MEDINA

EUROSCAL – Paving the Road Towards Automated Cybersecurity Certification in Europe

(Whitepaper)

Editor(s):	Jesus Luna Garcia
Responsible Partner:	Robert Bosch GmbH
Status-Version:	Final – v1.0
Date:	06.09.2023
Distribution level:	Public

Project Number:	952633
Project Title:	MEDINA

Editor(s):	Jesus Luna Garcia, Bosch
Contributor(s):	Thomas Ruebsamen, Bosch Valentin Acker, Bosch Levi Lübbe, Bosch
Reviewer(s):	Cristina Martinez Martinez, TECNALIA
Approved by:	All Partners
Recommended readers:	Cloud Service Providers, Auditors, Regulators

Keyword List:	EUCS, OSCAL, EUROSCAL, Automation, Interoperability
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	04.08.2023	First draft version	Bosch
v0.2	29.08.2023	Revised draft	Bosch
v0.3	06.09.2023	Full version	Bosch
v1.0	06.09.2023	Final revised version	Cristina Martinez

Table of contents

List of tables

List of figures

Terms and abbreviations

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Conformity Assessment Body
CSA or EU CSA	Coordination and Support Action
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management tools
DLT	Distributed Ledger Technologies
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
IaaS	Infrastructure As A Service
JSON	JavaScript Object Notation
ICT	Information and Communication Technology
NIST	National Institute for Standards and Technology
OSCAL	Open Security Controls Assessment Language
PaaS	Platform As A Service
R&D	Research and development
SaaS	Software as a Service
TOM	Technical and Organizational Measure
UUID	Universally Unique Identifier
XML	Extensible Markup Language
YAML	Yet Another Markup Language

Executive Summary

Despite the evident advantages automation could bring to traditional cloud cybersecurity certification processes, and in particular to underlying conformance assessments, there are still challenges associated to interoperability and standardization between all involved stakeholders. We refer not only to underlying implementations of relevant tools like the so-called Cloud Security Posture Management (CSPM), but also to the standardized representation of Infrastructure-as-Code cloud services (IaC), catalogues of security requirements, and the security configuration of cloud services to assess. These are necessary challenges to address before the notion of continuous (automated) monitoring of compliance can be fully realized e.g., in the new European Cybersecurity Certification Scheme for Cloud Service (EUCS). In this context, the present whitepaper introduces EUROSCAL, a MEDINA-driven initiative to promote the European use of NIST OSCAL (Open Security Controls Assessment Language) as a feasible solution for achieving interoperability and automating cloud security certification processes.

1 Introduction

In April 2019 the EU Cybersecurity Act (EU CSA) was published, which aims improving customers' trust in the European ICT market through a set of novel certification schemes. One of those schemes, the European Cybersecurity Certification Scheme for Cloud Service (EUCS[1]) is being developed by the European Union Agency for Cybersecurity (ENISA). EUCS focuses on the certification of cloud services and proposes three different levels of assurance (i.e., Basic, Substantial, and High) each with its own set of cybersecurity requirements, and conformance assessment rules. For example, EUCS for Basic assurance (codename CS-Basic) relies on self-assessments whereas CS-High introduces the notion of continuous (automated) monitoring for a subset of requirements.

The EUCS notion of continuous monitoring conveys important technological and organizational challenges for all involved stakeholders (e.g., Cloud Service Providers, Conformance Assessment Bodies, National Certification Authorities), which will influence the future development of tools and processes. Interoperability is one major challenge associated to the CS-High requirements where some level of automated compliance monitoring is needed. It is common to find native implementations of Cloud Security Posture Management tools (CSPM) offered by cloud service providers to their customers, commercialized by 3rd party vendors, or even offered as open source software (OSS). Unfortunately, it is also common to find that such tools are based on proprietary protocols/schemas/API which make almost impossible interoperability. In our opinion, this issue is partially responsible for the current lack of automation found in conformance assessment processes needed by certifications like EUCS. Given the complexity and scale of cloud computing ecosystems, standardized formats and specifications are urgently needed to fully realize the potential of automation in EUCS, and other relevant certification schemes.

