Deliverable D7.10

Training materials

Editor(s):	Magdalena Harseva (HPE)
Responsible Partner:	Hewlett Packard Italiana, SRL
Status-Version:	Final – v1.1
Date:	19.01.2024
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	Training materials
Due Date of Delivery to the EC	31.10.2023

Workpackage responsible for the Deliverable:	WP7 - Awareness, Training, and Sustainability
Editor(s):	Magdalena Harseva (HPE)
Contributor(s):	Cristina Martínez (TECNALIA) Artsiom Yautsiukhin (CNR) Jesus Luna García (Bosch)
Reviewer(s):	Hrvoje Ratkajec (XLAB) Cristina Martínez (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	All Partners

Abstract:	This deliverable compiles the different training materials generated in the course of the project.
Keyword List:	Training
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	02.10.2023	First draft version	Magdalena Harseva (HPE)
v0.2	20.10.2023	Final draft version	Magdalena Harseva (HPE)
v0.3	24.10.2023	Comments and corrections	Cristina Martínez (TECNALIA), Hrvoje Ratkajec (XLAB)
v0.4	30.10.2023	Comments addressed	Hrvoje Ratkajec (XLAB)
v1.0	15.11.2023	Ready for submission	Cristina Martínez (TECNALIA)
v1.1	19.01.2024	Revised based on feedback from reviewers	Cristina Martínez (TECNALIA)

Table of Contents

List of Tables

List of Figures

Terms and Abbreviations

AMOE	Assessment and Management of Organizational Evidence
API	Application Programming Interface
CCD	Company Compliance Dashboard
CCE	Continuous Certification Evaluation
CSP	Cloud Service Provider
EC	European Commission
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
GUI	Graphical User Interface
KPI	Key Performance Indicator
LCM	Life-Cycle Manager
HTML	Hypertext Mark-up Language
RAOF	Risk Assessment and Optimisation Framework
REST	Representational State Transfer
SATRA	Self-Assessment Tool for Risk Analysis
ToE	Target of Evaluation
ToC	Target of Certification
WF	Workflow
WP	Work package

Executive Summary

This deliverable presents the different training activities carried out during the MEDINA project lifecycle and compiles the materials for these activities produced during the project.

The consortium has participated in several events, such as lectures and seminars, in various universities and schools to create awareness and competence on the hot specific topic of continuous compliance/certification. MEDINA project partners have been involved in training events which are showed in Table 1 "List of MEDINA training activities". Specific training and awareness materials have been produced to disseminate the project results to a wider audience.

To promote the MEDINA integrated solution as an open-source environment, 4 sets of training videos have been created. This strategic choice was justified by the need to speed up the awareness of the MEDINA action and to promote a quick and wide adoption of the MEDINA results to increase their usability.

The dissemination and awareness outputs of the project's training activities are described in more detail in this deliverable.

1 Introduction

The initial objectives for the activities related to D7.10 were to address the future adoption and ensure the sustainability of the project results, considering the market trends, the business scenarios and the needs and strategies of the consortium and partners. This deliverable summarizes and gives up-to-date information about how the MEDINA partners collaborated and contributed to achieving the defined goals, as well as the materials they used.

1.1 About this deliverable

This deliverable will compile the different training activities generated during the project. We list and describe the results achieved throughout the life of the project, considering the defined KPIs and highlighting any deviations from what was originally planned.

1.2 Document Structure

This document is structured as follows:

- Section 1 gives a general introduction, scope, and structure of the deliverable.
- Section 2 summarises the main training activities carried out in the project.
- Section 3 describes in detail the training materials that were created during the project.
- Section 4 concludes the deliverable.

2 MEDINA Training Activities

During the project, the consortium conducted training activities in the technical area covered by the project to create awareness and competence on the hot specific topic of continuous compliance/certification. As indicated in the MEDINA Dissemination and Communication Strategy [1], the project partners planned to participate in at least 2 training courses and to provide 2 online courses on the topics related to the project. In this regard, partners put some of the project suitable results into a format of training videos, so that others could benefit from it and get aware about MEDINA project and its achievements.

2.1 Training Events

The consortium participated in several events where the goals and results of the MEDINA project were promoted, as reported in D7.4 [2] and D7.5 [3]. Table 1 shows the list of these training activities. The description of each activity is included in Section 3.1.

Table 1. List of MEDINA training activities

#	Event	Date	Name and type of audience	Countries addressed	Size of audience	Partner
1	Talk "More than just a Risk Management" CyberSecurity Day 2023, Pisa, Italy	6 Oct, 2023	Academia/Industry /Secondary Schools	Italy	100	Artsiom Yautsiukhin (CNR)
2	Lecture "Valutazione e mitigazione del rischio di sicurezza cyber" (ENG: "Cyber Security Risk Assessment and Mitigation")". Cyber Security master in the University of Pisa.	31 Mar, 2023	Academia	Italy	60-70	Artsiom Yautsiukhin (CNR)
3	Lecture "MEDINA: Automation-based certification for cloud services in Europe". Barcelona Tech's MSc Programme in Cybersecurity.	12 Apr, 2023	Academia, Industry	Spain	30	Jesus Luna Garcia (Bosch)
4	Lecture "MEDINA – Paving the road towards continuous audit-based certification for cloud services in Europe", NECS PhD Winter School.	6 Feb, 2023	Academia, Researchers	EU	50	Jesus Luna Garcia (Bosch)
5	Seminar "Intelligent AI Security". TU Darmstadt (Germany).	14 Dec, 2022	Academia, Industry	US, Singapore, EU	30	Jesus Luna Garcia (Bosch)

#	Event	Date	Name and type of audience	Countries addressed	Size of audience	Partner
6	TAS-S Seminar "From Continuous Monitoring to Continuous Cloud Cybersecurity Certification". Lancaster University (UK).	4 Feb, 2022	University seminar	UK, EU	30	Jesus Luna Garcia (Bosch)
7	Lecture "Cyber insurance". NeCS winter school.	18 Jan, 2022	Academia, Researchers	EU Online	25	Artsiom Yautsiuk hin (CNR)
8	Talk "Lo strumento di analisi e riduzione dei rischi" (ENG: The tool for risk analysis and reduction). CyberSecurity Day 2021	8 Oct, 2021	Academia, Researchers	IT	100	Artsiom Yautsiuk hin (CNR)
9	Webinar "Cybersecurity in automotive industry". Slovenian Chamber of Commerce members.	21 Sep, 2021	ICT Sector	SLO	50	Aleš Černivec (XLAB)

2.2 Training Videos

MEDINA has created four sets of training videos, specific for the relevant user roles defined in D5.5 [4]:

- Training videos for the user role "Auditor"
- Training videos for the user role "Cybersecurity Governance"
- Training videos for the user role "Product Security Engineer"
- Training videos for the user role "Developer/Integrator"

These training videos are accessible through the MEDINA website[1] (see Figure 1). Each set comprises training videos that have been recorded by the MEDINA partners and which have been uploaded to the MEDINA YouTube channel[2]. The videos have been categorized in four playlists, one for each set (see Figure 2). Table 2 shows the full list of videos for each playlist.

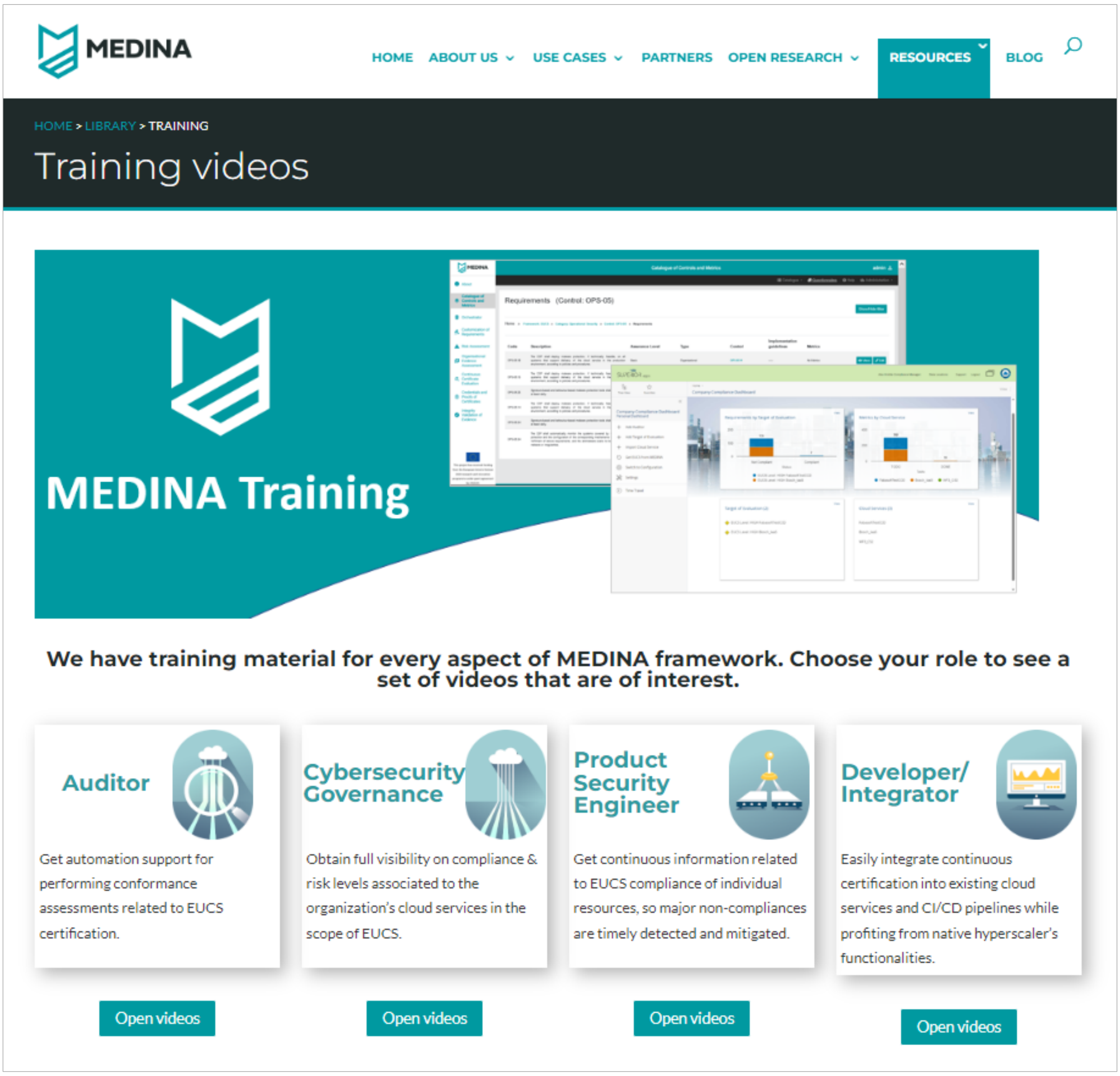
Each playlist starts with the promotional video of the MEDINA Project, which gives an overview of the project, followed by an explanation of the MEDINA Framework and a demonstrator of the MEDINA Integrated UI. Next, depending on the set of training videos, we have included a video describing an associated use case.

Technical videos follow, which have been recorded for each component or group of related components, as represented in the MEDINA framework architecture described in D5.5 [4]. Each video includes a few slides explaining the main objective and functionality of the component, as

[1] Please refer to: https://medina-project.eu/training-videos/

[2] Please refer to: https://www.youtube.com/@MedinaprojectEU

well as a demonstrator of this functionality. To guide the design and recording of the videos, the partner TECNALIA has provided both a template and detailed guidelines, which have been followed in the recording of all videos. *APPENDIX B: Material for the preparation of the training videos* includes the presentations used for the recording of each video.



HOME > LIBRARY > TRAINING

Training videos

We have training material for every aspect of MEDINA framework. Choose your role to see a set of videos that are of interest.

Auditor

Get automation support for performing conformance assessments related to EUCS certification.

Open videos

Cybersecurity Governance

Obtain full visibility on compliance & risk levels associated to the organization's cloud services in the scope of EUCS.

Open videos

Product Security Engineer

Get continuous information related to EUCS compliance of individual resources, so major non-compliances are timely detected and mitigated.

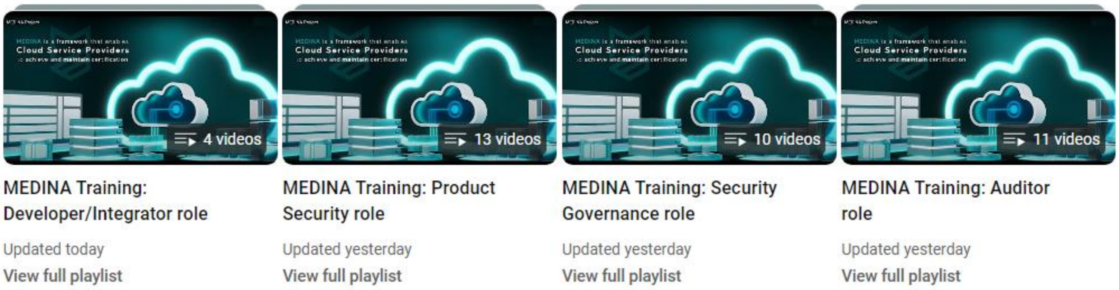
Open videos

Developer/ Integrator

Easily integrate continuous certification into existing cloud services and CI/CD pipelines while profiting from native hyperscaler's functionalities.

Open videos

Figure 1. "Training" page on the MEDINA website



MEDINA Training: Developer/Integrator role
Updated today
View full playlist

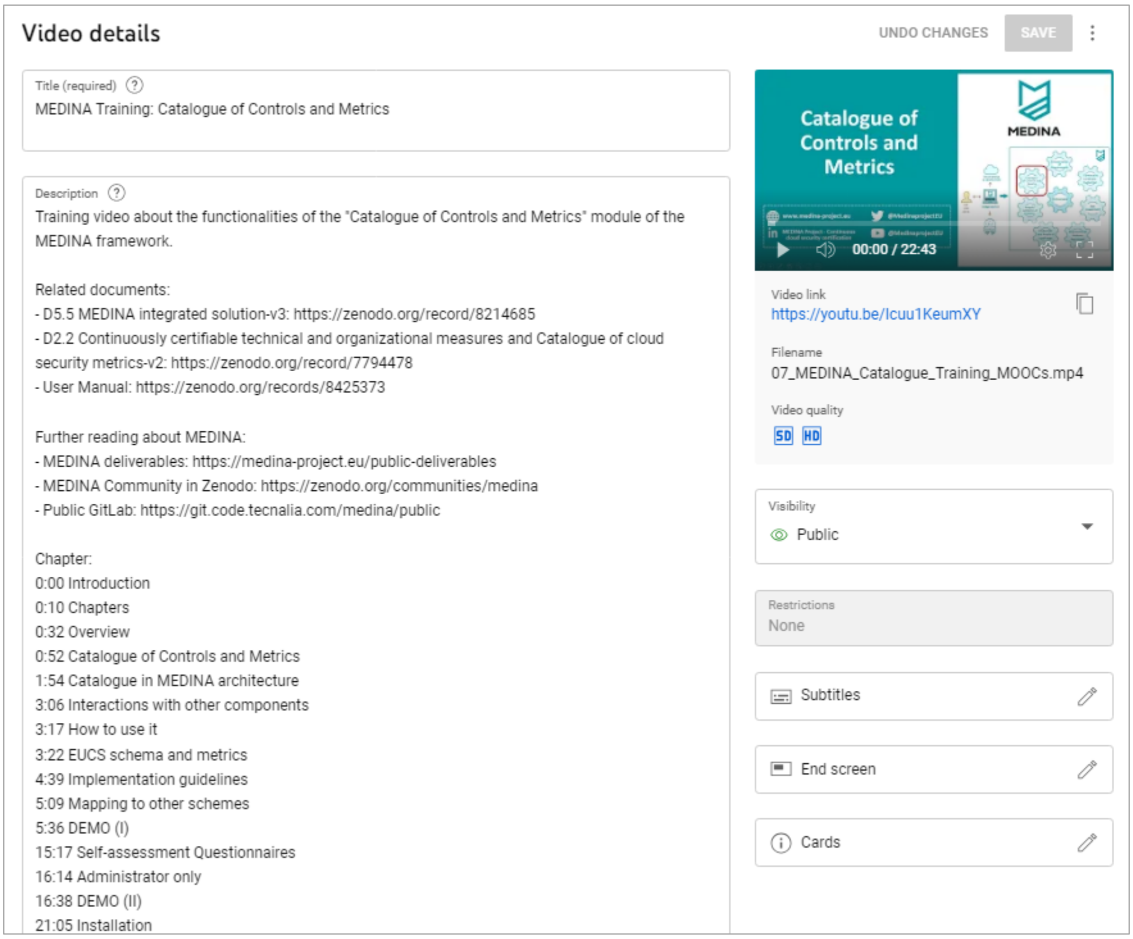
MEDINA Training: Product Security role
Updated yesterday
View full playlist

MEDINA Training: Security Governance role
Updated yesterday
View full playlist

MEDINA Training: Auditor role
Updated yesterday
View full playlist

Figure 2. Playlists of the training videos in the MEDINA YouTube channel

The description of the videos in YouTube has been enriched by adding useful links to the MEDINA deliverables, user manuals, and public repositories in Gitlab and Zenodo (see Figure 3). In addition, we have included chapter markers which allow a chapter navigation when watching videos.



Video details

UNDO CHANGES SAVE

Title (required)
MEDINA Training: Catalogue of Controls and Metrics

Description
Training video about the functionalities of the "Catalogue of Controls and Metrics" module of the MEDINA framework.

Related documents:
- D5.5 MEDINA integrated solution-v3: https://zenodo.org/record/8214685
- D2.2 Continuously certifiable technical and organizational measures and Catalogue of cloud security metrics-v2: https://zenodo.org/record/7794478
- User Manual: https://zenodo.org/records/8425373

Further reading about MEDINA:
- MEDINA deliverables: https://medina-project.eu/public-deliverables
- MEDINA Community in Zenodo: https://zenodo.org/communities/medina
- Public GitLab: https://git.code.tecnalia.com/medina/public

Chapter:
0:00 Introduction
0:10 Chapters
0:32 Overview
0:52 Catalogue of Controls and Metrics
1:54 Catalogue in MEDINA architecture
3:06 Interactions with other components
3:17 How to use it
3:22 EUCS schema and metrics
4:39 Implementation guidelines
5:09 Mapping to other schemes
5:36 DEMO (I)
15:17 Self-assessment Questionnaires
16:14 Administrator only
16:38 DEMO (II)
21:05 Installation

Video link
https://youtu.be/Icuu1KeumXY

Filename
07_MEDINA_Catalogue_Training_MOOCs.mp4

Video quality
SD HD

Visibility
Public

Restrictions
None

Subtitles

End screen

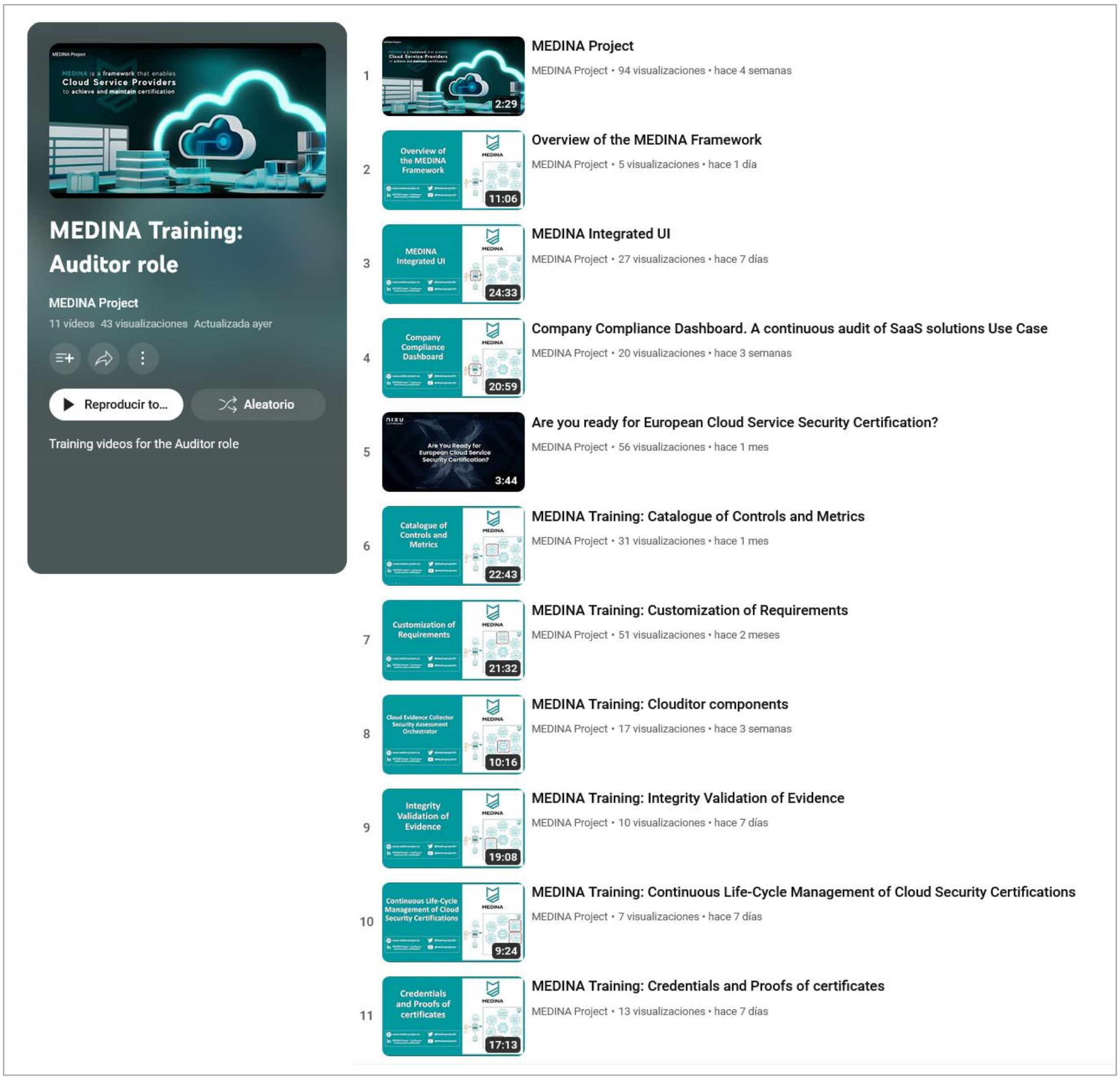
Cards

Figure 3. Enriched description for a training video in YouTube

2.2.1 Training videos for the user role Auditor

The auditor role in MEDINA is a Conformity Assessment Body (CAB) that performs conformity assessment services with the goal of demonstrating that specified requirements are fulfilled.

