required for the PoC, beyond that provided to the MEDINA consortium by the EC.
- No additional development activities took place, beyond those committed in the MEDINA's Description of Action document (DoA).
- This present report is made also available as a MEDINA's dissemination activity.
- The PoC is fully based on EUCS requirements and methodologies described on the draft specification published by ENISA on December 2020.
- No National Accreditation Body (NAB) was involved in the PoC.

3.2 Approach

Given the above objective of the PoC, the rest of this section further details the experimentation performed by MEDINA.

3.2.1 Team

The MEDINA team participating in this PoC consisted of the following:

Table 1. MEDINA team participating in the ENISA PoC

Role	Company	Contact	Email
CAB	Nixu	Niki Klaus	Niki.Klaus@nixu.com
CSP	BOSCH	Jesus Luna Garcia	jesus.lunagarcia@de.bosch.com
CSP	Fabasoft	Björn Fanta	bjoern.fanta@fabasoft.com

3.2.1.1 NIXU (CAB)

Nixu is a cybersecurity services company on a mission to keep the digital society running. Nixu's passion is to help organizations embrace digitalization securely. Partnering with its clients Nixu provides practical solutions for ensuring business continuity, an easy access to digital services and data protection. It aims to provide the best workplace to its team of almost 400 cybersecurity professionals with a hands-on attitude.

Nixu is the largest company specialized in cybersecurity services on the Nordic market. Its clients are typically large, internationally operating companies or government organizations. Nixu has Nordic roots and employs experts in Finland, Sweden, the Netherlands, Denmark, and Romania. From these locations, Nixu's experts work on customer assignments around the world.

Nixu has a strong brand and it has established its position as a trusted cybersecurity partner for its clients. More than 30 years of experience in the sector, the best experts in the industry, and a wide range of comprehensive cybersecurity services make Nixu a reliable partner for clients and an attractive place to work for cybersecurity experts. Founded in 1988, Nixu's shares are listed on the Nasdaq Helsinki Stock Exchange.

Nixu Certification Oy is a fully owned subsidiary of Nixu Corporation and operating as an official Information Security Inspection Body approved by the National Cyber Security Centre (NCSC-FI) and as a certification body accredited by the Finnish Accreditation Service (FINAS).

Nixu Certification is accredited to perform audits for e.g. ISO 27001 as well as Katakri 2015 (Information security audit tool for authorities) on protection levels IV and III (corresponding to international classification levels Restricted and Confidential). Nixu is also an accredited CSA STAR auditor (Cloud Security Alliance) which is an international certification scheme based on the Cloud Controls Matrix (CSA CCM). The national cloud certification criteria in Finland is called PiTuKri. Nixu has worked with the criteria but currently no conformity assessment bodies can request an accreditation for the standard.

3.2.1.2 Robert Bosch GmbH (CSP and service)

The Bosch Group (www.bosch.com) is a leading global supplier of technology and services. Its operations are divided into four business sectors: Automotive Technology, Industrial Technology, Consumer Goods, and Energy and Building Technology. The Bosch Group comprises Robert Bosch GmbH and its roughly 360 subsidiaries and regional companies in some 50 countries. If its sales and service partners are included, then Bosch is represented in roughly 150 countries. This worldwide development, manufacturing, and sales network are the foundation for further growth. The Bosch Group's products and services are designed to fascinate, and to improve the quality of life by providing solutions which are both innovative and beneficial. In this way, the company offers technology worldwide that is "Invented for life."

Robert Bosch's central security governance unit (C/IDS) is responsible for the global IT security governance of the Bosch group. It provides Bosch with state-of-the-art IT security requirements and processes for ICT services and products (including Cloud).

Recognizing that the process of digital transformation and the productive phase of the IoT has begun to accelerate, Bosch sees clearly that becoming "best-in-class" will be a differential factor in the IoT market. Furthermore, "best-in-class" must be achieved based on a holistic/end-to-end manner considering all involved services in the supply chain, which evidently include cloud computing back-ends.

With this goal in mind, Bosch participation in the ENISA POC for the EUCS aims to bring obtained know-how from the EU H2020 project MEDINA (https://medina-project.eu/) on the topic of automated monitoring for EUCS' high level of assurance. Considering security as a quality measure, Bosch expects that the experience and feedback obtained from the ENISA POC will further pave the road for our organization towards EUCS adoption. Furthermore, given the evident synergies between EUCS and MEDINA, we also see a clear win-win situation for both initiatives, for which Bosch is delighted to contribute.

It is worth to mention that Bosch, represented by Dr. Jesus Luna Garcia for the ENISA POC, is also member of the ENISA AdHoc WG for EUCS. Furthermore. Dr. Luna is also technical manager of the MEDINA project.

Bosch in its role of cloud service provider is mainly using both Microsoft Azure and Amazon AWS to deploy resources allowing enablement of our PaaS which are used as backends of connected

products. Take for example our public cloud-based Bosch IoT Suite[2], which is the basis on which we build IoT solutions, services, and projects. At the time of writing, the Bosch IoT Suite connects more than ten million sensors, devices, and machines with their users and enterprise systems.

3.2.1.3 Fabasoft and the Fabasoft Cloud (CSP and service)

Fabasoft (www.fabasoft.com) is a European software manufacturer and cloud provider with over 30 years of experience in document and process management. Fabasoft digitalizes and accelerates business processes in the course of informal collaborations and structured workflows both within companies and governmental institutions. The software products and cloud services from Fabasoft ensure the consistent capture, sorting, process-oriented handling, secure storage and context-sensitive finding of all digital business documents. These functions are used in both on-premises installations, as well as in Software as a Service (SaaS) cloud solutions. Beyond that, the Fabasoft Appliance Concept offers a direct way to provide customers with standardized complete systems (hardware and software) for use in their own data processing centers.