In this whitepaper we discuss the experiences of the EU MEDINA project[2] on the topic of continuous (automated) monitoring in EUCS by leveraging NIST OSCAL (Open Security Controls Assessment Language[3]). OSCAL is a promising solution for achieving interoperability and enabling automation in EUCS and beyond. We also introduce EUROSCAL[4], a MEDINA-driven initiative for realizing the full potential of OSCAL not only in EUCS, but also in other EU-based certification schemes. Our goal is to positively influence relevant stakeholders, in particular Regulators, so automation of cybersecurity certification process can become a reality in the future thanks to OSCAL, EUCS, and MEDINA.

This whitepaper is based on the draft version of the European Cybersecurity Certification Scheme for Cloud Service (EUCS), published on December 22nd 2020, and available online at https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

The rest of this whitepaper is organized as follows: Section 2 introduces the basic notions related to both MEDINA and OSCAL, only to the extend required to present EUROSCAL in Section 3. Section 4 shows an illustrative example related to the use of OSCAL in the MEDINA/EUCS context. Finally, Section 5 summarizes our future plans with EUROSCAL.

[1] Draft version available at https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[2] Please refer to https://medina-project.eu/
[3] Please refer to https://pages.nist.gov/OSCAL/
[4] Please refer to https://euroscal.eu/

2 Background

2.1 EU-funded MEDINA Project

In an effort to solve some of the challenges related to the topic of trustworthiness in cloud services, 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 draft document 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.

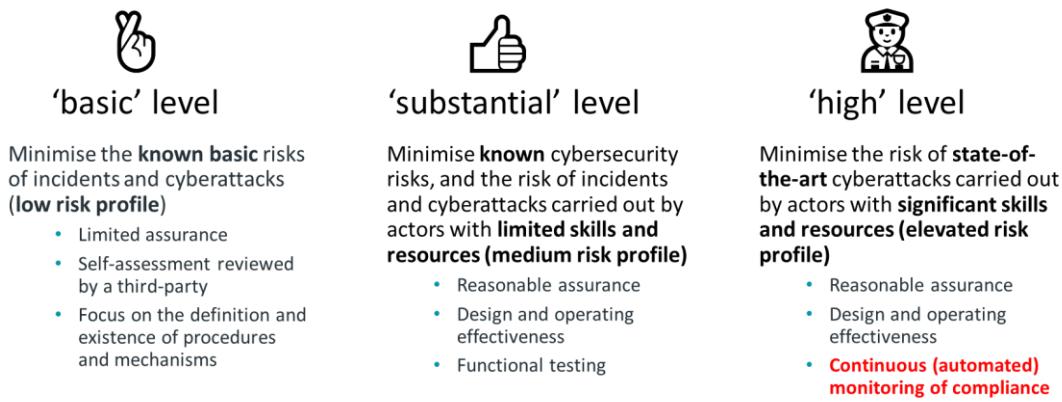

Figure 1. EUCS levels of assurance at a glance (adapted from ENISA)

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 main pillars from MEDINA, and their relevance for the uptake of EUCS' notion of continuous (automated) monitoring.

2.1.1 Compliance Metrics Catalogue

The current EUCS draft provides an organized set of security requirements, mostly based on international standards, which shall we leveraged to certify cloud services. A subset of such requirements mandates the implementation of continuous monitoring through automated means.

At the time of writing this report, EUCS does not define the concrete guidelines or "compliance metrics" which can be used to automatically assess those requirements. The lack of standard EUCS-metrics can become a problem for CSP and CABs, which might need to leverage their own custom metrics for implementing/assessing EUCS requirements in an automated manner. Such levels of heterogeneity might add further complexity to the underlying EUCS' certification process for high assurance.

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.

2.1.2 Risk-based approach for 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 and requirements shall address the concrete needs of a CSP, by also taking into consideration the targeted EUCS assurance level.

2.1.3 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 (Natural Language Processing). The expected outcome should comprise aspects like scope of the certification, assurance level and conformity assessment method.

2.1.4 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 evidence 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.

2.1.5 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 standardization bodies, 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.

2.2 OSCAL – Open Security Controls Assessment Language

As referred in the official website, "NIST is developing the Open Security Controls Assessment Language (OSCAL) as a standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls"[5].

OSCAL aims to provide a homogeneous manner of representing security controls and control baselines (like those in EUCS), which nowadays are represented in proprietary formats which require data conversion and manual effort to describe their implementation. OSCAL seeks to enable security professionals the creation of a standardized set of machine-readable formats to improve the automation of processes like security assessments, auditing, and continuous compliance monitoring.