The set of training videos designed for the auditor user role comprises 11 videos, as shown in Figure 4, and is available at this link: MEDINA Training: Auditor role - YouTube. Section 3.2 includes the description of these videos.



MEDINA Training: Auditor role

MEDINA Project

11 vídeos 43 visualizaciones Actualizada ayer

Reproducir to... Aleatorio

Training videos for the Auditor role

1 MEDINA Project — 2:29
MEDINA Project • 94 visualizaciones • hace 4 semanas

2 Overview of the MEDINA Framework — 11:06
MEDINA Project • 5 visualizaciones • hace 1 día

3 MEDINA Integrated UI — 24:33
MEDINA Project • 27 visualizaciones • hace 7 días

4 Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case — 20:59
MEDINA Project • 20 visualizaciones • hace 3 semanas

5 Are you ready for European Cloud Service Security Certification? — 3:44
MEDINA Project • 56 visualizaciones • hace 1 mes

6 MEDINA Training: Catalogue of Controls and Metrics — 22:43
MEDINA Project • 31 visualizaciones • hace 1 mes

7 MEDINA Training: Customization of Requirements — 21:32
MEDINA Project • 51 visualizaciones • hace 2 meses

8 MEDINA Training: Clouditor components — 10:16
MEDINA Project • 17 visualizaciones • hace 3 semanas

9 MEDINA Training: Integrity Validation of Evidence — 19:08
MEDINA Project • 10 visualizaciones • hace 7 días

10 MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications — 9:24
MEDINA Project • 7 visualizaciones • hace 7 días

11 MEDINA Training: Credentials and Proofs of certificates — 17:13
MEDINA Project • 13 visualizaciones • hace 7 días

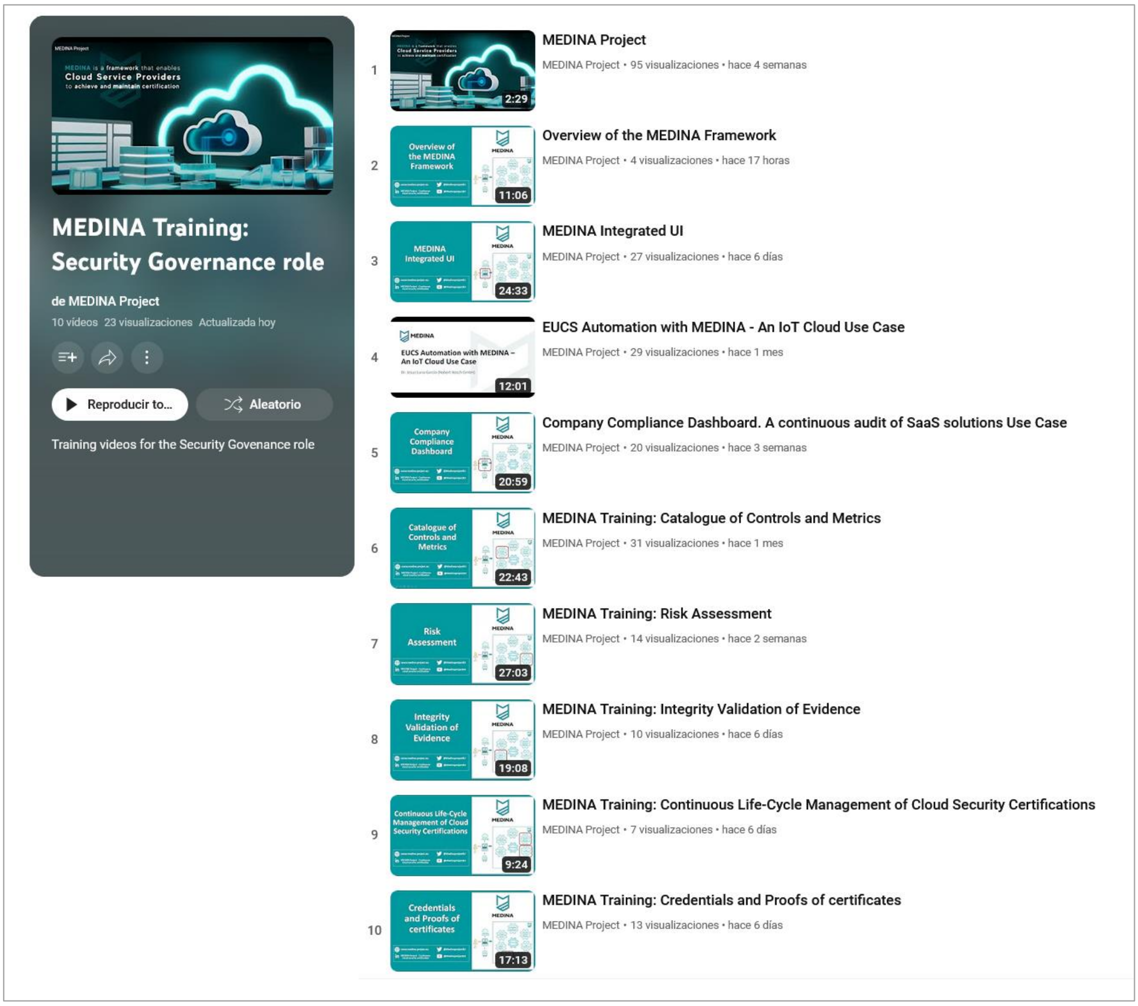
MEDINA is a framework that enables Cloud Service Providers to achieve and maintain certification
Overview of the MEDINA Framework
MEDINA Integrated UI
Company Compliance Dashboard
Are You Ready for European Cloud Service Security Certification?
Catalogue of Controls and Metrics
Customization of Requirements
Cloud Evidence Collector Security Assessment Orchestrator
Integrity Validation of Evidence
Continuous Life-Cycle Management of Cloud Security Certifications
Credentials and Proofs of certificates

Figure 4. Training videos for the "Auditor" role

2.2.2 Training videos for the user role Cybersecurity Governance

The Cybersecurity Governance role in MEDINA has as main objective the protection of the company's business models, products, services, and data.

The set of training videos designed for the Cybersecurity Governance user role comprises 10 videos, as shown in Figure 5, and is available at this link: MEDINA Training: Security Governance role - YouTube. Section 3.2 includes the description of these videos.



MEDINA Training: Security Governance role

de MEDINA Project

10 videos 23 visualizaciones Actualizada hoy

Reproducir to... Aleatorio

Training videos for the Security Govenance role

1 MEDINA Project
MEDINA Project • 95 visualizaciones • hace 4 semanas
2:29

2 Overview of the MEDINA Framework
MEDINA Project • 4 visualizaciones • hace 17 horas
11:06

3 MEDINA Integrated UI
MEDINA Project • 27 visualizaciones • hace 6 días
24:33

4 EUCS Automation with MEDINA - An IoT Cloud Use Case
MEDINA Project • 29 visualizaciones • hace 1 mes
12:01

5 Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case
MEDINA Project • 20 visualizaciones • hace 3 semanas
20:59

6 MEDINA Training: Catalogue of Controls and Metrics
MEDINA Project • 31 visualizaciones • hace 1 mes
22:43

7 MEDINA Training: Risk Assessment
MEDINA Project • 14 visualizaciones • hace 2 semanas
27:03

8 MEDINA Training: Integrity Validation of Evidence
MEDINA Project • 10 visualizaciones • hace 6 días
19:08

9 MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications
MEDINA Project • 7 visualizaciones • hace 6 días
9:24

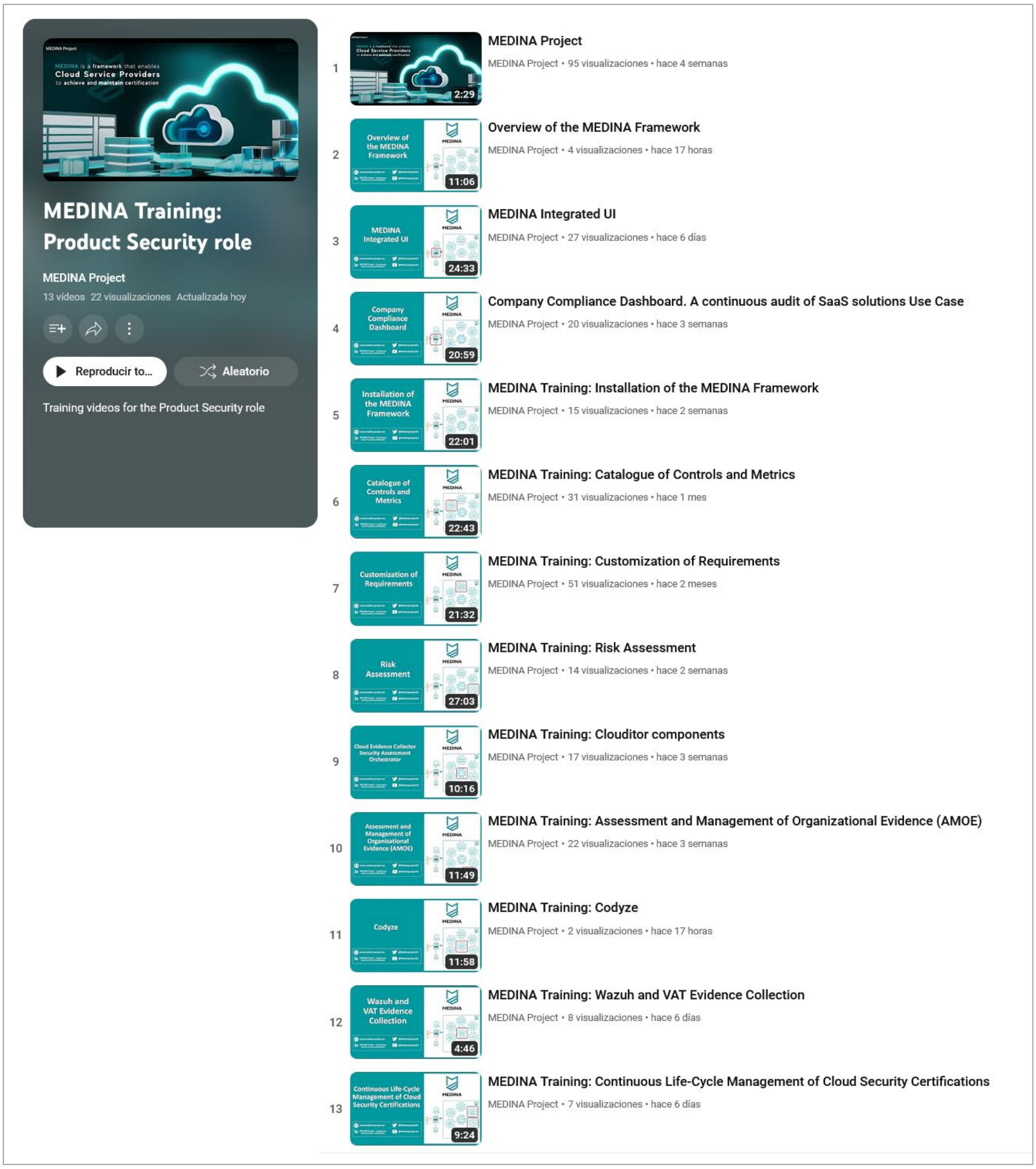
10 MEDINA Training: Credentials and Proofs of certificates
MEDINA Project • 13 visualizaciones • hace 6 días
17:13

Figure 5. Training videos for the "Security Governance" role

2.2.3 Training videos for the user role Product Security Engineer

The Product Security Engineer role in MEDINA oversees the build, deploy, and run of a product and its system components.

The set of training videos designed for the Product Security Engineer user role comprises 13 videos, as shown in Figure 6, and is available at this link: MEDINA Training: Product Security role - YouTube. Section 3.2 includes the description of these videos.



MEDINA Training: Product Security role

MEDINA Project

13 vídeos 22 visualizaciones Actualizada hoy

Reproducir to... Aleatorio

Training videos for the Product Security role

1	2:29	**MEDINA Project** MEDINA Project • 95 visualizaciones • hace 4 semanas
2	11:06	**Overview of the MEDINA Framework** MEDINA Project • 4 visualizaciones • hace 17 horas
3	24:33	**MEDINA Integrated UI** MEDINA Project • 27 visualizaciones • hace 6 días
4	20:59	**Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case** MEDINA Project • 20 visualizaciones • hace 3 semanas
5	22:01	**MEDINA Training: Installation of the MEDINA Framework** MEDINA Project • 15 visualizaciones • hace 2 semanas
6	22:43	**MEDINA Training: Catalogue of Controls and Metrics** MEDINA Project • 31 visualizaciones • hace 1 mes
7	21:32	**MEDINA Training: Customization of Requirements** MEDINA Project • 51 visualizaciones • hace 2 meses
8	27:03	**MEDINA Training: Risk Assessment** MEDINA Project • 14 visualizaciones • hace 2 semanas
9	10:16	**MEDINA Training: Clouditor components** MEDINA Project • 17 visualizaciones • hace 3 semanas
10	11:49	**MEDINA Training: Assessment and Management of Organizational Evidence (AMOE)** MEDINA Project • 22 visualizaciones • hace 3 semanas
11	11:58	**MEDINA Training: Codyze** MEDINA Project • 2 visualizaciones • hace 17 horas
12	4:46	**MEDINA Training: Wazuh and VAT Evidence Collection** MEDINA Project • 8 visualizaciones • hace 6 días
13	9:24	**MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications** MEDINA Project • 7 visualizaciones • hace 6 días

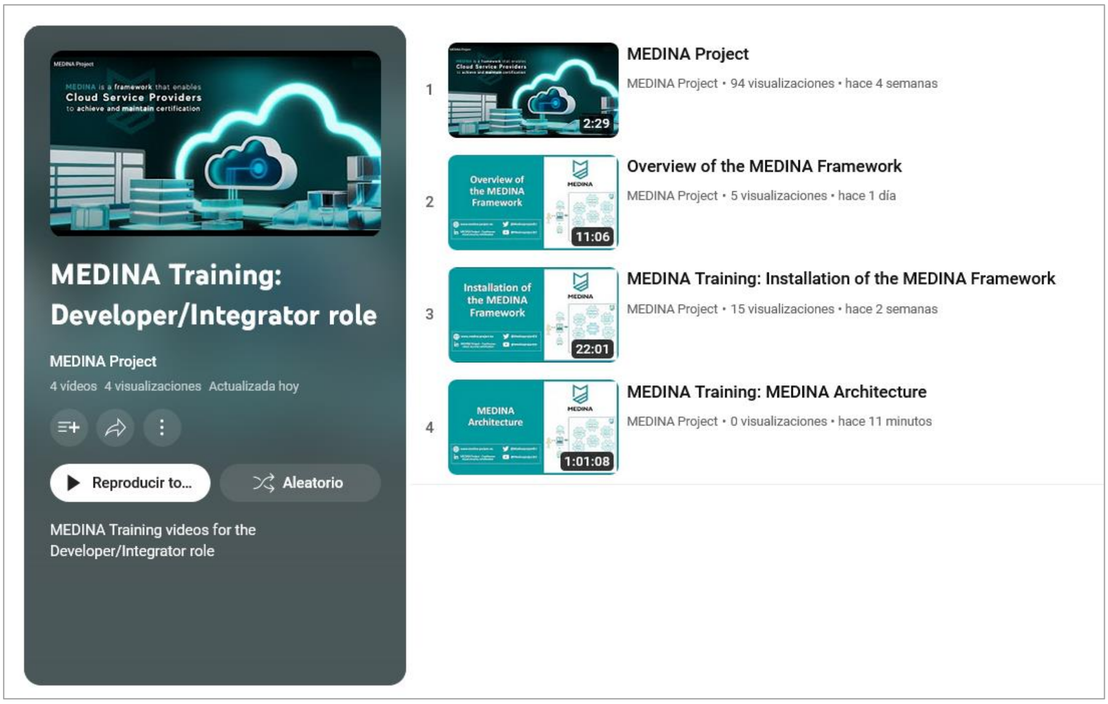
MEDINA is a framework that enables Cloud Service Providers to achieve and maintain certification
Overview of the MEDINA Framework
MEDINA Integrated UI
Company Compliance Dashboard
Installation of the MEDINA Framework
Catalogue of Controls and Metrics
Customization of Requirements
Risk Assessment
Cloud Evidence Collector Security Assessment Orchestrator
Assessment and Management of Organisational Evidence (AMOE)
Codyze
Wazuh and VAT Evidence Collection
Continuous Life-Cycle Management of Cloud Security Certifications
MEDINA

Figure 6. Training videos for the "Product Security Engineer" role

2.2.4 Training videos for the user role Developer/Integrator

The Developer/Integrator role in MEDINA is engaged with the implementation and integration of cloud services.

The set of training videos designed for the Developer/Integrator user role comprises 4 videos, as shown in Figure 7, and is available at this link: MEDINA Training: Product Security role - YouTube. Section 3.2 includes the description of these videos.



MEDINA Training: Developer/Integrator role

MEDINA Project

4 vídeos 4 visualizaciones Actualizada hoy

MEDINA Training videos for the Developer/Integrator role

1 MEDINA Project (2:29)
MEDINA Project • 94 visualizaciones • hace 4 semanas

2 Overview of the MEDINA Framework (11:06)
MEDINA Project • 5 visualizaciones • hace 1 día

3 MEDINA Training: Installation of the MEDINA Framework (22:01)
MEDINA Project • 15 visualizaciones • hace 2 semanas

4 MEDINA Training: MEDINA Architecture (1:01:08)
MEDINA Project • 0 visualizaciones • hace 11 minutos

Figure 7. Training videos for the "Developer/Integrator" role

3 MEDINA Training Material

This section includes a summary of the material produced by MEDINA project partners to support the training activities presented in Section 2. The details of the presentations can be found in *APPENDIX A: Material for the preparation of* the Training Events.

3.1 Material for the preparation of the Training Events

MEDINA partners presented a total of nine talks, lectures and webinars to an audience at universities and schools, such as Lancaster University and The European Network for Cybersecurity (NeCS) PhD School. In the following sections we provide a summary for each of these activities. The presentations used can be found in *APPENDIX A: Material for the preparation of* the Training Events

3.1.1 Talk "More than just a risk assessment".

The talk was delivered by Artsiom Yautsiukhin (CNR) in the scope of CyberSecurity Day 2023, a yearly event organised by the cyber security group of IIT-CNR in Pisa. The talk, which was delivered in Italian (title: "Piu che solo gestione del rischio"), described the possibility to use risk assessment to support the certification evaluation process. This is the direct result of CNR's work in the MEDINA project. Moreover, the talk included the description of the dynamic risk assessment, also developed in scope of MEDINA.

3.1.2 Lecture "Cyber Security Risk Assessment and Mitigation"

This was a lecture for Master students (about 60-70 persons) delivered by CNR on-line in Italian (title: "Valutazione e mitigazione del rischio di sicurezza cyber") within the Cyber Security master in the University of Pisa.

The course focused on risk assessment and risk treatment. The topics covered in the lecture were: Basic terms and concepts, Risk Management vs. Risk Assessment, Risk assessment, Risk identification, Assets, Threats, Vulnerabilities/Security controls, Risk analysis, Risk evaluation, and Risk Treatment.