In the Fabasoft Cloud customers can choose where their data are to be stored, Fabasoft offers several European cloud locations. In each location data are stored synchronously in separate data centers. Both data transmission and data storage are carried out in encrypted form in the data centers. Fabasoft Cloud locations are currently available in Germany, Austria and Switzerland.

The Data Centers provide Fabasoft with the necessary rack space, power and cooling. In addition, they establish the connection between the Data Centers and provide internet routing. The infrastructure at platform level, to host, run and extend the cloud services is set-up, deployed and maintained by Fabasoft itself. This ensures full-stack control and enables Fabasoft to test and verify security controls on all layers. Fabasoft Cloud services are operated exclusively by Fabasoft.

Fabasoft/Fabasoft Cloud is already compliant with the following standards or certifications:

- ISO 9001
- ISO 20000-1
- ISO 27001 including ISO 27018 controls
- BSI C5:2017 (C5:2020 audit is currently in progress)
- ISAE 3402 Type 2
- SOC2 Type 1 (SOC2 Type 2 audit is currently in progress)
- TÜV Rheinland Certified Cloud Service
- Cyber Trust Gold Label

3.2.2 Timeline

The ENISA PoC took place between April-2021 and September-2021, just as seen in the following figure:

[2] Please refer to https://bosch.io/iot-technology/

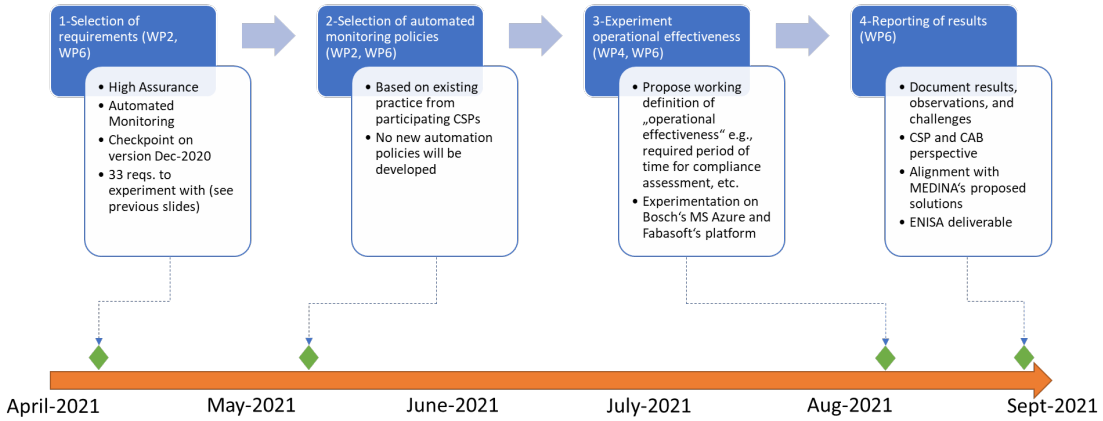

Figure 1. Timeline of the ENISA PoC.

Based on the presented timeline, the ENISA PoC was performed as shown on the next table.

Table 2. Detailed description of adopted approach

Stage	Explanation	Comment
1	Selection of EUCS requirements	The requirements to implement came from the EUCS High Assurance baseline, where the keyword "automated monitoring" is used.
2	Selection of automated monitoring policies	The automated monitoring policies (for the Azure testbed) were selected based on the set of chosen EUCS requirements. Such policies came from the custom catalogue developed by Bosch.
3	Experiment the EUCS concept of *operational effectiveness* for automated monitoring requirements	The selected policies were deployed in a testbed (cf. Section 3.2.4) for a period of 30 days to simulate the EUCS notion of *operational effectiveness*.
4	Document results, observations and challenges	The present report was produced to compile results and recommendations related to the real-world usage of the experimented EUCS requirements.

3.2.3 Implemented Requirements

The set of requirements used for the ENISA PoC is shown in the next table.

Table 3. EUCS requirements for the ENISA PoC

Requirement ID	Requirement Text
OIS-02.4	The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
ISP-03.7	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-03.5	The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program
HR-05.4	The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2
HR-06.7	The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers
AM-01.6	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date
AM-03.6	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.
AM-04.4	The verification of the commitment defined in AM-04.1 shall be automatically monitored
PS-02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1
OPS-05.3	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities
OPS-07.2	The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1
OPS-07.3	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1

Requirement ID	Requirement Text
OPS-09.5	When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1
OPS-12.4	The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1
OPS-13.7	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2
OPS-18.6	The CSP shall equip with automatic update mechanisms 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-21.3	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications
IAM-03.11	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03
IAM-03.12	The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons
CS-04.5	The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1
CCM-03.10	The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues
CCM-04.3	The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1
CCM-05.3	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1
PM-04.7	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).
PM-04.8	The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action

Requirement ID	Requirement Text
IM-03.4	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period
CO-03.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions
CO-03.5	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-03.4	The CSP shall automatically monitor the accesses performed by or on behalf of investigators to ensure that they correspond to the determined legal basis
PSS-04.3	An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images

3.2.4 Testbed

For the presented ENISA PoC, we leveraged Bosch's continuous compliance monitoring service (CCM), in particular the one deployed in the Microsoft Azure cloud. At the time of writing such service is continuously monitoring compliance of more than 27.400 cloud resources with respect to Bosch's internal security governance framework (based on ISO/IEC 27001). For Bosch CCM in Azure we have custom-developed approximately 120 policies[3] able to continuously assess the security posture of widely used services like Virtual Machines and SQL databases. Such CCM service as deployed in Microsoft Azure, along with the current developed policy set mapped to EUCS, was the basis for the performed ENISA POC.