In order to achieve its goals, OSCAL proposes a *stack of layers* to provide structured information all over the model (e.g., communicating the set of Controls to be implemented and assessed). Each layer is composed of one or more *models*, each one containing a data structure fulfilling a specific purpose (e.g., representing the EUCS catalogue of requirements). In this layered model, the lower OSCAL layers provide information to the upper ones. At the time of writing, the OSCAL specification[6] contains the following layers and models:

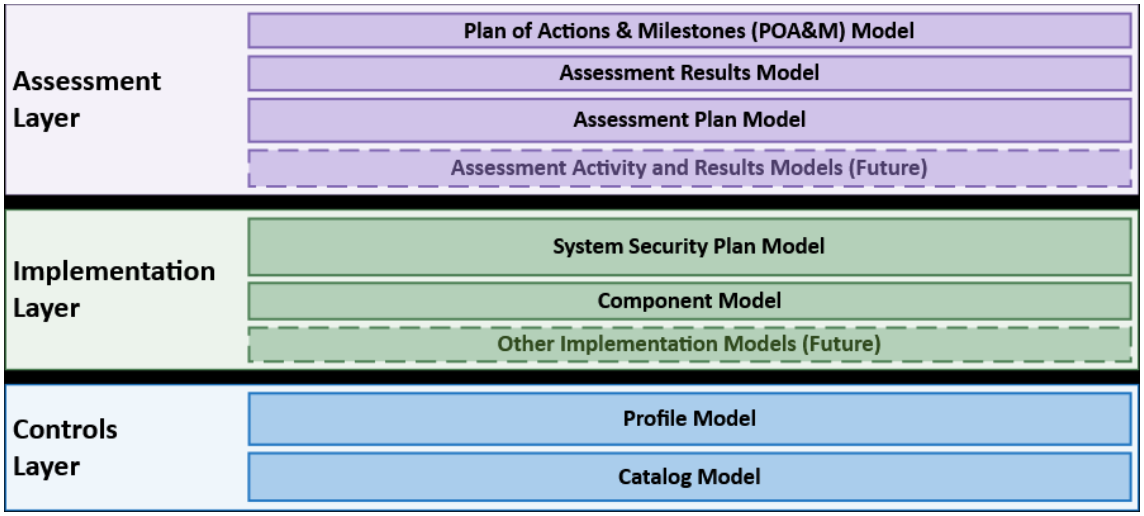

Figure 2. Layers and Models in OSCAL

At a glance, the goals of each represented layer and model are shown in the table below.

Table 1. OSCAL's Layers and Models at a glance

Layer	Explanation
Controls Layer	Provides information about Catalogues of controls and any applicable Profile specification. It is comprised of the following models: • Catalog model: represents an organized set of controls e.g., EUCS. • Profile model: used for selecting, organizing and tailoring a specific set of controls e.g., extension profiles in EUCS.
Implementation Layer	This layer focuses on representing the implementation of a system under

[5] Please refer to https://pages.nist.gov/OSCAL/about/
[6] Please refer to https://pages.nist.gov/OSCAL/concepts/layer/

	a specific Control baseline, as well as the individual component[7] that may be integrated into a system. This layer provides the following models: • System Security Plan (SSP) model: expresses the security implementation/configuration of the actual component. It usually comprises the actual Controls (see Control layer) being implemented by the component. • Component Definition model: defines information about the individual component itself, and it is intended to be imported into the SSP.
Assessment Layer	As implied from its name, the Assessment layer supports the actual conformance assessment / continuous compliance process by documenting all findings and the corresponding supporting evidence. Furthermore, this layer also supports documenting the identification and management of remediation tasks along with the corresponding risks. The models comprising this layer are the following: • Assessment Plan model: provides a machine-readable format for describing information about the assessment process e.g., when the system will be assessed, scope of the assessments, and conformance assessment activities to be performed. • Assessment Result model: represent information produced by the assessment activities. This includes the results / findings from the assessments along with the gathered evidence. As we will see later, this model is essential for enabling the notion of continuous certification in MEDINA. • Plan of Action and Milestones (POA&M) model: summarizes the assessment findings which need to be addressed by the corresponding system owners.