The lecture also included some general information about cyber security standards.

3.1.3 Lecture "MEDINA: Automated-based certification for cloud services in Europe"

In the context of Barcelona Tech's MSc Programme in Cybersecurity, Dr. Jesus Luna García (Bosch) was invited to a lecture for academic staff and students on the topic "MEDINA: Automated-based certification for cloud services in Europe". This 120 mins. lecture covered background aspects related to MEDINA (e.g., the new EU Cybersecurity Certification Scheme for Cloud Services, EUCS for short) and provided a deep dive on the developed framework, standardization efforts and practical experiences related to its validation. The participants in this lecture asked interesting questions related to the implemented techniques for technical compliance validation, and about the future of MEDINA (exploitation activities and planned spin-off initiatives). Emphasis was put on suggesting commercialization of components like Clouditor, which is seen as a "one of its kind" because its unique design around EUCS.

As part of the lecture, an online survey was made available for the participants asking about their thoughts related to EUCS. The online results, which were consistent with the in-class discussions, clearly shown the overall perception of the effort it will take cloud providers to obtain this new certification. This is precisely where MEDINA provides a clear added value. We hope that future adopters of the developed framework will confirm how the automation and trustworthiness given by MEDINA will result in clear benefits for their business.

3.1.4 Lecture "MEDINA – Paving the road towards continuous audit-based certification for cloud services in Europe."

During this session, delivered by Dr. Jesus Luna García (Bosch), the audience (mostly grad students from all over Europe) found out about the EU Cybersecurity Act (EUCSA) and the hard-work ENISA is putting in developing the novel EU Cybersecurity Certification Scheme for Cloud Services (EUCS). After some basic terminology related to certification processes was introduced, the lecture presented the MEDINA project with a specific focus on its architectural framework and ongoing leverage of NLP-techniques. A demo session was also included to communicate, in a concrete manner, the developed framework and its advantages for all involved stakeholders. Finally, the lecture closed by elaborating on the question "What comes after MEDINA?", where diverse topics were briefly discussed e.g., certification of AI trustworthiness, and future sustainability of MEDINA's outcomes.

3.1.5 Seminar "Intelligent AI Security"

This session, delivered by Dr. Jesus Luna García (Bosch), focused on discussing how the notion of continuous (automated) monitoring can also support AI trustworthiness. Initial ideas have been shaped in the follow-up project COBALT.

3.1.6 TAS-S Seminar "From Continuous Monitoring to Continuous Cloud Cybersecurity Certification"

This seminar, delivered by Dr. Jesus Luna García (Bosch) at the University of Lancaster, is part of the industrial engagements organized by the institution, with the goal of engaging its academic/research community in current cyber security topics. MEDINA presented its approach to both EUCS and continuous audit-based certification, along with a glimpse into the future of the proposed framework where artificial intelligence is expected to play a major role.

3.1.7 Lecture "Cyber insurance"

The lecture was delivered by Artsiom Yautsiukhin (CNR) in the scope of NeCS winter school in 2022. Although, the primary focus of the lecture was on cyber insurance, various topics related to cyber security economics and management were discussed. In particular, the topic of cyber risk assessment took a significant part of the course, as a prerequisite for cyber insurance.

3.1.8 Talk "A tool for risk analysis and reduction"

The talk was delivered by Artsiom Yautsiukhin (CNR) in the scope of the CyberSecurity Day 2021, a yearly event organised by the cyber security group of IIT-CNR in Pisa. It was based on the initial risk assessment tool, which was used as the starting point for the SATRA tool used in MEDINA. The talk included the topic of risk assessment, i.e., how to conduct risk assessment with the tool. Moreover, this presentation also presented CNR's idea about conducting risk reduction (the basis for risk optimisation functionality later used in MEDINA).

3.1.9 Webinar "Cybersecurity in automotive industry"

In cooperation with ICT horizontal, SRIP PMiS, XLAB conducted an expert discussion on the importance of cybersecurity, which is one of the important topics in the field of information and communication technologies and is also increasingly mentioned in connection with the automotive industry and production processes.

The webinar addressed the issue of data protection, which is increasingly being exchanged within supply chains, and special attention was paid to the expert presentation of the standardization requirements of products and components in the automotive industry in relation to cybersecurity and certification.

3.2 Material for the preparation of the Training Videos

The MEDINA training sets comprise a total of 18 videos that have been uploaded to the MEDINA YouTube channel[3]. In the following we present the list of videos and a description of their content.

3.2.1 Classification of the videos

Table 2 shows the titles of the videos that make up the training sets, the links to the videos in YouTube, and the partner responsible for their creation and recording. Each video has been classified into one or more sets, depending on the user role for which it is intended (see Section 2.2).

Table 2. List of Training videos

			Target Audience / Role			
#	**Video Title**	**Partner**	**Auditor**	**Security Governance**	**Product Security**	**Developer/ Integrator**
1	MEDINA Project	**TECNALIA**	X	X	X	X
2	Overview of the MEDINA Framework	**BOSCH**	X	X	X	X
3	MEDINA Integrated UI	**BOSCH**	X	X	X	
4	EUCS Automation with MEDINA - An IoT Cloud Use Case	**BOSCH**		X		
5	Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case	**FABASOFT**	X	X	X	
6	Are you ready for European Cloud Service Security Certification?	**NIXU**	X			
7	MEDINA Training: MEDINA Architecture	**TECNALIA**			X	X
8	MEDINA Training: Installation of the MEDINA Framework	**HPE**			X	X
9	MEDINA Training: Catalogue of Controls and Metrics	**TECNALIA**	X	X	X	
10	MEDINA Training: Customization of Requirements	**CNR, HPE**	X		X	
11	MEDINA Training: Risk Assessment	**CNR**		X	X	
12	MEDINA Training: Clouditor components	**FhG**	X		X	

[3] Please refer to: https://www.youtube.com/@MedinaprojectEU

			Target Audience / Role			
#	Video Title	Partner	Auditor	Security Governance	Product Security	Developer/ Integrator
13	MEDINA Training: Assessment and Management of Organizational Evidence (AMOE)	FABASOFT			X	
14	MEDINA Training: Codyze	FhG			X	
15	MEDINA Training: Wazuh and VAT Evidence Collection	XLAB			X	
16	MEDINA Training: Integrity Validation of Evidence	TECNALIA	X	X		
17	MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications	XLAB, FhG, CNR	X	X	X	
18	MEDINA Training: Credentials and Proofs of certificates	TECNALIA	X	X		

3.2.2 Description of video contents

Table 3 shows a summary of the content of each of the videos depicted in Table 2. A detailed description of all the MEDINA components is available in the Deliverable D5.5 [4].

The presentations used in the recording of the videos can be found in *APPENDIX B: Material for the preparation of the training videos.*

Table 3. Description of the MEDINA Training videos

#	Title	Description
1	MEDINA Project	MEDINA promotional video presenting the value proposition of the project, who is aimed at, and what its benefits are.
2	Overview of the MEDINA Framework	Training video that provides some basic background of the European Cybersecurity Certification Scheme for cloud services (or EUCS for short), followed by a short overview of the European funded MEDINA project, along with the contributed framework.
3	MEDINA Integrated UI	Demonstration of the functionality of the MEDINA Integrated User Interface.
4	EUCS Automation with MEDINA - An IoT Cloud Use Case	Training video on the Use Case implemented by Bosch in the MEDINA project.
5	Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case	Training video about the functionalities of the "Company Compliance Dashboard", application developed by Fabasoft which makes use of the APIs provided by the MEDINA components.
6	Are you ready for European Cloud Service Security Certification?	Training video showing Nixu's auditor view on MEDINA and Cloud Service Certification

#	Title	Description
7	MEDINA Training: MEDINA Architecture	Training video presenting an overview of the MEDINA framework architecture. First, a diagram with the building blocks of the framework is presented, then, the data model is shown, followed by the user management, and the description of each of the individual components in the MEDINA architecture.
8	MEDINA Training: Installation of the MEDINA Framework	Training video about the installation of the MEDINA framework. It presents the Hardware Infrastructure and the Installation of Kubernetes Cluster.
9	MEDINA Training: Catalogue of Controls and Metrics	Training video about the **Catalogue of Controls and Metrics** component, that stores the EUCS certification scheme (draft version August-2022). On the one hand, it offers an API to the rest of MEDINA components to access the scheme information. And, on the other hand, it has a Graphical User Interface that allows the user to navigate through the EUCS, to consult it.
10	MEDINA Training: Customization of Requirements	Training video about the **Customization of requirements** functionality, that includes three components: NL2CNL Translator, CNL Editor, DSL Mapper. This functionality allows the user to select the requirement associated with a set of security metrics, customize it, and then sent this information to the assessment tools.
11	MEDINA Training: Risk Assessment	Training video about the **Risk Assessment and Optimization Framework (RAOF)** component, that is self-Assessment Tool for Risk Analysis (SATRA). The goal of the tool is to provide a risk-based analysis of non-conformities (with EUCS) for Cloud services.
12	MEDINA Training: Clouditor components	Training video about three Clouditor-based components: **Cloud Evidence Collector, Security Assessment** and **Orchestrator.** The Cloud Evidence Collector collects evidence using cloud APIs, such as configurations of virtual machines and storages. The Security Assessment receives evidence from the Cloud Evidence Collector and assesses it using pre-defined metrics. The Orchestrator receives, forwards, and stores evidence and assessment results. It offers many interfaces to other components, such as the Catalogue of Controls and Metrics and the Continuous Certification Evaluation.
13	MEDINA Training: Assessment and Management of Organizational Evidence (AMOE)	Training video about the **AMOE** component, a gathering tool for organizational evidence based on policy documents. The extracted evidence is presented to a user/auditor for inspection. The user can decide if the presented evidence does fit the requirements and set an assessment status. The defined assessment results can be forwarded to the rest of the MEDINA framework by sending it to the Orchestrator.
14	MEDINA Training: Codyze	Training video about **Codyze**, which is a Static code analysis tool that checks source code for security non-compliances.
15	MEDINA Training: Wazuh and VAT Evidence Collection	Training video about **Wazuh** and **Vulnerability Assessment Tools (VAT)**. Wazuh is an open-source security monitoring tool for threat detection, integrity monitoring, incident response and basic compliance monitoring. Vulnerability Assessment Tools (VAT) act as a vulnerability scanning and detection framework, comprised of: • two web vulnerability scanners (W3af and OWASP ZAP)

#	Title	Description
		• a network discovery and auditing tool Nmap • a framework for including user-defined custom scripts for detecting specific issues or simply notifying about unavailability of services
16	MEDINA Training: Integrity Validation of Evidence	Training video about the **MEDINA Evidence Trustworthiness System** component, which maintains an improved audit trail of evidence and assessment results. It uses Blockchain technology as secure backbone and provides a manual and automatic way of verification of evidence and assessment results integrity. Provides a record of information on a verifiable way (verification), a record of information on a permanent way (traceability) and guarantees resistance to modification of stored data (integrity).
17	MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications	Training video about three components of the MEDINA framework related to the Continuous Life-Cycle Management of Cloud Security Certifications, namely **Continuous Certification Evaluation** (CCE), **Risk Assessment Optimization Framework** (RAOF) and **Automated Life-Cycle Manager** (LCM). The Continuous Certification Evaluation collects assessment results from the Orchestrator and builds an evaluation tree for the Target of Evaluation (ToE), representing the aggregated assessment results on higher levels of the certification scheme (e.g., EUCS). The Risk Assessment Optimization Framework receives the evaluation tree and performs a risk assessment process. The Automated Life-Cycle Manager receives operational effectiveness measures from CCE and risk information from RAOF and computes the status of the ToE certification.
18	MEDINA Training: Credentials and Proofs of certificates	Training video about the **Self Sovereign Identity (SSI)** component, which provides secure proofs to automatically verify the validity of a certificate. Every change of certificate provokes the emission of a verifiable credential that will allow the CSP to issue a secure proof of the certificate status.

4 Conclusions

This deliverable presented the relevant training activities carried out during the MEDINA project lifecycle. It gave a detailed description of all the training events and training videos as well as the materials used for them. All partners are involved in these activities either as a contributors or leaders.

The achievement of the KPIs defined for training demonstrates that the strategy followed is appropriate.

Finally, we would like to remark that, although this deliverable covers the training activities that partners undertook to disseminate the results of the project, partners will always look for additional ways to spread knowledge about MEDINA.

5 References

[1] MEDINA Consortium, “D7.2 Dissemination and Communication Strategy,” 2021.

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

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

[4] MEDINA Consortium, “D5.5 MEDINA integrated solution-v3,” 2023.

APPENDIX A: Material for the preparation of the Training Events

This Appendix contains the slides of the presentations which were used during the MEDINA training events in Table 1.

1. **Talk "More than just a risk assessment"**. Cybersecurity Day 2023, University of Pisa (Italy), 6 October 2023. Autor: Artsiom Yautsiukhin (CNR)

2. **Lecture "Valutazione e mitigazione del rischio di sicurezza cyber"** (ENG: "Cyber Security Risk Assessment and Mitigation")". Cyber Security Master, University of Pisa (Italy), 31 March 2023. Autor: Artsiom Yautsiukhin (CNR)

3. **Lecture "MEDINA: Automation-based certification for cloud services in Europe".** Tech's MSc Programme in Cybersecurity**,** Barcelona (Spain), 12 April 2023. Autor: Jesus Luna Garcia (Bosch)

4. **Lecture "MEDINA – Paving the road towards continuous audit-based certification for cloud services in Europe"**. NECS PhD Winter School, 6 February 2023. Autor: Jesus Luna Garcia (Bosch)

5. **Seminar on "Intelligent AI Security"**. TU Darmstadt (Germany), 14 December 2022. Autor: Jesus Luna (Bosch)

6. **TAS-S Seminar "From Continuous Monitoring to Continuous Cloud Cybersecurity Certification"**. Lancaster University (UK), 4 February 2022. Autor: Jesus Luna Garcia (Bosch)

7. **Lecture "Cyber insurance"**. NeCS Winter School, 18 January 2022. Autor: Artsiom Yautsiukhin (CNR)

8. **Talk "Lo strumento di analisi e riduzione dei rischi".** Cybersecurity Day 2021, 8 October 2021. Autor: Artsiom Yautsiukhin (CNR)

9. **Webinar "Cybersecurity in automotive industry"**. Slovenian Chamber of Commerce members, 21 September 2021. Autor: Aleš Černivec (XLAB)

Piu che solo gestione del rischio

Artsiom Yautsiukhin

CYBER LAB SECURITY
Consiglio Nazionale delle Ricerche

Ottimizzazione basata sul rischio e selezione del fornitore di sicurezza.

Consiglio Nazionale delle Ricerche

ISTITUTO
DI INFORMATICA
E TELEMATICA

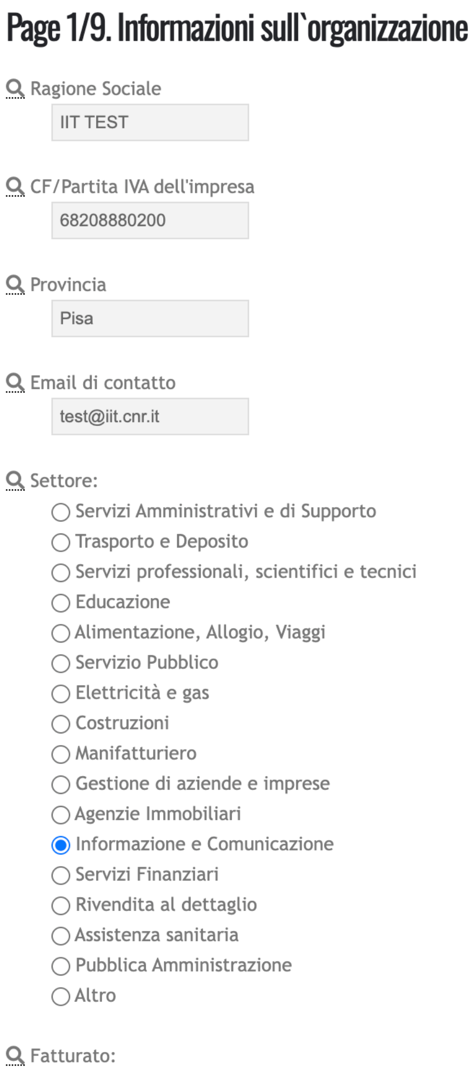
Servizio in breve

- Valutazione del rischio
  - Fornire un elenco di risorse
  - Rispondere al questionario (requisiti)
  - Calcolare il rischio (automaticamente)
- Ottimizzazione del rischio
  - Impostare il limite di budget
  - Impostare i costi di correzione
  - Trovare la configurazione ottimale
- Suggerimenti da ECSO radar
  - Ricercare le aziende che possono aiutare ad affrontare i requisiti non soddisfatti

SATRA

- SATRA is a Self-Assessment Tool for Risk Analysis
  - Implementato come un servizio
  - Consente di condurre una valutazione del rischio informatico ***veloce*** e ***semplice***
  - Richiede solo la fornitura di informazioni su
    - Requisiti di sicurezza affrontati
    - Principali risorse (assets)
  - Basato su schemi di certificazione per la sicurezza informatica:
    - ISO 27001, EUCS (può essere applicato ad altri standard come (N)CSF, C5, ecc.)

Descrivere l’organizzazione



Page 1/9. Informazioni sull`organizzazione

Ragione Sociale

IIT TEST

CF/Partita IVA dell'impresa

68208880200

Provincia

Pisa

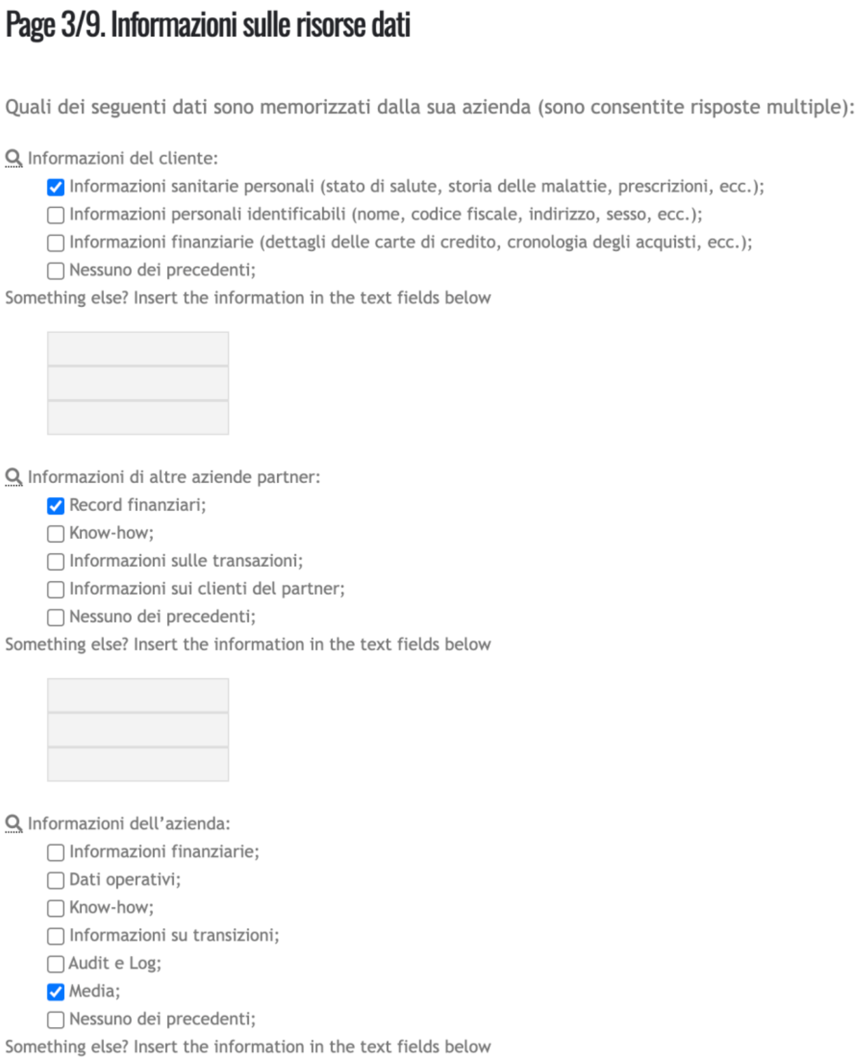
Email di contatto

test@iit.cnr.it

Settore:

○ Servizi Amministrativi e di Supporto
○ Trasporto e Deposito
○ Servizi professionali, scientifici e tecnici
○ Educazione
○ Alimentazione, Allogio, Viaggi
○ Servizio Pubblico
○ Elettricità e gas
○ Costruzioni
○ Manifatturiero
○ Gestione di aziende e imprese
○ Agenzie Immobiliari
● Informazione e Comunicazione
○ Servizi Finanziari
○ Rivendita al dettaglio
○ Assistenza sanitaria
○ Pubblica Amministrazione
○ Altro

Fatturato:



Page 3/9. Informazioni sulle risorse dati

Quali dei seguenti dati sono memorizzati dalla sua azienda (sono consentite risposte multiple):

Informazioni del cliente:

☑ Informazioni sanitarie personali (stato di salute, storia delle malattie, prescrizioni, ecc.);
□ Informazioni personali identificabili (nome, codice fiscale, indirizzo, sesso, ecc.);
□ Informazioni finanziarie (dettagli delle carte di credito, cronologia degli acquisti, ecc.);
□ Nessuno dei precedenti;

Something else? Insert the information in the text fields below

Informazioni di altre aziende partner:

☑ Record finanziari;
□ Know-how;
□ Informazioni sulle transazioni;
□ Informazioni sui clienti del partner;
□ Nessuno dei precedenti;

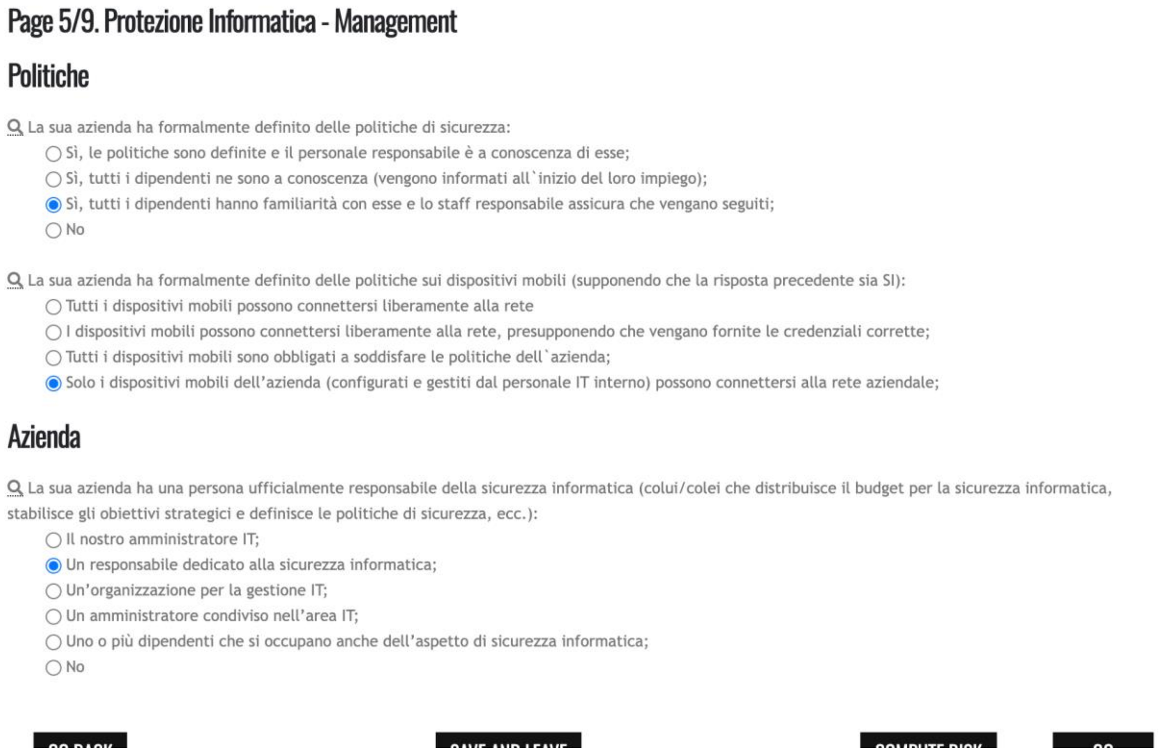
Something else? Insert the information in the text fields below

Informazioni dell’azienda:

□ Informazioni finanziarie;
□ Dati operativi;
□ Know-how;
□ Informazioni su transizioni;
□ Audit e Log;
☑ Media;
□ Nessuno dei precedenti;

Something else? Insert the information in the text fields below

Rispondere a domande sulla sicurezza cyber



Page 5/9. Protezione Informatica - Management

Politiche

La sua azienda ha formalmente definito delle politiche di sicurezza:

- ○ Sì, le politiche sono definite e il personale responsabile è a conoscenza di esse;
- ○ Sì, tutti i dipendenti ne sono a conoscenza (vengono informati all`inizio del loro impiego);
- ● Sì, tutti i dipendenti hanno familiarità con esse e lo staff responsabile assicura che vengano seguiti;
- ○ No

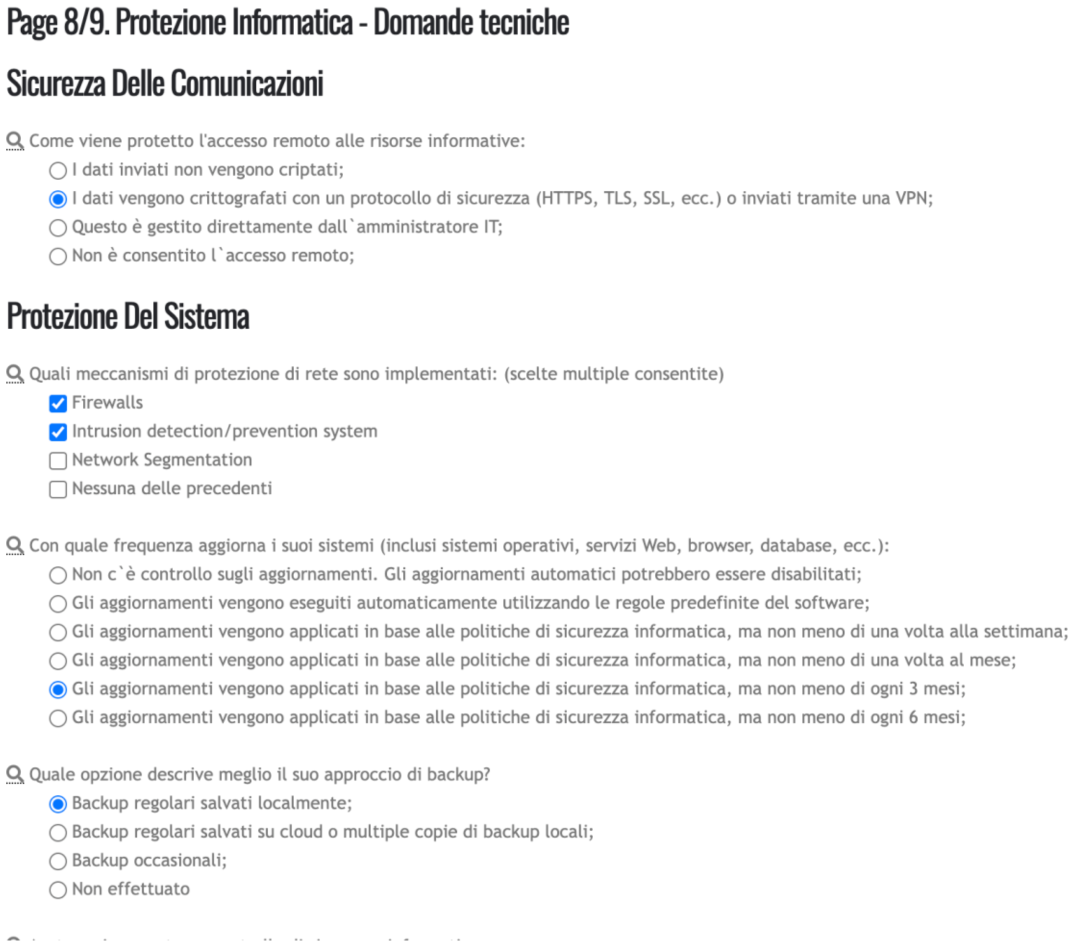
La sua azienda ha formalmente definito delle politiche sui dispositivi mobili (supponendo che la risposta precedente sia SI):

- ○ Tutti i dispositivi mobili possono connettersi liberamente alla rete
- ○ I dispositivi mobili possono connettersi liberamente alla rete, presupponendo che vengano fornite le credenziali corrette;
- ○ Tutti i dispositivi mobili sono obbligati a soddisfare le politiche dell`azienda;
- ● Solo i dispositivi mobili dell'azienda (configurati e gestiti dal personale IT interno) possono connettersi alla rete aziendale;

Azienda

La sua azienda ha una persona ufficialmente responsabile della sicurezza informatica (colui/colei che distribuisce il budget per la sicurezza informatica, stabilisce gli obiettivi strategici e definisce le politiche di sicurezza, ecc.):

- ○ Il nostro amministratore IT;
- ● Un responsabile dedicato alla sicurezza informatica;
- ○ Un'organizzazione per la gestione IT;
- ○ Un amministratore condiviso nell'area IT;
- ○ Uno o più dipendenti che si occupano anche dell'aspetto di sicurezza informatica;
- ○ No



Page 8/9. Protezione Informatica - Domande tecniche

Sicurezza Delle Comunicazioni

Come viene protetto l'accesso remoto alle risorse informative:

- ○ I dati inviati non vengono criptati;
- ● I dati vengono crittografati con un protocollo di sicurezza (HTTPS, TLS, SSL, ecc.) o inviati tramite una VPN;
- ○ Questo è gestito direttamente dall`amministratore IT;
- ○ Non è consentito l`accesso remoto;

Protezione Del Sistema

Quali meccanismi di protezione di rete sono implementati: (scelte multiple consentite)

- ☑ Firewalls
- ☑ Intrusion detection/prevention system
- □ Network Segmentation
- □ Nessuna delle precedenti

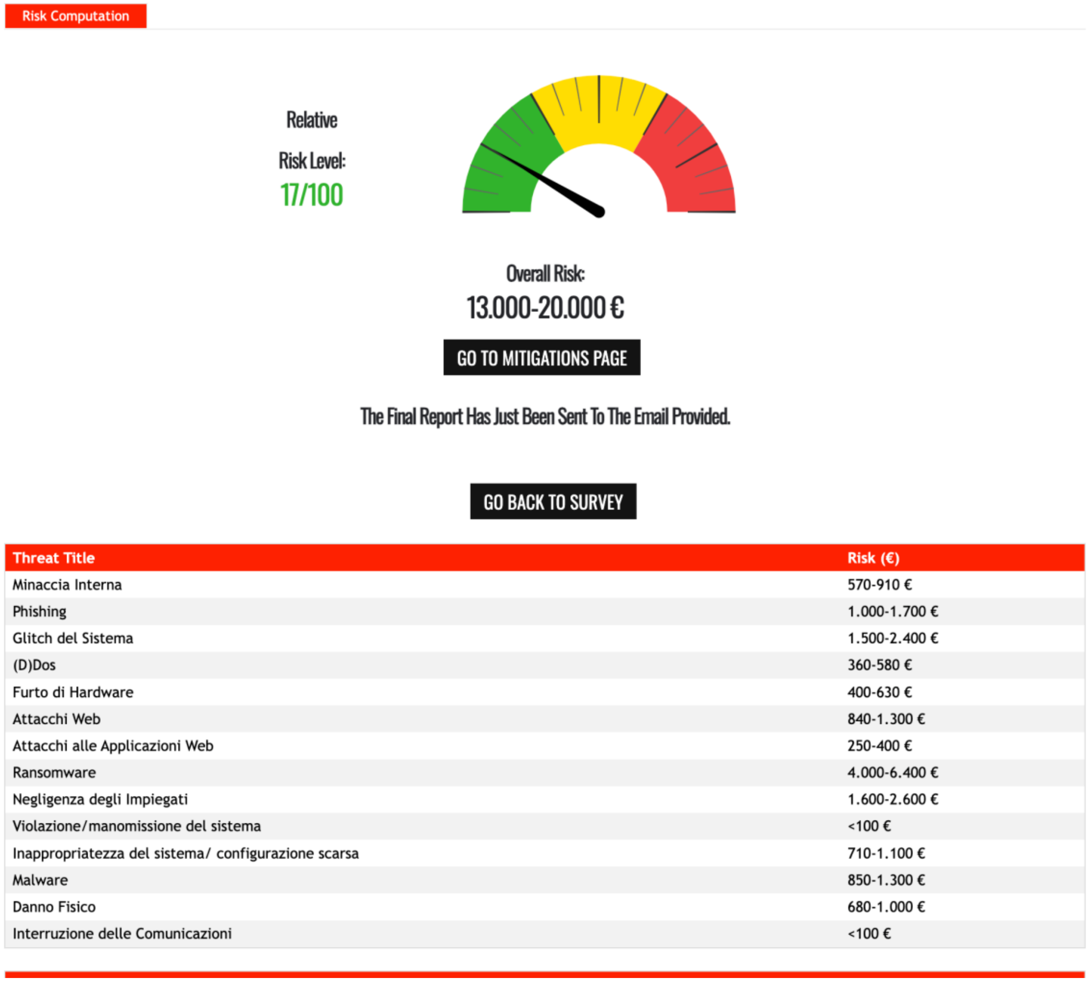
Con quale frequenza aggiorna i suoi sistemi (inclusi sistemi operativi, servizi Web, browser, database, ecc.):

- ○ Non c`è controllo sugli aggiornamenti. Gli aggiornamenti automatici potrebbero essere disabilitati;
- ○ Gli aggiornamenti vengono eseguiti automaticamente utilizzando le regole predefinite del software;
- ○ Gli aggiornamenti vengono applicati in base alle politiche di sicurezza informatica, ma non meno di una volta alla settimana;
- ○ Gli aggiornamenti vengono applicati in base alle politiche di sicurezza informatica, ma non meno di una volta al mese;
- ● Gli aggiornamenti vengono applicati in base alle politiche di sicurezza informatica, ma non meno di ogni 3 mesi;
- ○ Gli aggiornamenti vengono applicati in base alle politiche di sicurezza informatica, ma non meno di ogni 6 mesi;

Quale opzione descrive meglio il suo approccio di backup?

- ● Backup regolari salvati localmente;
- ○ Backup regolari salvati su cloud o multiple copie di backup locali;
- ○ Backup occasionali;
- ○ Non effettuato

Resultato



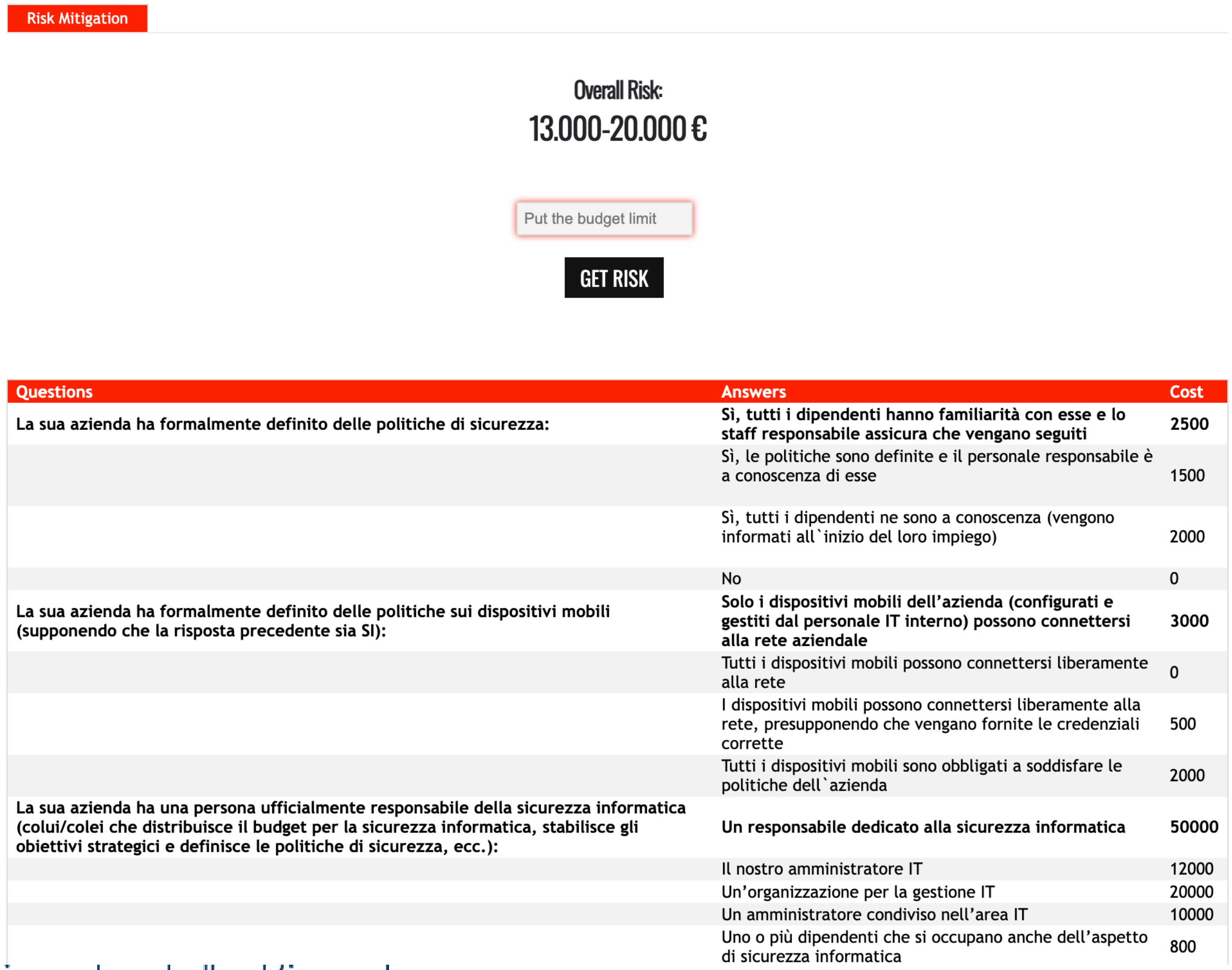
Relative
Risk Level:
17/100

Overall Risk:
13.000-20.000 €

The Final Report Has Just Been Sent To The Email Provided.

Threat Title	Risk (€)
Minaccia Interna	570-910 €
Phishing	1.000-1.700 €
Glitch del Sistema	1.500-2.400 €
(D)Dos	360-580 €
Furto di Hardware	400-630 €
Attacchi Web	840-1.300 €
Attacchi alle Applicazioni Web	250-400 €
Ransomware	4.000-6.400 €
Negligenza degli Impiegati	1.600-2.600 €
Violazione/manomissione del sistema	<100 €
Inappropriatezza del sistema/ configurazione scarsa	710-1.100 €
Malware	850-1.300 €
Danno Fisico	680-1.000 €
Interruzione delle Comunicazioni	<100 €

Ottimizzazione. Input



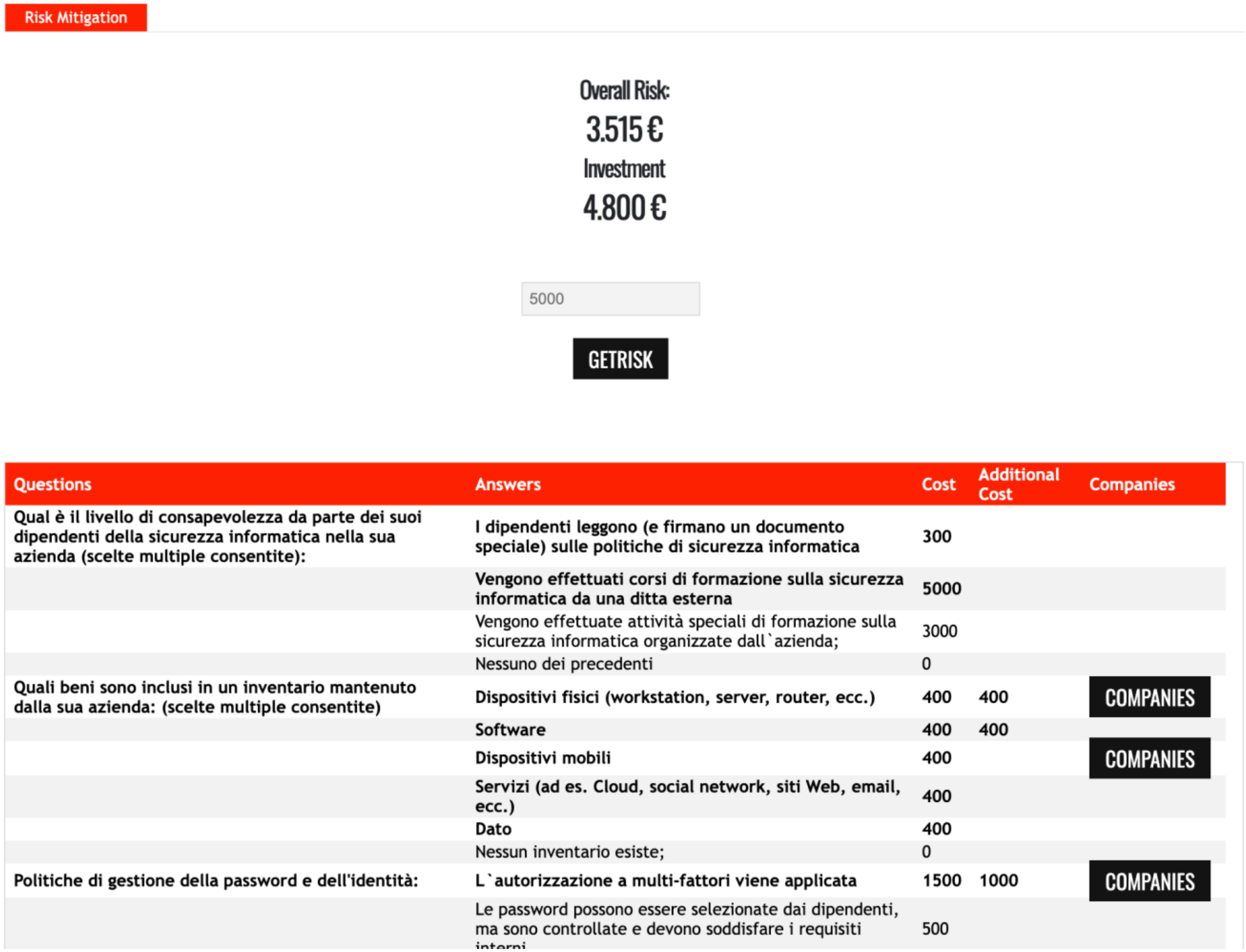
Risk Mitigation

Overall Risk:

13.000-20.000 €

Questions	Answers	Cost
La sua azienda ha formalmente definito delle politiche di sicurezza:	**Sì, tutti i dipendenti hanno familiarità con esse e lo staff responsabile assicura che vengano seguiti**	**2500**
	Sì, le politiche sono definite e il personale responsabile è a conoscenza di esse	1500
	Sì, tutti i dipendenti ne sono a conoscenza (vengono informati all`inizio del loro impiego)	2000
	No	0
La sua azienda ha formalmente definito delle politiche sui dispositivi mobili (supponendo che la risposta precedente sia SI):	**Solo i dispositivi mobili dell'azienda (configurati e gestiti dal personale IT interno) possono connettersi alla rete aziendale**	**3000**
	Tutti i dispositivi mobili possono connettersi liberamente alla rete	0
	I dispositivi mobili possono connettersi liberamente alla rete, presupponendo che vengano fornite le credenziali corrette	500
	Tutti i dispositivi mobili sono obbligati a soddisfare le politiche dell`azienda	2000
La sua azienda ha una persona ufficialmente responsabile della sicurezza informatica (colui/colei che distribuisce il budget per la sicurezza informatica, stabilisce gli obiettivi strategici e definisce le politiche di sicurezza, ecc.):	**Un responsabile dedicato alla sicurezza informatica**	**50000**
	Il nostro amministratore IT	12000
	Un'organizzazione per la gestione IT	20000
	Un amministratore condiviso nell'area IT	10000
	Uno o più dipendenti che si occupano anche dell'aspetto di sicurezza informatica	800

Ottimizzazione. Resultato



Risk Mitigation

Overall Risk:

3.515 €

Investment

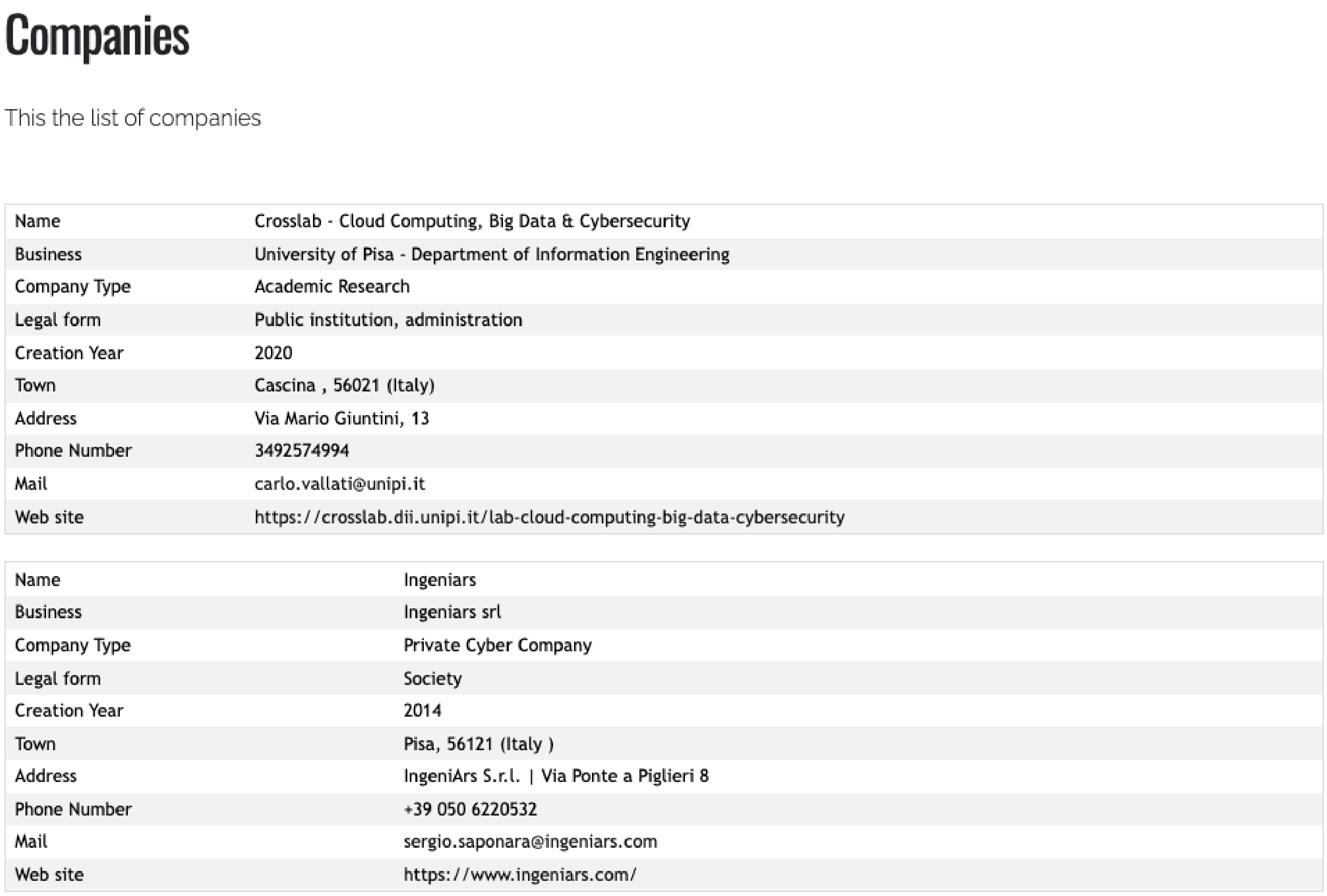
4.800 €

5000

GETRISK

Questions	Answers	Cost	Additional Cost	Companies
Qual è il livello di consapevolezza da parte dei suoi dipendenti della sicurezza informatica nella sua azienda (scelte multiple consentite):	I dipendenti leggono (e firmano un documento speciale) sulle politiche di sicurezza informatica	300		
	Vengono effettuati corsi di formazione sulla sicurezza informatica da una ditta esterna	**5000**		
	Vengono effettuate attività speciali di formazione sulla sicurezza informatica organizzate dall`azienda;	3000		
	Nessuno dei precedenti	0		
Quali beni sono inclusi in un inventario mantenuto dalla sua azienda: (scelte multiple consentite)	Dispositivi fisici (workstation, server, router, ecc.)	400	400	COMPANIES
	Software	400	400	
	Dispositivi mobili	400		COMPANIES
	Servizi (ad es. Cloud, social network, siti Web, email, ecc.)	400		
	Dato	400		
	Nessun inventario esiste;	0		
Politiche di gestione della password e dell'identità:	L`autorizzazione a multi-fattori viene applicata	1500	1000	COMPANIES
	Le password possono essere selezionate dai dipendenti, ma sono controllate e devono soddisfare i requisiti interni	500		

Suggerimenti per fornitori di sicurezza e consulenti. ECSO radar



Companies

This the list of companies

Name	Crosslab - Cloud Computing, Big Data & Cybersecurity
Business	University of Pisa - Department of Information Engineering
Company Type	Academic Research
Legal form	Public institution, administration
Creation Year	2020
Town	Cascina , 56021 (Italy)
Address	Via Mario Giuntini, 13
Phone Number	3492574994
Mail	carlo.vallati@unipi.it
Web site	https://crosslab.dii.unipi.it/lab-cloud-computing-big-data-cybersecurity

Name	Ingeniars
Business	Ingeniars srl
Company Type	Private Cyber Company
Legal form	Society
Creation Year	2014
Town	Pisa, 56121 (Italy)
Address	IngeniArs S.r.l. | Via Ponte a Piglieri 8
Phone Number	+39 050 6220532
Mail	sergio.saponara@ingeniars.com
Web site	https://www.ingeniars.com/

Supporto dinamico basato sul rischio per la verifica della conformità

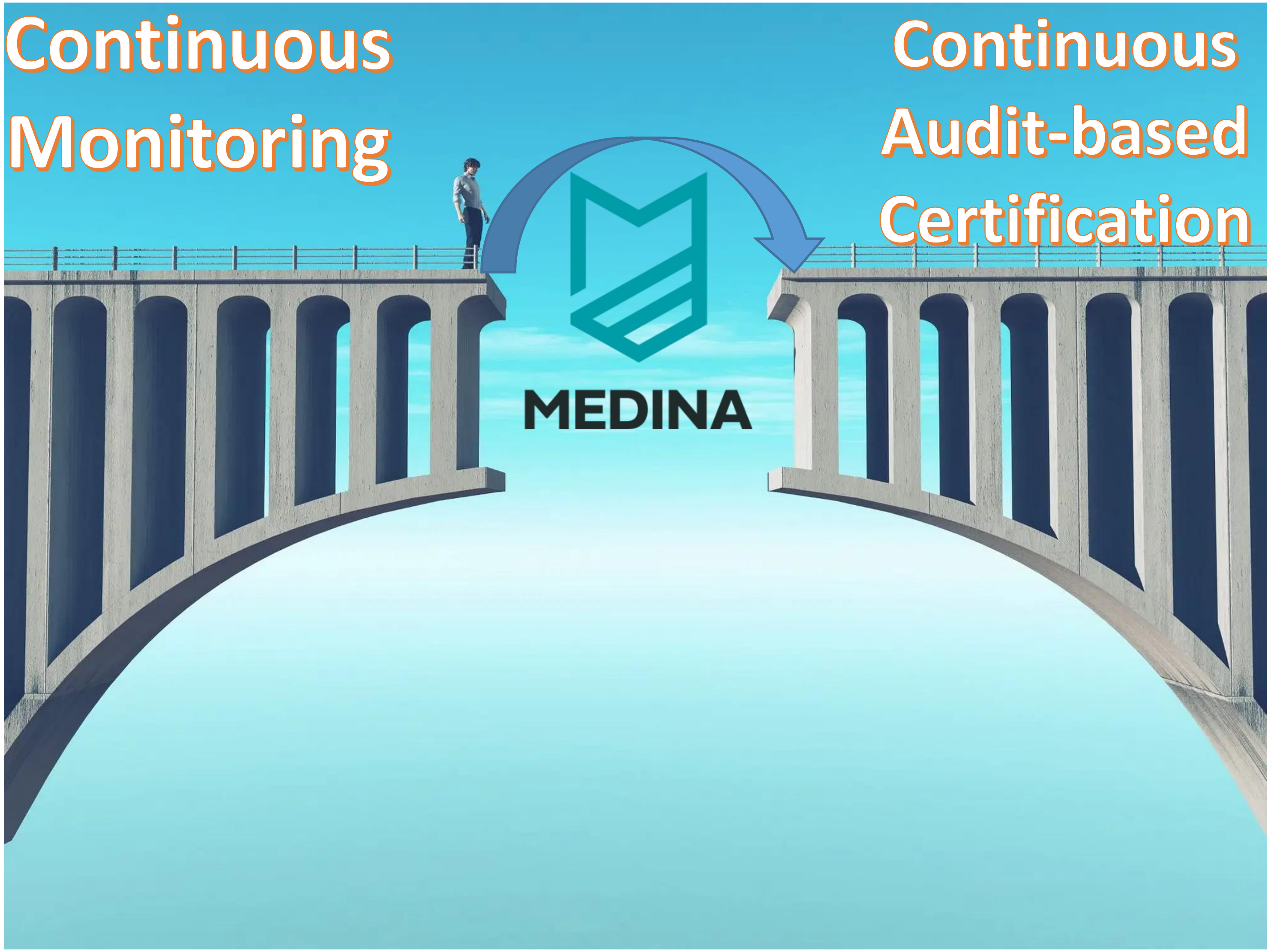
Scopo di MEDINA

- Fornire un ***quadro*** completo che potenzia il controllo e la fiducia dei consumatori del cloud nei servizi cloud consumati, supportando i fornitori di servizi cloud per il ***raggiungimento di una certificazione continua*** in linea con il Regolamento europeo sulla cibersicurezza (EUCSA).

Background: EU Cybersecurity Act

- The EU Cybersecurity Act (EUCSA, April-2019), Propone la creazione di un quadro di certificazione a livello dell'Unione Europea che permette ai clienti di prendere decisioni informate sulla sicurezza informatica
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - EUCS – Cybersecurity Certification Scheme for Cloud Services
- ENISA (EU Agency for Cybersecurity) ha organizzato un Gruppo di Lavoro Ad Hoc per preparare la proposta di ***EUCS*** (European Cybersecurity Standard).
  - La versione provvisoria è stata rilasciata il 22 dicembre 2020.

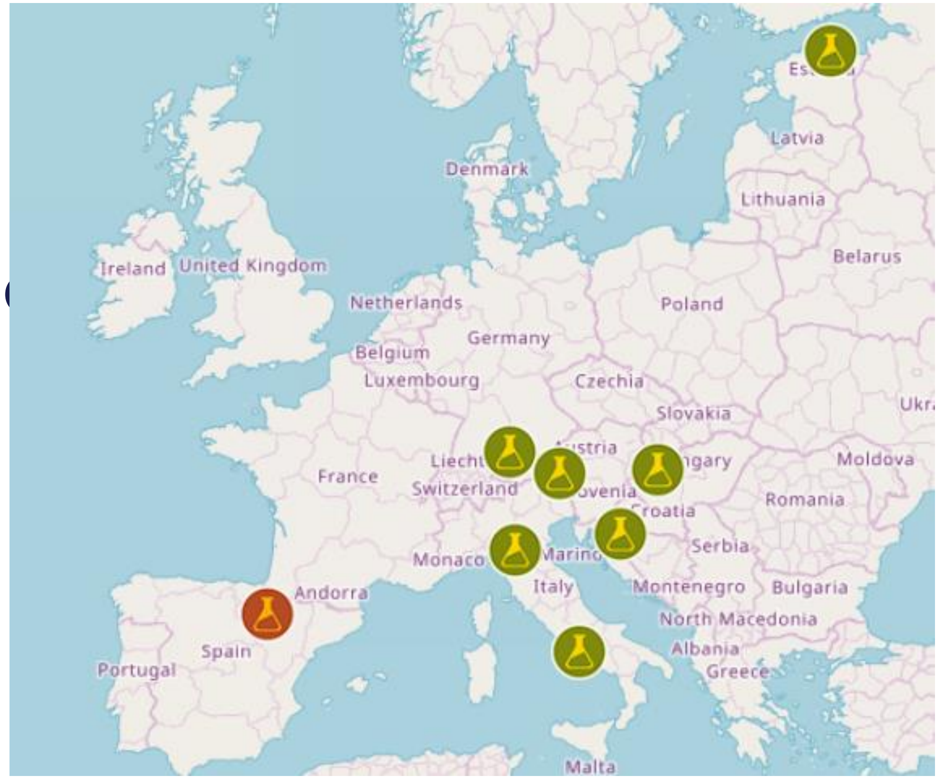
MEDINA – Bridging the Gap



MEDINA At a Glance

- 1st November 2020 – 30th October 2023

- https://medina-project.eu/
- https://twitter.com/medinaproject



tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft®

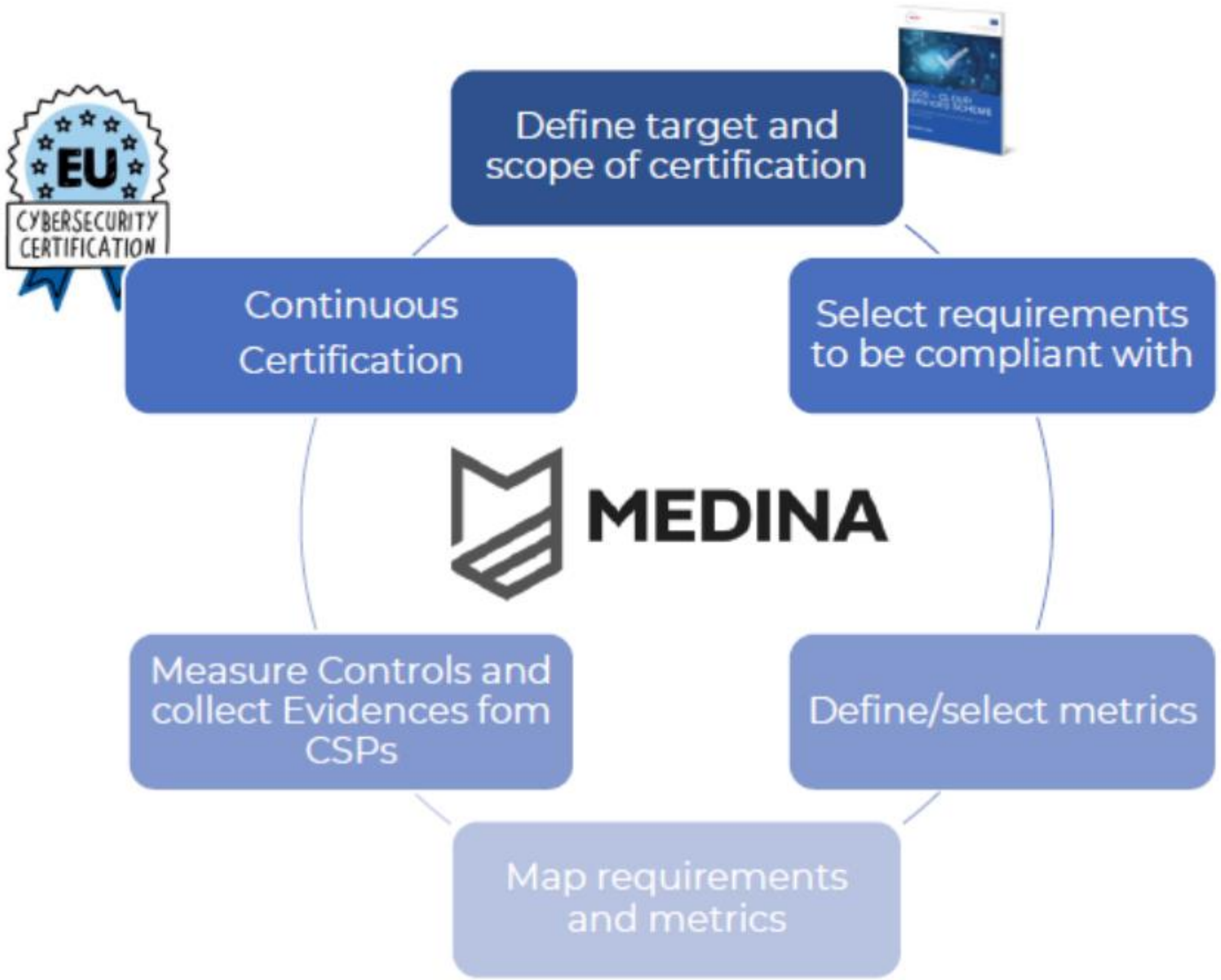
Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Medina Framework



Define target and scope of certification

Select requirements to be compliant with

Define/select metrics

Map requirements and metrics

Measure Controls and collect Evidences fom CSPs

Continuous Certification

Valutazione del rischio per la verifica della conformità

- L'obiettivo
  - Fornire un'analisi basata sul rischio delle non conformità (con EUCS) per i servizi cloud.