Fabasoft uses the monitoring tool app.telemetry[4] for almost every monitoring aspect within the Fabasoft Infrastructure and the SaaS solution parts. App.telemetry is an inhouse solution, which was build several years ago as the need for thorough investigation of actions and processes within systems and systems of systems was needed. The way it works is that it offers an agent to client structure, whereas every agent counts as a telemetry-point. Fabasoft's system architects carefully distributed a network of agents throughout hard- and software and today, Fabasoft is able to monitor and investigate the whole system, even for actions within the SaaS cloud solution. Investigative controls can be designed by filters and scripts and a compliance manager could refine controls to monitor manifold security aspects – fully anonymized, if needed. Currently a dedicated scrum team of developers is maintaining and improving app.telemetry for Fabasoft's and customer's needs. Due to Fabasoft's knowledge of creating controls for BSI C5 and SOC2 with app.telemetry, it is possible to adapt existing scripts to the EUCS or transform this know-how into new scripts and continuous data collection for new ones.

[3] More information about the underlying technology can be found here https://docs.microsoft.com/en-us/azure/governance/policy/
[4] https://www.fabasoft.com/en/products/fabasoft-apptelemetry

4 Results

This section summarizes the main results obtained from the ENISA PoC.

4.1 Metrics for EUCS Requirements

In order to develop the automation policies corresponding to the EUCS requirements in scope of the experimentation (see Table 3), we realized the need for eliciting "compliance metrics". Such metrics provide concrete information for automating EUCS requirements, namely:

- Requirement ID: corresponding to the actual ID based on the EUCS core document.
- Metric Name: descriptive name for the metric, which can be used later for the automation policy.
- Metric Description: short explanation of the metric's purpose (i.e., how it relates to the corresponding EUCS requirement).
- Scale: possible set of values which can be taken by the metric depending on the referenced EUCS requirement.

The metric bridges the gap between the EUCS requirement and its concrete machine-readable implementation in an assessment policy (technology-dependent). Our experimentation demonstrated that with a metric containing the information mentioned above, plus the target value specified by the CSP, it was enough for developing the corresponding automation policies in our testbed.

A draft version of MEDINA's metrics catalogue can be found in Appendix A, and it was used as starting point to implement the automated assessment policies discussed in the following section. Please notice that at the time of writing, the introduced metrics catalogue does not provide full coverage of all related EUCS high requirements.

4.2 Automated Assessment Policies

Once metrics have been written for the EUCS requirements, as referred in the previous section, it is possible to develop the corresponding automated assessment policies for the CSP. It is worth to notice that at the state of practice, the language used to write the automation policies is highly depend on the CSP or underlying technological provider[5]. However, based on our field experience, most policy languages available in commercial solutions/public CSPs, support the minimum set of primitives needed to represent metrics like the ones found in Appendix A.

It is worth to notice that assessment polices are related to specific cloud services (e.g., Virtual Machine, SQL server, Virtual Network and so on) i.e., each service needs its own set of assessment policies even if the same EUCS requirement is being evaluated.

An excerpt of the automated assessment policies leveraged in this experimentation, and their relationship to the EUCS requirements, can be seen in the following table:

[5] Usually called Cloud Security Posture Management system (CSPM).

Table 4. Excerpt of leveraged Automation Policies (Azure)

Policy Definition (Azure specific)	Azure Service	EUCS Requirement ID
/providers/Microsoft.Management/managementgroups/RB/providers/Microsoft.Authorization/policyDefinitions/EISA-OPS-401-AKS-ContainerMonitoring	Kubernetes	OPS-12.4 OPS-13.7
/providers/Microsoft.Management/managementGroups/RB/providers/Microsoft.Authorization/policyDefinitions/EISA-OPS-401_DiagLogs_AnServ	LogAnalytics	OPS-12.4 OPS-13.7
/providers/Microsoft.Management/managementGroups/RB/providers/Microsoft.Authorization/policyDefinitions/EISA-COM-105_VNet_APIMgt-disable-developer	API Manager	OPS-21.3
/providers/Microsoft.Management/managementGroups/RB/providers/Microsoft.Authorization/policyDefinitions/EISA-COM-105_VNet_APIMgt	API Manager	CS-04.5

During the performed experimentation, we only deployed automation policies for the Azure resources related to our testbed (see Section 3.2.4), which resulted in a coverage of less than 50% of the targeted set of EUCS requirements. Furthermore, the deployed policies related only to the Azure cloud, so other non-cloud systems in the focus of the requirements (e.g., IT security training records for employees) were out of scope.

Finally, it is also worth to notice that not all resources in our testbed supported the implementation of the relevant automation policies as required by EUCS. While a Virtual Machine could be automatically assessed for OPS-05.4 (antimalware scans), this was not possible for a Storage Account service due to technical limitations on the CSP-side.

4.3 Visualizations - EUCS Dashboard (Proof of concept)

As part of our ENISA POC related to the topic of "operational effectiveness" in EUCS for automated monitoring requirements, we developed a draft dashboard to visualize/experiment compliance levels based on the automated assessment policies (presented in the previous section). The dashboard takes as input dataset the results from the automated assessments as supported by the Azure platform i.e., either Compliant or Non-Compliant. During the experimentation, these compliance results were collected for a set of test resources (called Subscription) once per-day in a period of 30 days. The developed visualizations are described in the rest of this section.

The first screen of the dashboard (see Figure 2) includes three visualizations. The first one shows the total number of non-compliances in the Azure subscription with a line chart. The second visualization on the right-hand side displays the average EUCS compliance in percentage. The third and last visualization on this page is a line chart which shows the non-compliances per assessed Azure resource type. As described in Section 3.2.4, this visualization considers only the three resource types (storageaccounts, virtualmachines, virtualnetworks) used for the specific purposes of this ENISA POC[6].

[6] To provide additional test capabilities, the configuration of the tested resources was changed during the 30-day period in order to simulate different compliances and non-compliances.