At the time of writing, the current OSCAL release provides the corresponding references and schemas (XML, JSON and YAML) for all presented layers and models.

[7] In OSCAL, a "component" can be considered an EUCS "cloud service".

3 EUROSCAL – The EU Friends of OSCAL

In the EU-funded MEDINA project we identified that the notion of continuous audit-based certification (in particular for EUCS) strongly relied in two major topics: automation and compliance metrics. Both topics are strongly related, because a machine-readable representation of relevant EUCS metrics is needed to enable the automation of underlying continuous compliance monitoring processes. Furthermore, our research also shown that the solution for tackling those topics should not only focus on the technical challenges, but also on non-technical aspects like standardization, and influencing relevant stakeholders to motivate acceptance of automation.

The proposal of MEDINA for achieving this goal relies on the creation of an open/community-driven initiative known as EUROSCAL[8] – The EU Friends of OSCAL, where relevant European stakeholders will collaborate on a voluntary manner to exchange ideas and trigger spin-off activities towards adopting OSCAL. EUROSCAL is expected to become a central hub for learning the basics of OSCAL, and also to allow relevant stakeholders (including Regulators) realizing the potential of OSCAL for providing automation to cloud cybersecurity certification processes (in particular EUCS and other national schemes from Member States). Automation through interoperability and standardization will pave the road towards developing more efficient, objective, and trustworthy certification processes.

The rest of this section is devoted to introducing EUROSCAL in the context of MEDINA.

3.1 Tackling the Continuous Compliance Monitoring Challenges

Challenges addressed by OSCAL comprehend important topics which are also essential for the uptake of the MEDINA framework. We refer to the following:

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

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

where automated assessments need to rely on machine-readable schemas which can interoperate between the different components of the contributed framework.

Previously listed challenges are not specific to MEDINA, but we foresee them as critical for providing automation to cybersecurity certification/EUCS processes in the near future. In this context, OSCAL plays a central role by pursuing automation thanks to interoperable and standardized machine-readable formats. Not only OSCAL enables reduction of manual processes, but it also aims to improve the way system security assessments are performed, while paving the road towards "true" continuous certification. A short discussion on OSCAL usage scenarios explored in MEDINA can be found in Section 4.

3.2 The EUROSCAL Manifesto

In its efforts to maximize the use of automation in (EUCS) cybersecurity certification processes, MEDINA proposed the creation of the EUROSCAL initiative. Beyond promoting the usage of the developed MEDINA framework, EUROSCAL seeks to gather interested EU-based stakeholders playing a role in the cybersecurity certification community. In this context we include cloud service providers (wiling to get an EUCS certification), conformance assessment bodies (CABs, EUCS certifiers), regulators (e.g., National Cybersecurity Certification Authority), and developers (providing OSCAL-aware tools and services). These stakeholders shape our EUROSCAL community.