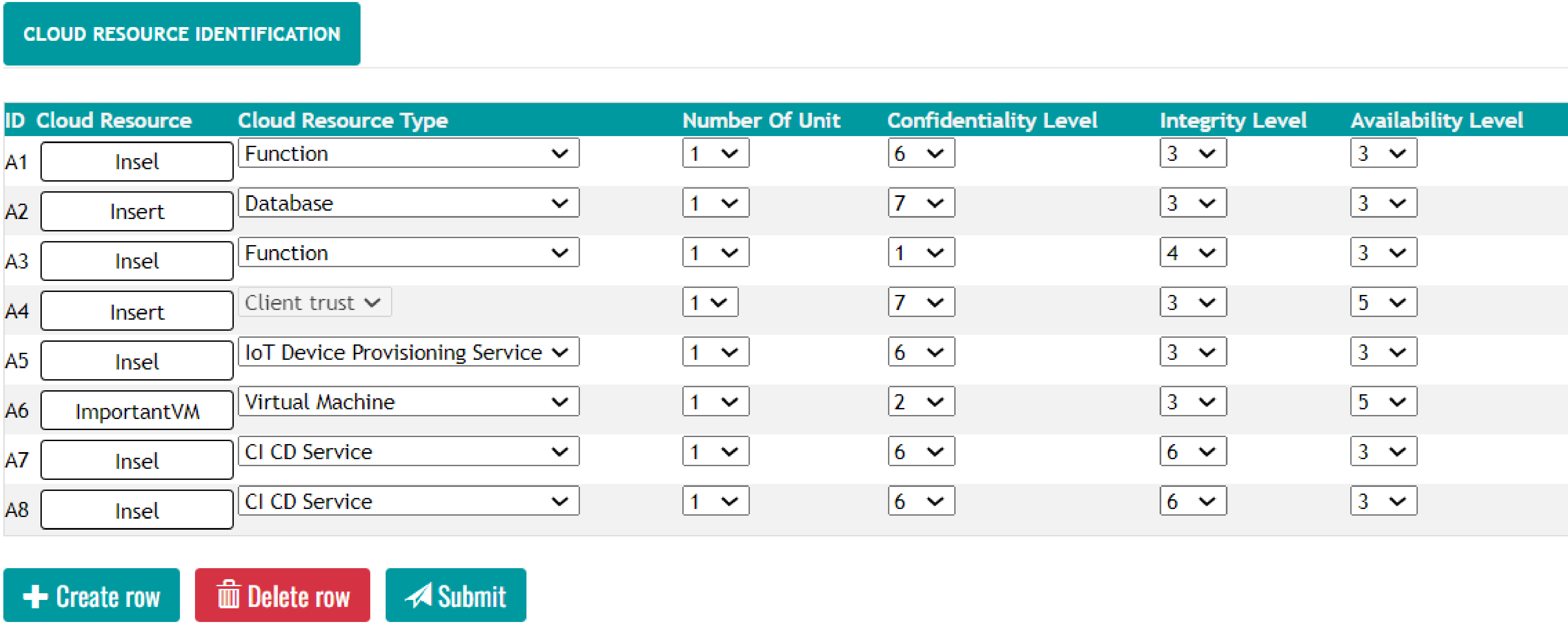
- Ogni CSP effettua una valutazione del rischio (valutazione interna del rischio)
  - Non intendiamo sostituirla
  - Tuttavia, il nostro strumento può essere utilizzato per questo scopo.

- La nostra valutazione del rischio:
  - supporta il processo di valutazione per la certificazione (contro EUCS)
  - è progettata per il Cloud
  - può essere utilizzata
    - per un'analisi "manuale" da parte di un operatore (ad esempio, un responsabile della conformità)
    - per un'analisi automatica (supponendo che le informazioni aggiornate vengano fornite automaticamente)
  - supporta l'ottimizzazione degli sforzi futuri per garantire la conformità.

SATRA in breve

- Input
  - **Minacce** (e frequenza) – elencate nello strumento
  - **Risorse/Assets** (Impatto CIA) – fornite da un operatore
  - **Vulnerabilità** (probabilità di successo) – requisiti EUCS implementati raccolti tramite un questionario o monitorati
- Elaborazione
  - Metodo completamente **automatico** che combina frequenza, impatto e vulnerabilità.
  - Risultato: valore *rischio reale*
- Valutazione della non conformità
  - *Non-confomity gap = Rischio reale – Rischio ideale*
  - Deviazione maggiore o minore: confrontare la differenza con una soglia.

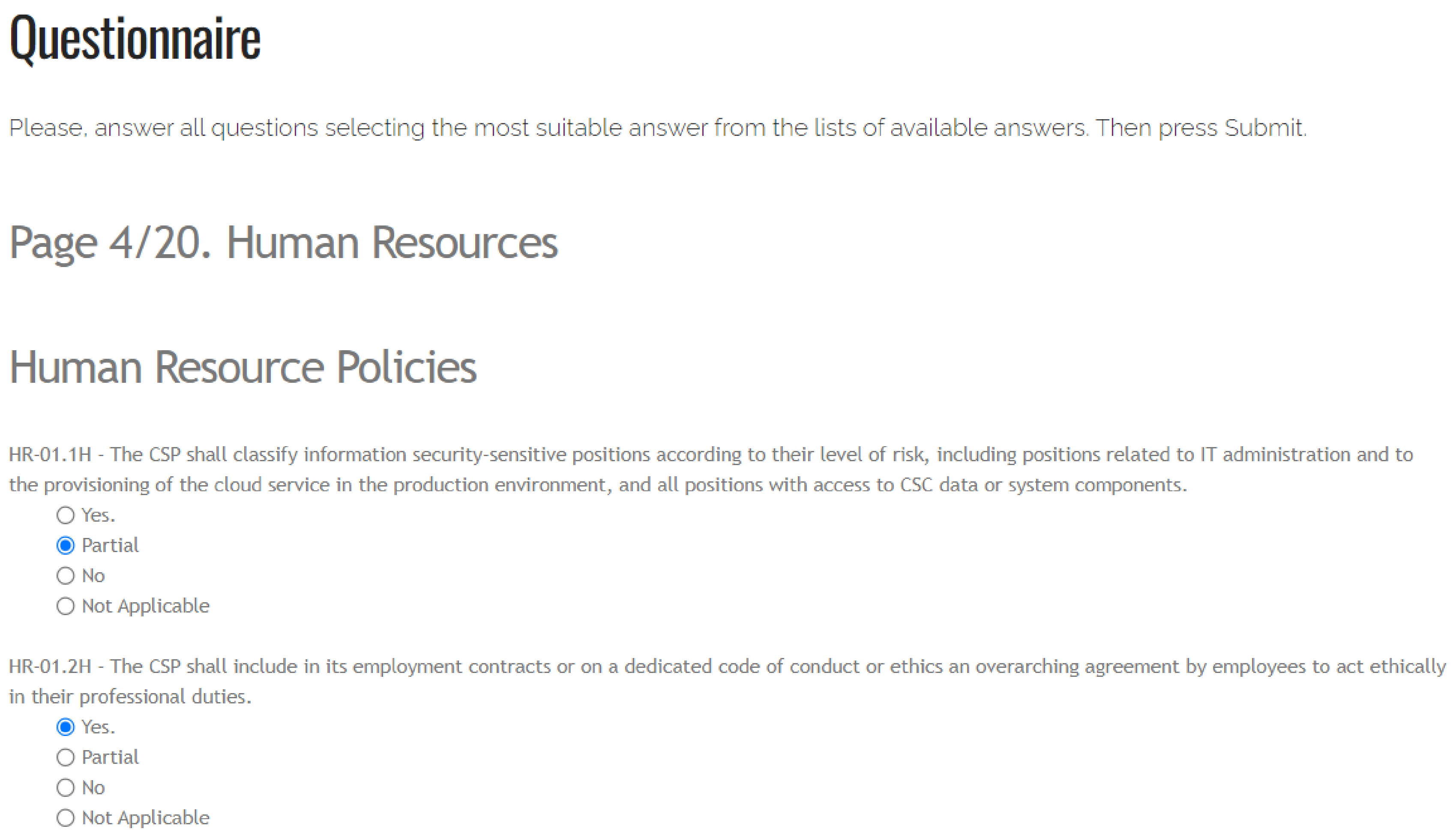
Input. Assets



CLOUD RESOURCE IDENTIFICATION

ID	Cloud Resource	Cloud Resource Type	Number Of Unit	Confidentiality Level	Integrity Level	Availability Level
A1	Insel	Function	1	6	3	3
A2	Insert	Database	1	7	3	3
A3	Insel	Function	1	1	4	3
A4	Insert	Client trust	1	7	3	5
A5	Insel	IoT Device Provisioning Service	1	6	3	3
A6	ImportantVM	Virtual Machine	1	2	3	5
A7	Insel	CI CD Service	1	6	6	3
A8	Insel	CI CD Service	1	6	6	3

Input. Requisiti



Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

Page 4/20. Human Resources

Human Resource Policies

HR-01.1H - The CSP shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the cloud service in the production environment, and all positions with access to CSC data or system components.

- ○ Yes.
- ● Partial
- ○ No
- ○ Not Applicable

HR-01.2H - The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement by employees to act ethically in their professional duties.

- ● Yes.
- ○ Partial
- ○ No
- ○ Not Applicable

Output

Overall Risk:

49.6796/100

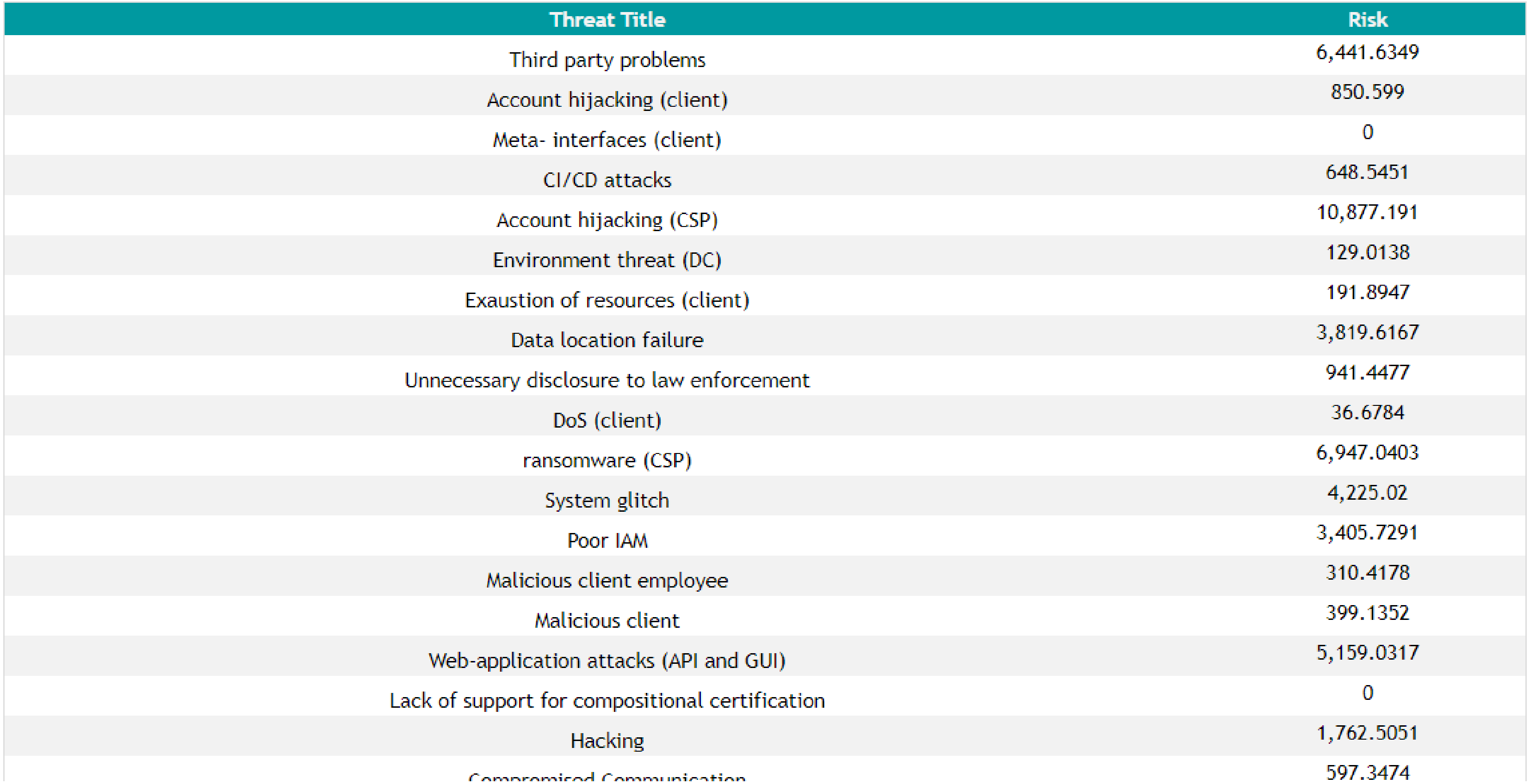
Best

48.9484/100

Non Conformity Gap

0.7312

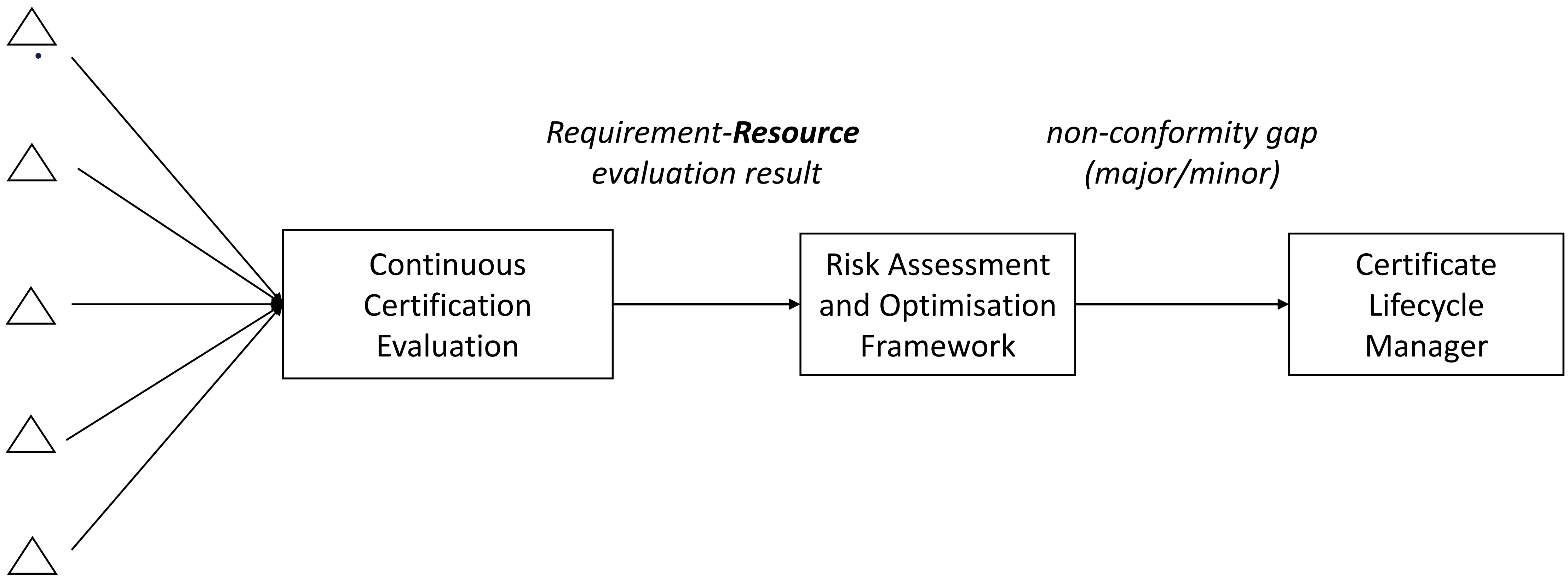
Major



Threat Title	Risk
Third party problems	6,441.6349
Account hijacking (client)	850.599
Meta- interfaces (client)	0
CI/CD attacks	648.5451
Account hijacking (CSP)	10,877.191
Environment threat (DC)	129.0138
Exaustion of resources (client)	191.8947
Data location failure	3,819.6167
Unnecessary disclosure to law enforcement	941.4477
DoS (client)	36.6784
ransomware (CSP)	6,947.0403
System glitch	4,225.02
Poor IAM	3,405.7291
Malicious client employee	310.4178
Malicious client	399.1352
Web-application attacks (API and GUI)	5,159.0317
Lack of support for compositional certification	0
Hacking	1,762.5051
Compromised Communication	597.3474

Certificazione continua

metrics



*Requirement-**Resource** evaluation result*

non-conformity gap (major/minor)

Continuous Certification Evaluation

Risk Assessment and Optimisation Framework

Certificate Lifecycle Manager

Conclusioni

- SATRA è uno strumento per una valutazione del rischio rapida e semplice che può:
  - Valutare i rischi
  - Valutare la conformità (non conformità) con uno standard di sicurezza (EUCS)
  - Sostenere una distribuzione efficace degli sforzi
  - Aiuta a trovare fornitori di sicurezza e consulenti adatti
  - Condurre valutazioni dinamiche/automatiche del rischio e della conformità

  - Aiuta ad aumentare la consapevolezza della sicurezza cyber (specialmente per le PMI)

VALUTAZIONE E MITIGAZIONE DEL RISCHIO DI SICUREZZA CYBER

Artsiom Yautsiukhin

OUTLINE

- Come misurare la sicurezza cyber?
- Valutazione del rischio e termini relativi
- Valutazione del rischio cyber
  - Identificazione del rischio
    - Cyber assets
    - Tipiche minacce cyber
    - Controlli di sicurezza cyber
    - Strumenti e metodi
  - Analisi e ponderazione del rischio
- Trattamento del rischio
- Conclusione

3

COME MISURARE LA SICUREZZA CYBER?

COME MISURARE LA SICUREZZA CYBER?

“If you can’t measure it,
you can’t improve it”
Lord Kelvin

- Obiettivo:
  - Prendere una decisione razionale per migliorare la tua sicurezza cyber.

- I problemi:
  - La decisione deve essere presa per **l'intero** sistema di sicurezza cyber;
  - Sicurezza cyber se molto **eterogenea** (include gestione, politiche, soluzioni tecniche, molteplici piccole opzioni per soluzioni tecnologiche, aspetti fisici e sociali, ecc.)
  - La decisione spetta ai **dirigenti**, non ai tecnici;
  - Le soluzioni di sicurezza (opzioni) sono **costose** e il budget per la sicurezza cyber è **limitato**;
  - Come prendere la decisione **razionalmente**? Quali misure/metriche utilizzare?
  - Anche sistemi IT simili sono **diversi**
  - Il contesto della sicurezza cyber **sta cambiando**

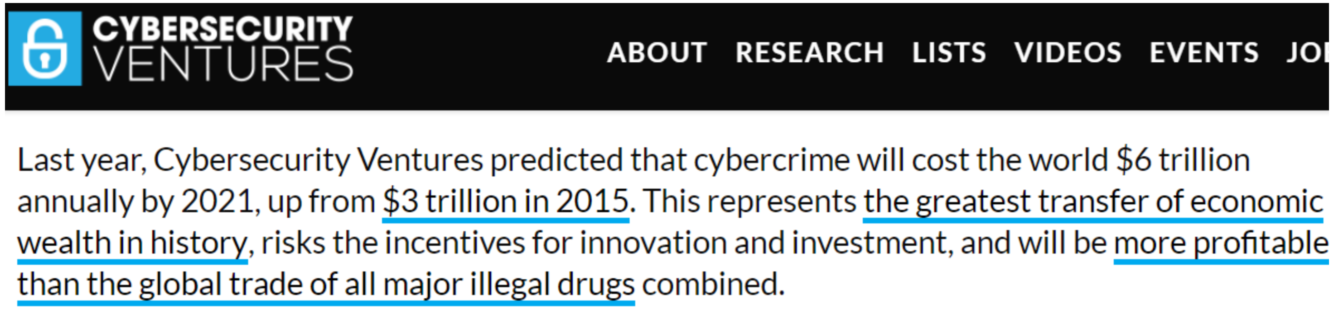
UN APPROCCIO: CONFORMITÀ

- Conformità in poche parole:
  - Un elenco di controlli di sicurezza da implementare viene fornito da qualcuno; ad esempio, da
    - Un dirigente superiore (per le imprese grandi)
    - Un regolatore (ad esempio, per le infrastrutture critiche)
    - Alcuni "standard"
  - È necessario implementare questi controlli
    - Può essere visto come una lista di controllo: un elenco di controlli che devono essere "spuntati".

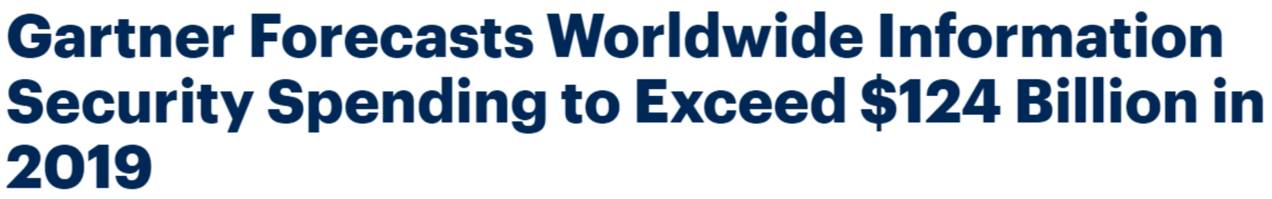
- Pro:
  - Semplice
  - Poca responsabilità
  - Può essere utilizzato per ottenere un certificato (un processo molto più complesso)

- Contro:
  - La necessità di fidarsi della fonte che ha generato la lista di controlli
  - I controlli potrebbero non esserti utili
  - Facile da esagerare (spendi troppo)
  - Come definire un elenco di controlli?