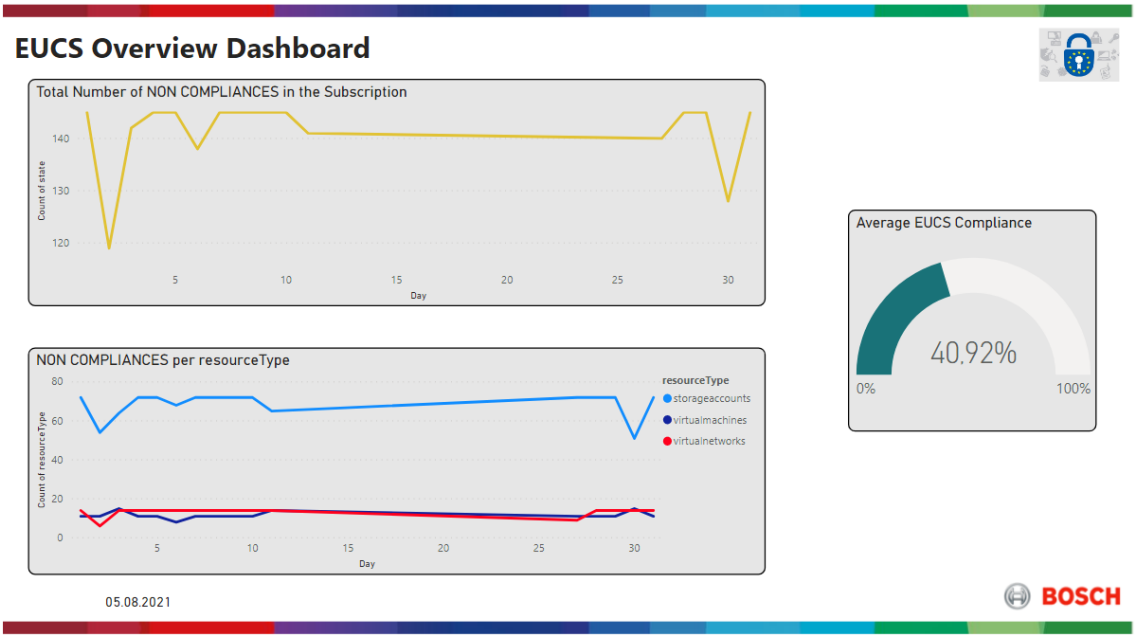

Figure 2. EUCS dashboard (Screen 1).

The second page (see Figure 3) includes two bar charts. The first one displays the EUCS requirement OPS-12.4. and includes the matching non-compliant metrics/automation policies in a 30 days view. The second visualization shows the EUCS requirement CS-04.5 with its matching non-compliant policies.

Developed visualizations can be further extended for a productive version of an EUCS dashboard, which might include all relevant EUCS requirements and associated metrics/policies. Such improvement were out of scope for this ENISA POC.

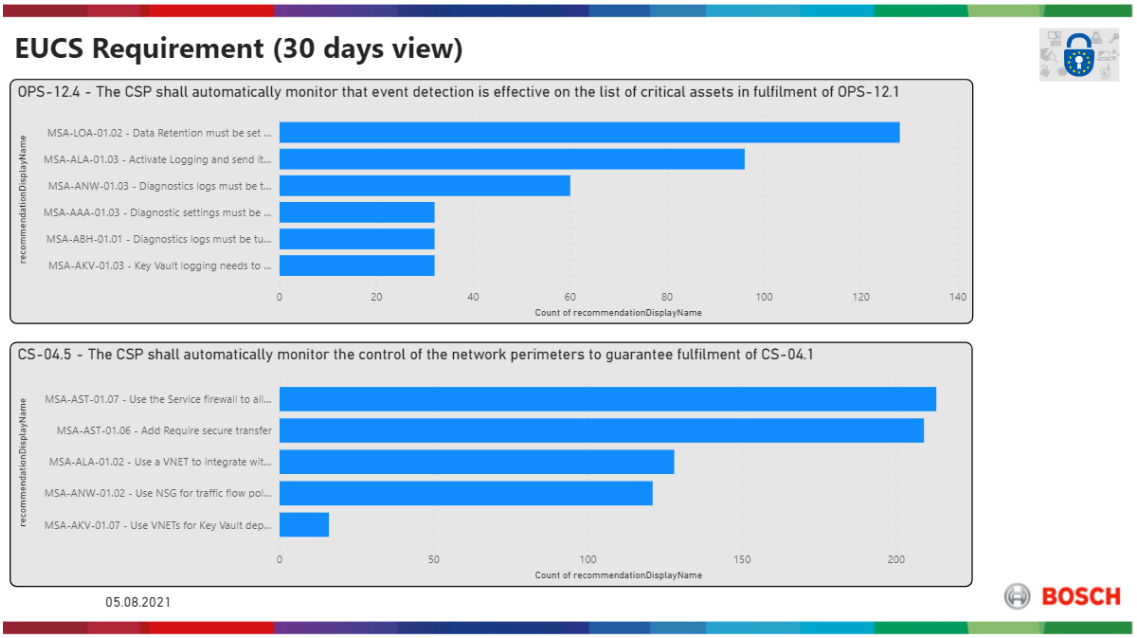

Figure 3. EUCS dashboard (Screen 2).

Developed visualizations were useful to start understanding the continuous compliance behaviour of the resources being assessed. For example, it was noticeable that the number of

non-compliances fluctuated during the analysed period probably because of a cloud resource being updated or redeployed.

In the case of visualizations like those shown in Figure 3, we notice that one EUCS requirement can be fulfilled by more than one assessment policy. This fact might complicate the auditor's decision about the (non-)compliance status of the evaluated cloud service.