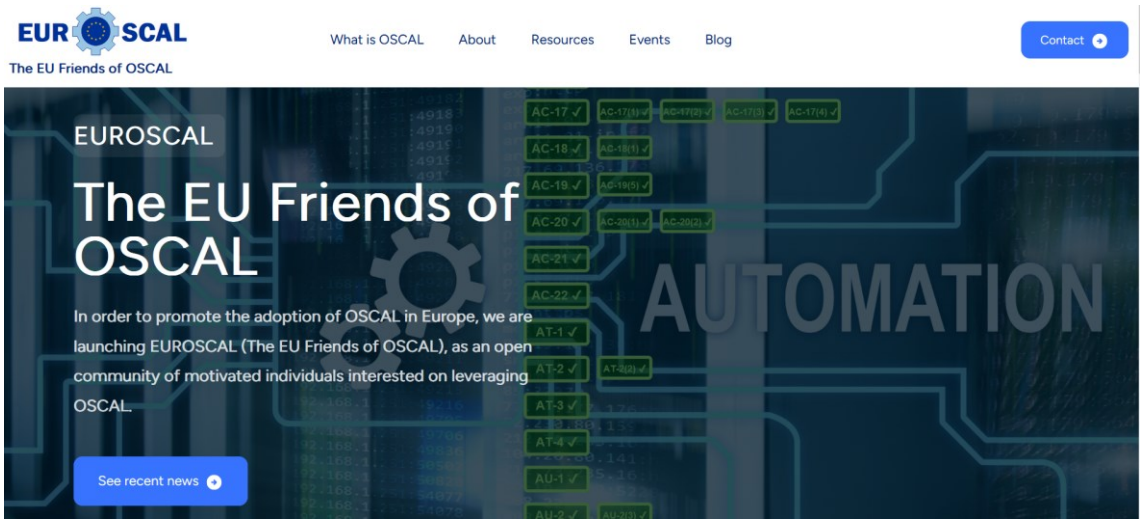

Figure 3. EUROSCAL landing page at www.euroscal.eu

EUROSCAL is expected to be community-driven, and although it can be sustained with the effort of upcoming EU-funded research projects, it is our belief that we will gather enough "critical mass" for making it a self-sustainable initiative. Furthermore, with the support of the already existing NIST OSCAL community, we also aim to establish international collaboration on this respect.

In a nutshell, the goals being pursued by EUROSCAL (our "Manifesto") are:

1. *Create a community of EU-based stakeholders interested in OSCAL.*
2. *Support the standardization of OSCAL in Europe.*
3. *Foster discussions aimed to leverage OSCAL in innovative EU-based tools, services, and initiatives.*
4. *Empower EU-cybersecurity certification processes with OSCAL-based automation.*

At the time of writing the most relevant activities being discussed in the context of EUROSCAL include (i) continuous support to the standardization activities being led by ETSI CYBER[9] (ETSI, Bosch), (ii) support to the representation of the BSI C5[10] catalogue of controls in OSCAL format (PwC, BSI, Bosch), and (iii) support leveraging OSCAL in the context of EUCS (ENISA EUCS Ad Hoc Working Group). These and other relevant topics are expected to continue developing even after the MEDINA project comes to an end.

[9] Please refer to https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/03.01.01_60/tr_10330504v030101p.pdf

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

4 OSCAL and MEDINA – Example

This section presents a usage example where OSCAL was investigated in the context of MEDINA for providing automation to EUCS certification processes. The presented scenario was developed during the execution of the H2020 MEDINA project and more information can be found on the respective website (www.medina-project.eu).

4.1 Overview

In the context of the cybersecurity certification schemes proposed by the EU Cybersecurity Act (EUCSA), ENISA (EU Agency for Cybersecurity) created the AdHoc Working Group (AHWG) to prepare the candidate scheme for cloud services (EUCS – EU Cybersecurity Certification Scheme for Cloud Services). EUCS introduces the notion of continuous (automated) monitoring for checking compliance with some of the proposed cybersecurity requirements (in particular a subset from EUCS's high assurance baseline). Acknowledging the technical and organizational challenges associated with the notion of "EUCS-continuous", the EU-funded MEDINA project proposed a framework to achieve automated audit-based certification aligned to the underlying EUCS principles. As part of the proposed framework, MEDINA investigated the usage of OSCAL for automatizing different processes related to EUCS, in particular those seen in Figure 4.