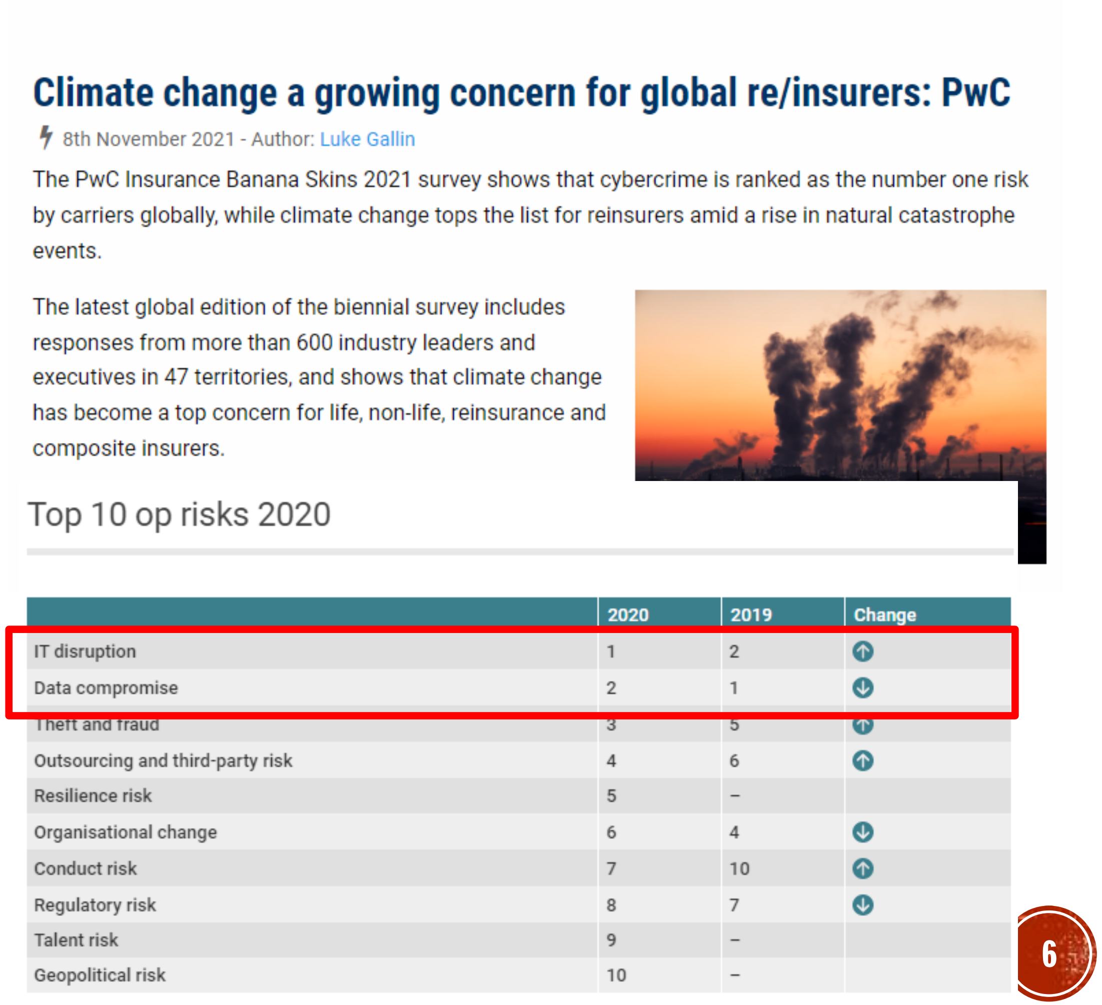
LA SICUREZZA CYBER NON È SOLO UN PROBLEMA TECNICO!



Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.



Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019



Climate change a growing concern for global re/insurers: PwC

8th November 2021 - Author: Luke Gallin

The PwC Insurance Banana Skins 2021 survey shows that cybercrime is ranked as the number one risk by carriers globally, while climate change tops the list for reinsurers amid a rise in natural catastrophe events.

The latest global edition of the biennial survey includes responses from more than 600 industry leaders and executives in 47 territories, and shows that climate change has become a top concern for life, non-life, reinsurance and composite insurers.

Top 10 op risks 2020

	2020	2019	Change
IT disruption	1	2	↑
Data compromise	2	1	↓
Theft and fraud	3	5	↑
Outsourcing and third-party risk	4	6	↑
Resilience risk	5	–	
Organisational change	6	4	↓
Conduct risk	7	10	↑
Regulatory risk	8	7	↓
Talent risk	9	–	
Geopolitical risk	10	–	

ALTERNATIVA: VALUTAZIONE DEL RISCHIO

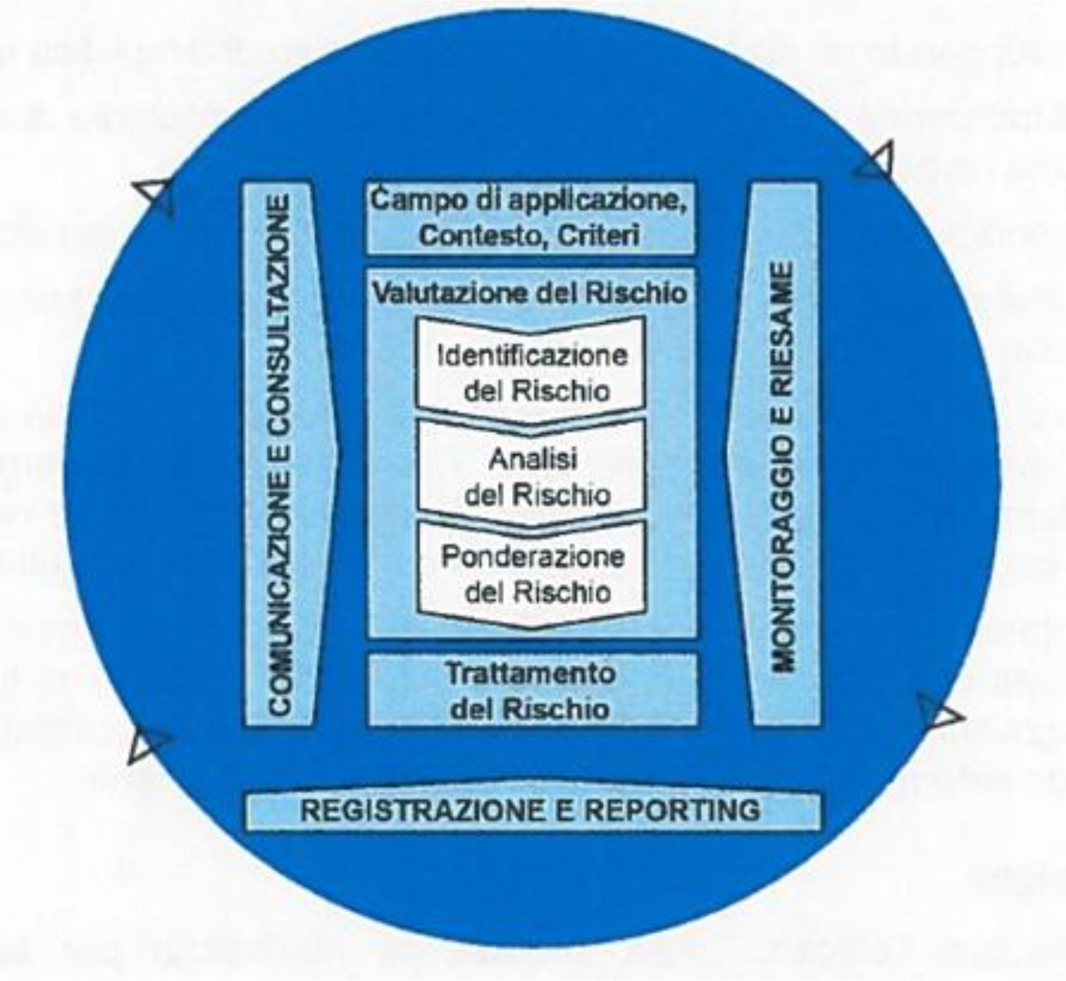
- Valutazione del rischio in poce parole:
  - Soppesa le tue capacità e le tue esigenze, usando
    - Assets principali
    - potenziali minacce
    - Controlli di sicurezza installati
  - Analizza lo stato attuale e i possibili miglioramenti
    - Sei contento dei rischi attuali?
    - Cosa puoi fare per migliorare il tuo livello di rischio
- Pros:
  - Risponde alle **tue** esigenze
  - Ottimizza le decisioni
  - Facile da capire e utilizzare dal gestore
  - Supporta la giustificazione delle decisioni prese
- Cons:
  - Richiede una buona conoscenza (e dati) sulla sicurezza cyber

8

VALUTAZIONE DEL RISCHIO E TERMINI RELATIVI

GESTIONE DEL RISCHIO

- **Gestione del rischio** – attività coordinata per dirigere e controllare un'organizzazione in relazione al rischio [ISO 31000]



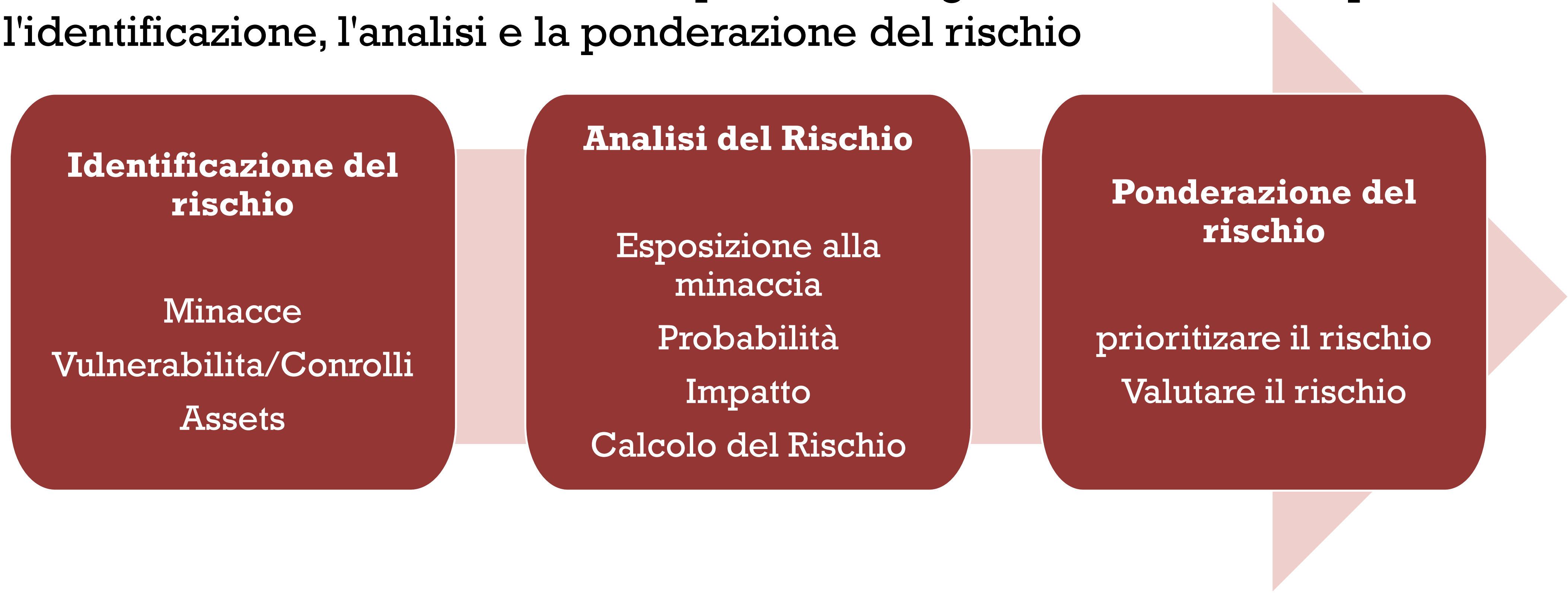
COMUNICAZIONE E CONSULTAZIONE
Campo di applicazione, Contesto, Criteri
Valutazione del Rischio
Identificazione del Rischio
Analisi del Rischio
Ponderazione del Rischio
Trattamento del Rischio
MONITORAGGIO E RIESAME
REGISTRAZIONE E REPORTING

PRINCIPI DI GESTIONE DEL RISCHIO

- Integrato
- Strutturato e completo
- Personalizzato
- Inclusivo
- Dinamico
- Le migliori informazioni disponibili
- Fattori umani e culturali
- Miglioramento continuo

VALUTAZIONE DEL RISCHIO

Valutazione del rischio – un sottoprocesso di gestione del rischio per l'identificazione, l'analisi e la ponderazione del rischio



Identificazione del rischio

Minacce

Vulnerabilita/Conrolli

Assets

Analisi del Rischio

Esposizione alla minaccia

Probabilità

Impatto

Calcolo del Rischio

Ponderazione del rischio

prioritizare il rischio

Valutare il rischio

TRATTAMENTO DEL RISCHIO

- La valutazione del rischio stima il livello attuale del rischio
  - Dove siamo?
- Il trattamento del rischio aiuta a pianificare i passaggi per affrontare i rischi eccessivi
  - Che cosa facciamo?
- L'implementazione di piu o migliori controlli è solo un modo (riduzione del rischio) per trattare i rischi!
  - Trattamento del rischio ≠ più controlli
  - Trattamento del rischio ⊃ più controlli
- I problemi individuati possono (e dovrebbero essere) risolti a livello di rischio, con altri strumenti (inclusi l'evitamento del rischio, il trasferimento del rischio e l'accettazione del rischio).

GESTIONE DELLA SICUREZZA

- In genere, la gestione della sicurezza è maggiormente focalizzata
  - sugli aspetti tecnici
  - sulla riduzione della probabilità del verificarsi di una minaccia
  - sull'aumento della forza della sicurezza.

- Non prende (esplicitamente) in considerazione il possibile impatto.
  - Gestione della sicurezza È governata dalle decisioni di gestione del rischio

- Ma la differenza con la gestione del rischio è sfumata e non è cruciale
  - Alcuni dicono addirittura che la gestione della sicurezza = gestione del rischio

STANDARD DI GESTIONE DEL

- Cyber Risk Management
  - ISO 31000 – Risk management – Guidelines
  - **ISO 27001 – Information security management systems — Requirements**
  - NIST 800-37 – Risk Management Framework for Information Systems and Organizations
- Cybersecurity framework
  - **NIST Cybersecurity Framework**
  - Framework Nazionale per la Cybersecurity e la Data Protection [Ital
- Cyber Risk Assessment
  - ISO 27005 – Information security risk assessment
  - NIST 800-30 – Guide for Conducting Risk Assessments
  - Other risk management methodologies:
    - CIS RAM, OCTAVE, Magerit, Mehari, Microsoft, etc.
- Control lists:
  - ISO 27002 – Code of practice for information security controls
  - NIST 800-53 - Security and Privacy Controls
  - CIS Controls

15

VALUTAZIONE DEL RISCHIO CYBER

VALUTAZIONE DEL RISCHIO CYBER

- La valutazione del rischio è uno strumento **universale** per la gestione di qualsiasi tipo di rischio
- Allora, cos'è la valutazione del rischio **cyber**?
  - È l'applicazione del processo di valutazione del rischio universale al dominio cyber, tenendo conto delle peculiarità dell'ambiente cyber.
    - Come definire l'ambito del sistema di sicurezza cyber?
    - Quali sono le tipiche cyber assets?
    - Quali minacce sono tipiche dei rischi cyber?
    - Quali sono i controlli di sicurezza cyber?
    - Come stimare l'impatto?
    - Come stimare le probabilità e l'esposizione?

TIPICO PROCESSO DI VALUTAZIONE DEL RISCHIO

- Definizione del contesto
- Identificazione del rischio
  - Assets
  - Minacce
  - Controlli/vulnerabilita
- Stima/analisi del rischio
  - Impatto
  - Esposizione
  - Probabilità
  - Calcolo del rischio
- Ponderazione del rischio
  - Prioritizzazione del rischio
  - Ponderazione del rischio

DEFINIZIONE DEL CONTESTO. CONTESTO

- È necessario comprendere l'ambiente in cui opera il sistema IT e quanto influisce sulla valutazione del rischio

- In particolare, devono essere presi in considerazione i seguenti punti:
  - Obiettivi, strategie e politiche aziendali delle organizzazioni
  - Processo, funzione e struttura aziendale
  - Requisiti legali, normativi e contrattuali
  - L'approccio generale dell'organizzazione alla gestione del rischio
  - Posizione geografica
  - Aspettative degli stakeholder
  - Posizione e ambiente socio-culturale

DEFINIZIONE DEL CONTESTO. SCOPO E CONFINI

- Scopo
  - assicura che tutte le assets pertinenti siano prese in considerazione durante la valutazione del rischio.
- Confini
  - aiuta a concentrarsi sulle minacce che potrebbero penetrare attraverso i confini.
- Nel contesto cyber, è importante prestare particolare attenzione all'ambito e ai confini a causa della natura distribuita dei sistemi IT:
  - Il servizio cloud rientra nei tuoi confini o no?
  - Le assets sui dispositivi connessi dall'esterno della rete devono rientrare nell'ambito della valutazione?
  - Le assets sui dispositivi mobili connessi alla rete devono essere incluse nell'ambito?

DEFINIZIONE DEL CONTESTO. CRITERI

- Criteri di valutazione del rischio
  - Questi sono i criteri per valutare i rischi di sicurezza cyber, che includono:
    - Importanza strategica dei processi aziendali esistenti
    - Sensibilità degli asset cyber
    - Obblighi legali, regolamentari e contrattuali
    - In che modo la riservatezza, l'integrità e la disponibilità delle risorse cyber influiscono sui processi aziendali
    - Aspettativa degli stakeholder e valore della fiducia e della reputazione.
- Criteri di impatto
  - Questi i criteri per valutare l'eventuale perdita:
    - Violazioni (perdita di riservatezza, integrità, disponibilità)
    - Operazioni sospese
    - Scadenze mancate
    - Perdita finanziaria (compresa la perdita di opportunità commerciali)
    - Perdita di reputazione
    - Incapacità di adempiere ai requisiti legali, regolamentari e contrattuali

- Criteri di accettazione del rischio
  - Questi criteri definiscono quali livelli di rischio sono accettati
  - Potrebbe avere diversi livelli
  - Potrebbe essere diverso per diversi rischi
  - Potrebbe dipendere dal profitto atteso

IDENTIFICAZIONE DEL RISCHIO

IDENTIFICAZIONE DEL RISCHIO. CYBER ASSETS

- Peculiarità nell'identificazione degli asset cyber
  - Le cyber assets potrebbero essere difficili da assegnare a un oggetto fisico (ad esempio, i dati del cliente sono archiviati su un server), perché sono facili da copiare, modificare e scambiare (ad esempio, comunicati tramite Intranet/Internet, elaborati su un desktop; backup su un NAS o cloud, ecc.).
  - Le cyber assets sono difficili da monitorare. Potrebbero essere copiati su cyber risorses diverse. Potrebbero essere elaborati e trasformati in una risorsa diversa (ad es. analisi o registri).
  - Non è banale identificare ed elencare tutti le cyber assets. Spesso il valore delle cyber assets è troppo minato (ad esempio, informazioni di identificazione personale, come posizione o e-mail).
  - Alcuni cyber asset sono molto importanti, ma non provocano perdite immediate o definitive. Esempio: credenziali.
  - Esistono modi non standard (a volte innovativi) per gli aggressori di abusare delle vostre assets o usarle per attaccare gli altri. Ad esempio, cryptojacking, botnet o attacchi alla supply chain.
  - Le assets potrebbero dipendere l'una dall'altra (ad esempio, i dati sono necessari per eseguire un processo aziendale)

IDENTIFICAZIONE DEL RISCHIO. CYB ASSETS

- Logico
  - Processi di business
  - Informazione
    - informazioni di identificazione personale,
    - informazioni sulla salute personale,
    - informazioni finanziarie
    - Competenza
    - Informazioni strategiche aziendali
    - Informazioni rilevanti per l'attività
  - Credenziali
  - Codice sorgente

- Contenitrici
  - Banche dati
  - File
  - Applicazioni
  - Comunicazione
  - E-mail
  - L'ambiente del sviluppo
  - Servizio web/sito web

- Fisico
  - server
  - Rete
  - Personale
  - IoT, dispositivo mobile
  - Desktop
  - Supporti (CD, NAS, ecc.)
  - Cloud
  - Carta

IDENTIFICAZIONE DEL RISCHIO. MINACCE

- Le minacce cyber sono, in gran parte, intenzionali. Il che significa che combattiamo contro altri umani:
  - Adattabile
  - Inventivo
  - Collaborativo
  - Pianificante
  - Paziente
  - Potrebbe essere persistente
- Le minacce cyber sono eterogenee e dinamiche
  - Compaiono nuove minacce
  - Le minacce esistenti si evolvono
  - Riappaiono vecchie minacce.