4.4 Machine-readable format for EUCS (Proof of Concept)

In order to enable the usage of automation in compliance assessment policies as envisioned by the EUCS, we saw the need of leveraging standardized machine-readable languages able to represent the different elements of this certification scheme (e.g., controls, requirements, assessments, etc.). To the best of our knowledge, NIST OSCAL[7] is probably the most mature candidate in this specific field. The rest of this section further elaborates on the initial POC we developed to represent the EUCS catalogue of requirements in OSCAL format.

This part of the ENISA POC was developed with the JSON scheme of OSCAL, although other available possibilities to develop the OSCAL scheme were XML and yaml. Our choice of JSON purely obeyed the expertise of the available team.

The EUCS requirements are modelled as a hierarchy comprising the following eight levels:

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

The OSCAL scheme is implemented within a catalog element, which contains an UUID and other applicable metadata.

```
{
  "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 Domain and Category is created with the attribute "title". With usage of "parts" and "prose" the Objective can be added into OSCAL.

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

          "parts":[
            {
```

[7] Please refer to https://pages.nist.gov/OSCAL/

```
                "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 Control is specified with “title” and Control ID with “id” and “properties”.


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

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


To complete the Control, the Control Objective must been added within “parts” and is displayed in “prose”. Requirements and Control IDs are implemented with “parts” within the upper “parts” of Control. Requirement ID is specified with “properties” and the requirement itself with “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 proposed mapping from EUCS to OSCAL is shown in the following table:

Table 5. Proposed EUCS to OSCAL mapping

OSCAL	EUCS	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

The resulting OSCAL representation of the EUCS requirements will be made available on the MEDINA code repositories during the execution of the project.

5 The CAB Perspective on Continuous Monitoring and Continuous Auditing

The PoC offered Nixu a great opportunity to analyse the concept of continuous auditing and provide feedback to develop the innovations. Although the change in audit practice is not governed by the certification bodies, they are the ones with the hands-on experience in auditing and therefore can provide valuable views to the development of continuous auditing. For example in the context of the PoC, having an auditor to interpret requirements and metrics derived from those requirements ensures that the continuous evaluation is done following the intent of the written requirements. Additionally, understanding of the current auditing and certification processes is beneficial when the focus of the research is to change these processes.

5.1 Analysis of the PoC

Based on the analysis of the metrics and framework created in the Medina project, it is possible to implement continuous monitoring which fulfils the intent of the written requirements by using automated evidence collection and analysis. This provides high expectations for the future, and it is likely that we will see a change in how audits are conducted and how the certification is managed. However, the implementation of the metrics must be evaluated case-by-case as each environment and scope is different in each audit. Like in many cases, industry best practices and guidance of governing bodies will eventually steer the implementation continuous audit towards a standardized way. The rest of this section elaborates on the CAB's perspective for transitioning from continuous monitoring to continuous auditing.

5.2 Changing from point-in-time audits to continuous auditing

The current audit practice follows a project-type approach where the auditee's certification follows an audit cycle consisting of individual audits, typically annually. Depending on the used standard, the cycle is started after the initial certification audit and then followed by surveillance audits aimed to ensure that the auditee is still complying to the requirements. When the cycle ends, a recertification audit comparable to the initial audit is conducted to start a new cycle. The challenge in this approach has always been that the audit is always a representation of the auditee's current state during one point in time, but there are limited ways to ensure that the auditee is maintaining the same quality level between audits. It could be that the auditee is considering the certification more as an annual project rather than as continuous and integral part of daily work and is thus focusing majority of the effort just prior to the audits.

Continuous auditing offers great opportunities both the auditee and the auditor. While the auditee can increase their security awareness and enhance their security posture by implementing continuous monitoring and auditing capabilities, the auditor gets more assurance of the auditee's compliance throughout the certification cycle. Additionally, a CAB can extend their service offering with new services and improve audit effectiveness by implementing new innovations and technologies to the auditing process. It is important to notice that the implementation of automated tools does not necessarily reduce the workload of an auditor in an audit, but instead it offers more ways to verify findings in more complex and larger environments. If we look at the current trends in information technology, it is evident that cloud-based solutions have become the go-to solution for many organizations. Assessing these environments can be challenging and any automated tools to help gather and analyse vast amounts of information are welcomed.

5.3 Verifying results in continuous audits

The fundamental change in auditing naturally means that the audit process is changed. The traditional approach to auditing, simplified, is to review documentation, interview persons and

verify findings by conducting additional tests, such as process observations, sample reviews or technical tests. By utilizing continuous auditing, the verification of results can be done based on the results collected by automated tools.

Continuous auditing itself does not mean that the role of a certification body would be just to check measurement results and grant a certificate. While certain parts of requirements can be assessed automatically by using measurable metrics, it does not mean that assessing all requirements in compliance frameworks can be fully automated or that all results could be approved as such. For example, if a cloud service provider implements continuous monitoring capabilities to assess requirements, the auditor must go beyond the assessment results to approve them. In order to approve measurement results, at least the following must be ensured:

- The selected metrics are correct, suitable and meet the intent of the requirement
- The measurement is configured and implemented correctly
    - Measurement results are accurate and consistent
- The target asset is correct, and all required assets are monitored
- The measurement result integrity is ensured
    - There must be audit trail for the measurement to prevent alteration of results
    - Medina explores the leveraging of blockchain and other innovative solutions to ensure integrity and accountability.

The change of continuous auditing in the actual audit process is that the configuration check of the continuous monitoring tools will replace some of the manual evidence gathering. What this allows is that the sample sizes can be larger and expanded over longer periods of time. On the other hand, some manual work is still required. Automated tools can be used to verify that certain processes are documented in policies and implemented as required but the actual verification of these processes might require human input in terms of interviews or process observations. However, with good and standardized design of metrics this gap can be narrowed down significantly.

5.4 From Continuous Auditing to Continuous certification

Ideally, the continuous auditing should lead to continuous certification where the status of the certificate is automatically monitored and updated based on the assessment results. There could be multiple implementation methods for continuous certification varying from auditee implemented evidence storage solutions to sophisticated auditor-implemented SOC-type monitoring solutions. However, the approved solutions are to be chosen by the standard owners and industries since the automated certification will change the maintenance of certification. There are still some challenges to be solved such as:

- What are the criteria for certificate suspension?
- How are findings categorized as major and minor nonconformities automatically?
- Is certificate suspended automatically after a finding or after auditor's analysis?
- How is the certificate status logged throughout the cycle?

The optimal solution should be that all significant findings leading possibly to certificate suspension should be evaluated by the auditor, but the evidence of all nonconformities would be saved throughout the certification lifecycle. By this way the probability of false positive findings affecting certification is minimized.

6 Recommendations

Based on the performed experimentation, and the main activities in the scope of MEDINA, the consortium elaborated the following recommendations aimed to support stakeholders' adoption of the EUCS concept of automated/continuous monitoring for high assurance requirements.

Table 6. MEDINA Recommendations

Recommendation	Comments
Provide a clear *implementation* guidance about EUCS requirements where some degree of automated monitoring is needed.	Close examination of the "Continuous (Automated) Monitoring" definition in the core EUCS document opens questions related to aspects like frequency for gathering compliance data, reference to use for comparing gathered data, and so forth. More detailed/concrete implementation guidance is needed for CSPs aiming to achieve continuous monitoring. As needed, we even suggest referencing technologies like Cloud Security Posture Management systems, which can greatly support implementation of continuous monitoring.
Provide clear *audit/assessment* guidance related to EUCS requirements needing some degree of automated monitoring.	In analogy to the previous recommendation, we also suggest including concrete guidance for auditors working on continuous monitoring. Such guidance should tackle aspects like identification of deviations on the continuous monitoring systems, definition of operational effectiveness in the automated monitoring context, and so forth. Such guidance must also provide information about what CABs are expected to do with data coming from the CSPs' continuous monitoring systems. For example, to guide CABs (and CSPs) on actions to take with "compliance fluctuations" identified during the audit period.
Consider integrating a catalogue of metrics as part of the implementation guidance for EUCS.	The MEDINA team sees the need for a catalogue of metrics to be released as part of the implementation guidance related to continuous monitoring. Such catalogue will reduce the subjectivity of both CSPs and CABs while implementing/assessing a requirement related to continuous monitoring. For our team, the proposed Metrics Catalogue is seen as a necessary requirement for guiding CABs in assessing operational

	effectiveness, and understanding the definition of target values defined by CSPs. The lack of such catalogue might result in partial implementations/assessments of "complex" EUCS requirements like PM-04.7.
Consider focusing the EUCS requirements needing some sort of automated monitoring only on capabilities offered by cloud platforms, and not by external systems.	Our experimentation focused on EUCS requirements purely implemented on a cloud-based testbed, which proved challenging by itself. We recommend a first version of EUCS to focus mostly on such type of requirements, therefore eliminating dependencies/complexities of non-cloud systems.
Guidance on selecting tools/technologies for automated (continuous) monitoring	Stakeholders in EUCS, in particular CSPs and CABs, need further guidance on the tools/technologies implied as required for leveraging automated (continuous monitoring). Such tools/technologies can become a security risk by themselves if they cannot provide the required assurance to stakeholders e.g., if a tool has known vulnerabilities. Furthermore, it is necessary to discuss if the tool/technology itself must be also EUCS certified (if cloud-based), or should provide any other kind of assurance/certification. This might introduce additional complexities (e.g., compositional certification aspects) to the already challenging EUCS High.
Actively monitor the development of NIST OSCAL.	Despite a machine-readable language is not required by EUCS, we strongly recommend following up activities like NIST OSCAL which is already being leveraged by international organizations like ISO. Providing the EUCS catalogue in an standardized machine-readable format, will benefit automation and adoption by CSPs.

APPENDIX A. Catalogue of elicited MEDINA Metrics for EUCS (Draft)

Requirement ID	Metric Name	Metric Description	Scale
HR-03.5	Personnel with access rights granted without acknowledgement security policies	Check if exist employees with access rights granted without acknowledgement of security policies	{1;0}
HR-03.5	Automatic monitoring of acknowledgement of security policies	Check if there is a possibility to monitor the verification of acknowledgement of security policies automatically	{1;0}
HR-04.7	Automatic monitoring of security awareness and training programs completion	Check if exists a possibility to monitor the completion of the security awareness and training program automatically	{1;0}