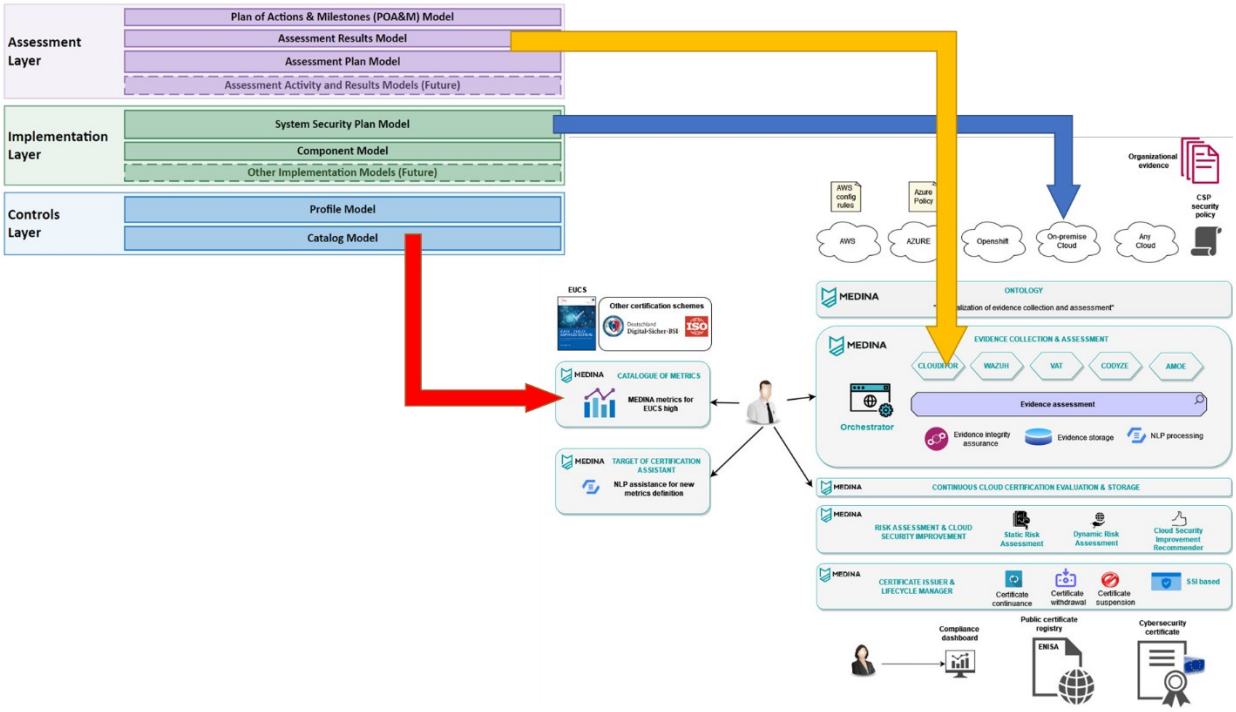

Figure 4. Leveraging OSCAL in the MEDINA framework

A usage scenario related to the Controls Layer was investigated during the lifetime of the MEDINA project, whereas leveraging the Implementation Layer and the Assessment Layer[11] is still work-in-progress[12]. The main findings related to the investigated scenario are presented in the rest of this section.

[11] Preliminary discussion on this usage scenario can be found here https://medina-project.eu/wp-content/uploads/2023/05/Bachelorarbeit_mit_EU_Nachweis.pdf (only in German)

[12] The current MEDINA framework supports provider-specific formats for representing different security configurations. More information can be found under www.medina-project.eu

4.2 OSCAL Format for the Draft[13] European Cybersecurity Scheme for Cloud Services (EUCS)

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

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

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

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

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

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

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

            }
          ],
```

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

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

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

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

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

```
"parts": [
                {
                  "id":"ops_02_obj",
                  "name":"control-objective",
                  "prose": "The capacities of critical resources such as personnel and IT
resources are monitored."
                },
                {
                  "id":"ops-02_smt",
                  "name":"statement",
                  "parts": [
                    {
                      "id":"ops-02_smt.3",
                      "name":"item",
                      "properties": [
                        {
                          "name":"label",
                          "value":"OPS-02.3"
                        }
                      ],
                      "prose": "The provisioning and de-provisioning of cloud services shall be
automatically monitored to guarantee fulfilment of OPS-02.1"

                    }
                  ]
                }
              ]
            },
```

The above presented mapping from EUCS to OSCAL's Catalog Model is summarized in the following table:

Table 2. Mapping EUCS to OSCAL's Catalog Model

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

5 The Way Forward

Undoubtedly, the synergies between the MEDINA project, EUCS and EUROSCAL are evident. Furthermore, EUROSCAL can potentially support the notion of a standardized and interoperable automation for (EUCS) cybersecurity certification processes thanks to the use of OSCAL. Automation in this field can sound like a utopia, however MEDINA has shown not only that it is technologically feasible, but also its advantages for all relevant stakeholders.

We acknowledge the fact that automation of conformance assessment processes is challenging to achieve nowadays, but it is our belief that EUROSCAL can contribute to reaching this goal in the future by relying on a community-driven approach.

By departing from the MEDINA framework, and the notion of continuous (automated) monitoring in EUCS, we aim to put together a network of experts and Regulators to work together towards achieving EUROSCAL's manifesto.

Even after the finalization of MEDINA, EUROSCAL will continue to be sustained thanks to other related EU-funded projects like Horizon Europe's COBALT and EMERALD. Further engagement activities and specific roadmaps will be created along with the EUROSCAL community in the following months.