HR-05.4	Internal employees with accesses granted after termination or change of employment	Check if exist internal employees with accesses granted after termination or change of employment, which should have been revoked according to the outcomes of the decision-making procedure	{1;0}
HR-05.4	External employees with accesses granted after termination or change of employment	Check if exist external employees with accesses granted after termination or change of employment, which should have been revoked according to the outcomes of the decision-making procedure	{1;0}
HR-05.4	Existance of a procedure for decision making on access rights after termination or change of employment	Check if exists an established procedure for decision-making about access rights of an employee after termination or change of employment	{1;0}
HR-05.4	Timely execution of decision making procedure about access rights after termination or change of employment	Check if the procedure for decision-making about access rights of an employee after termination or change of employment is performed before contract termination/change.	{1;0}
HR-05.4	Automatic revocation of rights on contract termination	Check if access rights are revoked on contract termination or change according to the decision making procedure automatically	{1;0}

Requirement ID	Metric Name	Metric Description	Scale
HR-06.7	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Automatic monitoring of confirmation of non-disclosure or confidentiality agreements	Check if exists a possibility of monitoring confirmation of non-disclosure or confidentiality automatically	{1;0}
PSS-04.3	VM and container images integrity checks	Are integrity checks performed at start-up of VM and container images?	{yes; no}
PSS-04.3	Automatic monitoring of VM and container images integrity checks	Are integrity checks of VM and container images automatically monitored?	{yes; no}
PSS-04.3	Reporting to CSCs about VM and container images integrity checks	Are the reports of VM and container images' integrity checks presented to the CSCs?	{yes; no}
CO-03.4	SWWhitelistEnabled	This metric is used to assess if the software whitelisting has been enabled on a cloud service / asset	[TRUE; FALSE]
CO-03.5	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
CS-04.5	HTTPSecurity	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPSOnly]

Requirement ID	Metric Name	Metric Description	Scale
CS-04.5	InternetFacingEnabled	This metric is used to assess if a cloud service/asset has enabled internet reachability	[TRUE; FALSE]
CS-04.5	IPSourceFilteringEnabled	This metric is used to assess if IP source filtering has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	SSLEnabled	This metric is used to assess if a cloud service/asset is using SSL	[TRUE; FALSE]
CS-04.5	MutualAuthnEnabled	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	NetworkFirewallEnabled	This metric is used to assess if a network-level firewall has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	JITAccessEnabled	This metric is used to assess if Just in time access (JIT) has been enabled on a cloud service / asset.	[TRUE; FALSE]
IAM-03.11	AuthNMechanism	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedIndentity, SSO]
IAM-03.12	AuthNMechanism	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedIndentity, SSO]
IAM-03.12	AnonAuthNForbiden	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[TRUE; FALSE]
IM-03.4	IncidentManagementEnabled	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
IM-03.4	IncidentRemediationUserApproval	This metric is used to assess if the automated incident remediation mechanism requires user approvals.	[TRUE; FALSE]
OIS-02.4	SecurityContactEnabled	This metric is used to assess if a security operator / security contact has been assigned on a cloud service/asset	[TRUE; FALSE]
OPS-02.3	ResourceProvisioningMonitorEnabled	This metric is used to assess if the CSP has enabled the automated monitoring of resources' provisioning and deprovisioning.	[TRUE; FALSE]
OPS-05.3	AntiMalwareEnabled	This metric is used to assess if the antimalware solution specified by the CSP on its security concept/operation manual has been enabled on a cloud service / asset.	[TRUE; FALSE]
OPS-05.4	AntiMalwareEnabled	This metric is used to assess if the antimalware solution specified by the CSP on its security concept/operation manual has been enabled on a cloud service / asset.	[TRUE; FALSE]
OPS-05.4	AntiMalwareResultsCompliant	This metric is used to assess if the antimalware solution reports no irregularities.	[TRUE; FALSE]
OPS-07.2	SelfServicePortalEnabled	This metric is used to assess if a self service portal for data backup monitoring is available.	[TRUE; FALSE]
OPS-07.3	BackupEnabled	This metric is used to assess if backups are enabled for a cloud service/asset	[TRUE; FALSE]
OPS-07.3	BackupRetention	This metric is used to assess the configured backup retention (days) on a cloud service/asset	[0; …; 99]
OPS-09.5	RemoteBackupLocation	This metric is used to assess the backup of a cloud service/asset is stored in a remote location	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
"OPS-12.4 "	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
"OPS-12.4 "	LoggingEnabled	This metric is used to assess if security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
"OPS-12.4 "	LogRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0; …; 99]
OPS-13.7	LoggingEnabled	This metric is used to assess if security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
OPS-13.7	LogRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0; …; 99]
OPS-18.6	AutomaticUpdatesEnabled	This metric is used to assess if automatic updates are enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	CryptoStorageEnabled	This metric is used to assess if cryptographic storage has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	HTTPSecurity	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPSOnly]
OPS-21.3	HTTPSVersion	This metric is used to assess the HTTP version used by the cloud service/asset	[1.0; 2.0]
OPS-21.3	JavaVersion	This metric is used to assess the Java Runtime version used by the cloud service/asset	[< 11; 11]

Requirement ID	Metric Name	Metric Description	Scale
OPS-21.3	LeastPriviledgeEnabled	This metric is used to assess if less priviledge access is enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	PHPVersion	This metric is used to assess the PHP version used by the cloud service/asset	[< 7.4; 7.4]
OPS-21.3	PythonVersion	This metric is used to assess the Python version used by the cloud service/asset	[< 3.8; 3.8]
OPS-21.3	SSLEnabled	This metric is used to assess if a cloud service/asset is using SSL	[TRUE; FALSE]
OPS-21.3	TlsVersion	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks.	[1.0; 1.1; 1.2; 1.3]
OPS-21.3	WAFEnabled	This metric is used to assess if a cloud service/asset has enabled WAF functionalities	[TRUE; FALSE]
OPS-21.3	MutualAuthnEnabled	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	ACLEnabled	This metric is used to assess if a service-level ACL has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	AnonAuthNForbiden	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[TRUE; FALSE]
OPS-21.3	SignedCommunicationEnabled	This metric is used to assess if the intra-cloud service / asset communication is digitally signed.	[TRUE; FALSE]
OPS-21.3	EncryptionAtRestEnabled	This metric is used to assess if encryption at rest has been enabled on a cloud service / asset	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
PM-04.7	OSLoggingEnabled	This metric is used to assess if OS-level security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
PM-04.8	IncidentManagementEnabled	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]
AM-01.6	Assets_discovery	This metric is used to assess if the inventory of assets is regularly monitored	[TRUE; FALSE]
AM-01.6	Assets_evaluation	This metric is used to assess if the inventory if assets are regularly monitored against policies	[TRUE; FALSE]
AM-03.6	Commisioning_requests_log	This metric is used to assess the existence of digital record of the commissioning requests including the approval or denial	[TRUE; FALSE]
AM-03.6	Decommisioning_requests_log	This metric is used to assess the existence of digital record of the decommissioning requests including the approval or denial	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_public	This metric is used to assess existence of a commissioning procedure which is public to internal and external employees	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_content_risks	This metric is used to assess the existence risk management procedures in the commisiong procedure	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_content_authorization	This metric is used to assess the existence of the information related to the verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies, before authorization to commission the asset can be granted	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
AM-04.4	Decommissioning_procedure_content_public	This metric is used to assess existence of a decommissioning procedure which is public to internal and external employees	[TRUE; FALSE]
AM-04.4	Decommissioning_procedure_content_content	This metric is used to assess the inclusion of the complete and permanent deletion of the data or the proper destruction of the media in the decommissioing procedure	[TRUE; FALSE]
PM-04.7	The percentage of compliance monitored	The percentage of monitored compliance of the third party with their regulatory and contractual obligations	[0;100]
PM-04.7	Automatic compliance monitored	The check that exists an automatic functionality to monitor compliance	{0;1}
PM-04.7	Automatic use of compliance results in other procedures	The check that the results of the monitoring automatically use in the listed procedures: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).	{0;1}
PM-04.8	List of violations and discrepancies	Check if exists a list of violations and discrepancies (can be a list of rules)	{0;1}
PM-04.8	Automatically detected violations and discrepancies	The percentage of violations and discrepancies which can be automatically detected	[0;100]
PM-04.8	Automatic reporting of detected violations	Check if there is a procedure for reporting to responsible personnel	{0;1}
CO-03.4	The percentage of internal audit requirements automatically monitored	In relation to M221: Check the percentage of implemented compliance monitors in scope.	[0;100]

Requirement ID	Metric Name	Metric Description	Scale
CO-03.4	Compliance status of internal audit requirements	In relation to M222: Check the compliance status of each compliance monitor in scope	[0;1]
CO-03.5	Asset_vulnerable	Check whether asset is vulnerable by checking if software version matches known vulnerable versions	[TRUE;FALSE]
CO-03.5	Asset_deviating	Check if asset is deviating to any requirement in place for that asset. All requirements must be complying to pass.	[TRUE;FALSE]
ISP-03.7	Monitor validity of security exceptions / approvals	Check if security approvals and exceptions are automatically monitored	[TRUE;FALSE]
ISP-03.7	Validity of security exceptions / approvals - up-to-date check	Check if security reviews and approvals are up-to-date	[TRUE;FALSE]
IM-03.4	Security Incident Solution Review - avaliability	(BSI-C5 / Sim-04) Check if customers have the ability to review security incident solutions.	[TRUE;FALSE]
IM-03.4	Security Incident Solution Review - up-to-date check	(BSI-C5 / Sim-04) Check if security incident solutions are up to date.	[TRUE;FALSE]
INQ-03.4	Investigation Monitoring	Monitor the data access performed by or on behalf of investigators.	[TRUE;FALSE]
PS-02.10	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging	>=0
PS-02.10	Access Audit Enabled	This metric is used to assess if access monitoring is enabled	[TRUE;FALSE]
OPS-06.2	EncryptedBackup	Check if data is backed up in encrypted, state-of-the-art form.	[TRUE;FALSE]
OPS-09.2	EncryptedBackupTransmission	Check if backup data is transmitted in state-of-the-art encrypted form.	[TRUE;FALSE]

Requirement ID	Metric Name	Metric Description	Scale
OPS-11.1	SecureDataHandling	Check if derived data is handled securely.	[TRUE;FALSE]
OPS-13.3	AuthenticatedCommunicationChannelForLogging	Check if communication to logging servers uses a authenticated communication channel.	[TRUE;FALSE]
OPS-13.3	ProtectedCommunicationChannelForLogging	Check if communication to logging servers is protected by integrity and confidentiality.	[TRUE;FALSE]
OPS-13.4	EncryptedCommunicationChannelForLogging	Check if communication to logging servers is encrypted using state-of-the-art encryption.	[TRUE;FALSE]
OPS-15.3	StrongAccessAuthenticationToLoggingAndMonitoring	Check if access to logging and monitoring uses strong authentication.	[TRUE;FALSE]
IAM-07.2	AuthenticatedAccess	Check if access is authenticated	[TRUE;FALSE]
IAM-08.4	StronglyHashedPassword	Check if passwords are stored using cryptographically strong hash functions	[TRUE;FALSE]
CS-05.4	StronglyEncryptedTunnel	Check if a strongly encrypted tunnel is used.	[TRUE;FALSE]
CO-03.5	SoftareRuleCompliant	Check if software adheres to security policy.	[TRUE;FALSE]
PSS-02.1	ProtectedSessionManagement	Check if session management software uses state-of-the-art encryption and session management	[TRUE;FALSE]
PSS-02.2	AutomaticSessionInvalidation	Check if session management software invalidates session after it has been detected invalid	[TRUE;FALSE]
PSS-02.3	ConfigurableSessionTimeout	Check if session management software invalidates session after a configurable timeout	[TRUE;FALSE]

Requirement ID	Metric Name	Metric Description	Scale
AM-04.4	Commitment_employee_to_policies	No. of alerts raised for employees without or outdated acknowledgment record	[0;100]?
IAM-03.11	Monitoring_AuthNMechanism	Monitoring for log events produced by automated mechanisms to check if they are working properly	[TRUE;FALSE]
IAM-03.12	Monitoring_number_AuthAttempts	Monitoring the number of log events produced by automated mechanisms advising for authentication attempts	[0;100]?
CCM-03.10	NumberofExecuted_Required_funcTests	Number of executed functional tests versus number of required functional tests	[0;1]
CCM-04.3	NumberofExecuted_Required_Changes	Number of changes executed versus number of changes approved in line with defined criteria	[0;1]
CCM-04.3	NumberofChangesExecuted_Required_ProdEnv	Number of changes in production environments executed by the designated roles versus all number of changes	[0;1]