IDENTIFICAZIONE DEL RISCHIO. MINACCE

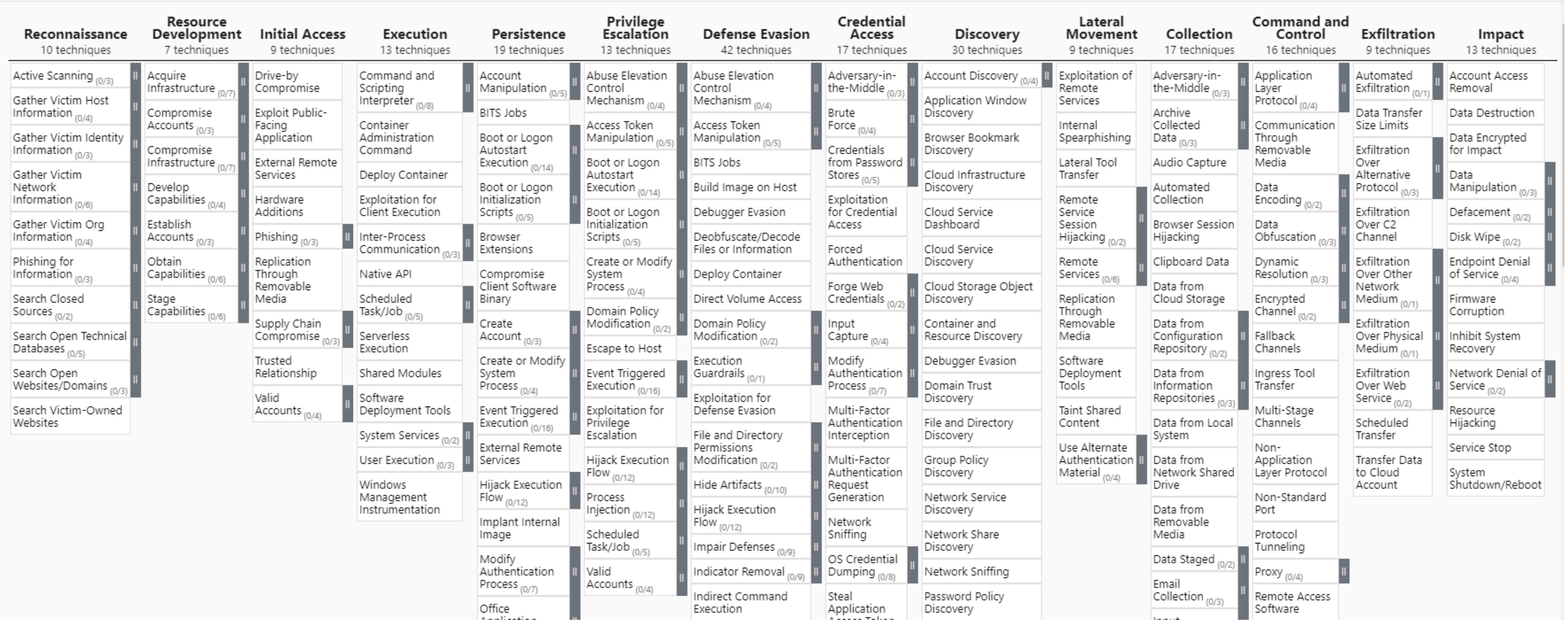
- Gli attacchi cyber spesso richiedono diversi passaggi per ottenere il risultato.
  - Un utente apre un'e-mail fraudolenta con un virus allegato.
  - Un virus viene eseguito sul dispositivo di una vittima. È installata una backdoor
  - Un attaccante ottiene l'accesso al sistema ed esegue un exploit per ottenere un accesso di livello superiore
  - E…
    - Rubare dati?
    - Implementare un bot? criptojacker?
    - Ottenere l'accesso a un server?
    - Piantare un ransomware?

- Vengono utilizzate diverse vulnerabilità
- Si verificano diverse minacce
- L'esito finale (impatto) è incerto.

IDENTIFICAZIONE DEL RISCHIO. SCENARI

- Una possibile soluzione: definire gli scenari.
- Uno scenario è un modo specifico per attaccare un sistema e ottenere determinati risultati. Aiuta a chiarire:
  - Chi è l'aggressore
  - Quali vulnerabilità vengono sfruttate
  - Qual è l'impatto previsto.
- In questo caso è possibile capire
  - Quali controlli possono impedirlo
  - Quale assets sono interessati e in che modo l`attackante gli puo compromettere.
- Ma
  - C'è (quasi) una quantità infinita di scenari
  - Non ci sono (quasi) statistiche disponibili per gli scenari
  - La maggior parte dei dati statistici disponibili si concentrano sulle minacce.

MITTRE ATT&CK MATRIX



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information
Search Closed Sources (0/2)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion
			User Execution (0/3)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (0/4)	Hide Artifacts (0/10)
				Office		Hijack Execution Flow (0/12)
						Impair Defenses (0/9)
						Indicator Removal (0/9)
						Indirect Command Execution

Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Modify Authentication Process (0/7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Application	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
	Network Share Discovery		Email Collection (0/3)	Remote Access Software		
	Network Sniffing		Input			
	Password Policy Discovery					

IDENTIFICAZIONE DEL RISCHIO. ATTACCANTI

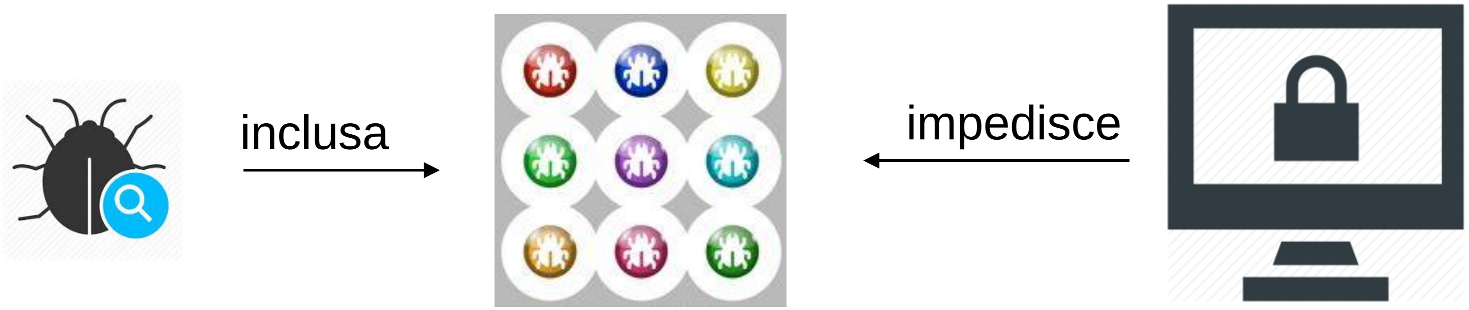
- Attaccante esterno
  - Criminale cyber
  - Cyber terrorista / nazione sponsorizzata
  - Virus/worm
  - Hacktivista
  - Spia industriale
- Attaccante interno
  - Abusatore
  - Hacker
- Cliente malizioso
- Attaccante fisico
- Fornitore
- Utente negligente
- Fallimenti
- Ambiente
  - Locali (inquinamento, riscaldamento, ecc.)
  - Globali (terremoto, alluvione, ecc.)

IDENTIFICAZIONE DEL RISCHIO. MINACCE

- Gli attaccanti possono essere caratterizzati da
  - Obiettivi
  - Capacità
  - Bersaglio
- Gli attaccanti eseguono le loro attività attraverso minacce o scenari
- Per riassumere: un attaccante esegue una minaccia/scenario specifico per sfruttare le vulnerabilità del sistema per realizzare il suo obiettivo compromettendo asset specifici (bersaglio)
  - Una **minaccia/scenario** definisce/lega le **vulnerabilità** da sfuttare e le **assets** da compromettere

VULNERABILITÀ VS CONTROLLI DI SICUREZZA

- Semplificazione dell'identificazione delle vulnerabilità:
  - Mancanza di controlli di sicurezza = una vulnerabilità



Bug specifico

Basso livello
Tecnico
Difficile ragionare

Tipo di bug

Alto livello
Generico
Ragionamento più semplice

Controllo di sicurezza

“Facile” da identificare
Generico
Elencato negli standard
(ISO 27002, CSF, CIS)

TIPICHE MINACCE CYBER

VIRUS, WORM AND RANSOMWARE

- **Virus** e **worm** sono programmi dannosi che possono modificare il funzionamento e il comportamento del computer. Virus e worm hanno meccanismi di propagazione diversi.
  - Virus. Un utente dovrebbe consentire l'esecuzione di un virus. Per esempio,
    - Aprire un allegato di posta dannoso
    - Consentire l'installazione di un programma infetto
    - Scaricare ed esegui un file infetto
  - Il worm si propaga autonomamente sfruttando le vulnerabilità nei servizi di rete.
- Il **ransomware** è un malware che crittografa i dati del computer compromesso, rendendo inutilizzabili i file e il sistema. Di solito, dopo viene richiesto un riscatto all'utente.
  - Distribuito in modi diversi, inclusi virus e worm, ma può anche essere installato da un utente malintenzionato che dispone di diritti di accesso sufficienti sul computer.

ATTACCHI BASATI SUL WEB ATTACCHI ALLE APPLICAZIONI WEB

- **Attacchi alle applicazioni Web**: un'ampia gamma di attacchi volti a sfruttare le vulnerabilità nella GUI e nelle API del servizio (ad esempio, attacchi SQL injection, Cross-Site scripting XSS). Mira a compromettere le applicazioni web.

- **Attacco basato sul Web**: un'ampia serie di attacchi durante i quali gli aggressori sfruttano le vulnerabilità nella codifica per ottenere l'accesso a un server o un computer. Mira a compromettere un sistema connesso a Internet.

ATTACCHI ALLA COMUNICAZIONE D(DOS)

- **Attacco alla comunicazione**: questa minaccia mira a intercettare o manomettere la comunicazione tra una vittima. L'attaccante può trovare un modo per decifrare la comunicazione (con crittografia assente o debole) o sfruttare le vulnerabilità dei protocolli non sicuri
  - Man in the middle attacca: un utente malintenzionato interrompe la comunicazione tra due vittime e costringe il traffico a fluire attraverso di lui, con la possibilità di leggere o modificare la comunicazione.

- **(D)DoS**: la minaccia Denial of Service mira a bombardare il servizio selezionato con un'enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi
  - (Distribuito) Denial of Service utilizza una moltitudine di fonti (bot) che inviano richieste al servizio.

ATTACCHI DI INGEGNERIA SOCIALE. ATTACCHI FISICI

- **Ingegneria sociale**: è una serie di minacce che mirano a manipolare, influenzare e ingannare una vittima al fine di indurla ad agire in un certo modo (ad esempio, concedere l'accesso a un sistema cyber, condividere informazioni segrete o credenziali).
  - *Phishing*: una tipica minaccia di ingegneria sociale che comunica con un utente tramite e-mail, messenger o altri mezzi di comunicazione.
  - Gli attacchi di ingegneria sociale richiedevano la presenza fisica
    - *Shoulder surfing*: sbirciare la digitazione della password
    - *Dumpster diving*: cercare le password nella lettiera
    - *USB drop*: lasciare che una chiavetta USB infetta venga prelevata e utilizzata da un dipendente
- **Attacchi fisici**: danni intenzionali all'hardware causati da aggressori (interni o esterni)
- **Manomissione**: modifica fisica di un hardware per alterarne la funzionalità o ottenere l'accesso alla rete.

INSIDER PARTNER/FORNITORE

- **Abuser**: un dipendente utilizza i propri diritti di accesso per compromettere il sistema. Per esempio, copiare i dati all'esterno della sede dell'azienda.

- **Insider hacker**: un utente malintenzionato che beneficia dell'accesso iniziale al sistema ma mira ad aumentare i propri privilegi compromettendo il sistema.

- **Ex dipendente** – un ex dipendente, che utilizza la propria conoscenza del sistema, credenziali ancora valide e/o backdoor precedentemente installate per comprometterlo.

- **Partner** – un partner che attacca il sistema, usando i suoi privilegi nel tuo sistema
  - Un partner potrebbe essere compromesso. L'hacker può mirare ad attaccare il tuo partner per usarlo come punto d'appoggio per attaccarti: attacco alla catena di approvvigionamento.

CLIENTE DANNOSO

- **Cliente dannoso**: un client che utilizza i servizi acquistati per lanciare un attacco a te o ai tuoi clienti

- **Cliente illegale**: un cliente che utilizza il tuo servizio per scopi illegali (ad esempio, inviare spam, ospitare contenuti illegali, fornire servizi dannosi, ecc.).

NEGLIGENZA DEL DIPENDENTE

- **Perdita o furto dell'hardware**: una minaccia correlata alla perdita fisica di un hardware. Questa minaccia in genere si traduce in una potenziale perdita di informazioni sensibili contenute su un dispositivo mobile (ad esempio, laptop o cellulare).
- **Danni fisici accidentali**: un'azione accidentale di un dipendente che causa danni fisici all'hardware. Ad esempio, caffè versato su un laptop.
- **Errore logico accidentale**: un errore accidentale o un'azione benigna che porta a compromettere il sistema. Un errore tipico è la condivisione di dati sensibili (ad esempio, concedendo l'accesso a dati sensibili al pubblico o condividendo informazioni senza sapere che sono private).

MINACCE AMBIENTALI GUASTI

- **Locale** – minacce ambientali che colpiscono solo la rete dell'impresa (inquinamento, riscaldamento, acqua, fuoco, polvere, impulsi elettromagnetici, ecc.)

- **Globale** – eventi naturali che danneggiano una vasta area (terremoto, alluvione, attività vulcanica, ecc.)

- **Glitch del sistema**: un errore accidentale nel funzionamento del sistema IT, che causa danni.

- **Guasto meccanico** - guasto meccanico che causa danni.

CONTROLLI DI SICUREZZA

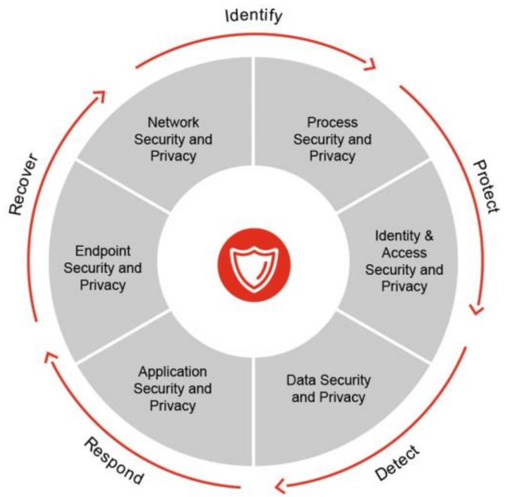
CONTROLLI DI SICUREZZA. ISO 27002 VS CSF

ISO

- Organizzazione
- Politiche
- Gestione delle assets
- Conformità
- Rapporti con i fornitori
- Protezione fisica e ambientale
- Risorse umane
- Controllo di accesso
- Crittografia
- Sicurezza della comunicazione
- Sicurezza operativa,
- Acquisizione, sviluppo e manutenzione del sistema
- Gestione degli incidenti
- Business continuity

NIST CSF

- Identificare
  - Gestione delle Asset, Organizzazione, Policy, Rapporti con i fornitori, Compliance
- Proteggere
  - Protezione fisica e ambientale, Risorse umane, Controllo degli accessi, Sicurezza delle operazioni, Crittografia, Sicurezza delle comunicazioni, Acquisizione, sviluppo e manutenzione del sistema
- Rilevare
  - Protezione del sistema
- Rispondere
  - Gestione degli incidenti
  - Business continuity
- Recuperare
  - Gestione degli incidenti


Identify
Protect
Detect
Respond
Recover
Network Security and Privacy
Process Security and Privacy
Identity & Access Security and Privacy
Data Security and Privacy
Application Security and Privacy
Endpoint Security and Privacy

POLITICHE

- Un insieme di politiche per la sicurezza cyber dovrebbe essere:
  - Definito
  - Approvato (dalla direzione)
  - Pubblicato
  - Comunicato ai dipendenti e ai soggetti esterni
  - Revisionato regolarmente

ORGANIZZAZIONE

- Definire ruoli e responsabilità
- Stabilire contatti con le autorità
- Definire le politiche per l'uso dei dispositivi mobili e il telelavoro

RISORSE UMANE

- Eseguire lo screening dei candidati
- Definire contrattualmente termini e condizioni in materia di sicurezza cyber
- Rendere la gestione per garantire che le politiche di sicurezza siano seguite
- Formare e formare i dipendenti
- Istituire un processo disciplinare
- Assicurarsi che la procedura di risoluzione del contratto includa le azioni di sicurezza richieste

GESTIONE DELLE ASSETS

- Creare, mantenere e aggiornare l'inventario delle risorse
- Definire il proprietario delle risorse
- Classificare le risorse
- Gestire supporti rimovibili
- Smaltimento sicuro dei supporti
- Transizione sicura dei supporti fisici

CONTROLLO DI ACCESSO

- Definisci criteri per il controllo degli accessi (in particolare, l'accesso alla tua rete IT)
- Definire come registrare e annullare un utente
- Definire formalmente in che modo viene concesso o revocato l'accesso
- Gestione speciale dei diritti di accesso privilegiato
- Specificare un processo di gestione formale per la gestione delle informazioni di autenticazione segrete e assicurarsi che gli utenti lo seguano.
- Definire le regole formali per la rimozione o la modifica dei diritti di accesso
- Assicurarsi che l'accesso sia concesso in base alle politiche di controllo degli accessi
- Stabilire procedure di accesso sicure e sistemi di gestione delle password
- Limitare l'accesso al codice sorgente.

CRITTOGRAFIA

- Definire i criteri per l'utilizzo dei controlli crittografici
- Definire le politiche per la gestione delle chiavi
  - Come usare
  - Come proteggere
  - Durata delle chiavi crittografiche

PROTEZIONE FISICA E AMBIENTALE

- Stabilire e proteggere il perimetro fisico
- Stabilire controlli fisici
  - Uffici sicuri e altre strutture
- Stabilire procedure per lavorare in aree sicure
- Definire e implementare le procedure per la consegna e il carico
- Implementare protezioni contro disastri naturali, attacchi e incidenti dannosi.
- Proteggere e mantenere apparecchiature, utenze, cavi, ecc.
- Definire e seguire le procedure per lo smaltimento e la rimozione delle apparecchiature.
- Definire politice clear desk e clear screen.

SICUREZZA DELLE OPERAZIONI

- Definire le procedure operative e le responsabilità
- Implementa la protezione da malware
- Implementare procedure di backup
- Implementare procedure di registrazione e monitoraggio
- Procedure definite per l'installazione di un software
- Implementare le procedure di gestione delle vulnerabilità
- Pianificare le attività di audit

SICUREZZA DELLA COMUNICAZIONE

- Definire le procedure di gestione per il controllo della rete
- Implementare e mantenere i meccanismi di sicurezza della rete (ad es. firewall, IDS/IPS, ecc.)
- Segregare le reti (se necessario).
- Definire come e quali informazioni possono essere trasferite
- Definire le regole per la messaggistica elettronica
- Definire i requisiti per gli accordi di riservatezza e non divulgazione per lo scambio di informazioni.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA

- Definire e implementare i requisiti di sicurezza per i nuovi sistemi informativi (in particolare, come le applicazioni scambiano informazioni nelle reti pubbliche)
- Definire regole per uno sviluppo sicuro
- Definire e implementare il controllo sulle modifiche ai sistemi
- Utilizzare i principi di ingegneria del sistema sicuro
- Ambiente di sviluppo sicuro
- Definire le regole per lo sviluppo in outsourcing
- Utilizzare i test di sicurezza e di accettazione del sistema

RAPPORTI CON I FORNITORI

- Definire le politiche di sicurezza per i fornitori

- Garantire che i requisiti di sicurezza siano negoziati, concordati e rispettati dal fornitore

- Rivedere e monitorare l'adempimento dei requisiti di sicurezza da parte del fornitore.

GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

- Definire le responsabilità e le procedure per la risposta all'incidenza e garantire la loro esecuzione
- Stabilire procedure di segnalazione per eventi e debolezze
- Garantire che gli eventi di sicurezza vengano analizzati e valutati.
- Garantire l'esecuzione delle procedure per la risposta agli incidenti
- Analizzare gli eventi accaduti e applicare azioni per riduzione dei rischi simili in futuro
- Memorizza le informazioni sugli eventi verificatisi.

BUSINESS CONTINUITY

- Definire i requisiti per, pianificare, implementare, rivedere le procedure di continuità operativa.

CONFORMITÀ

- Identificare le legislazioni e gli accordi contrattuali necessari per conformarsi
- Identificare i diritti di proprietà intellettuale e proteggerli
- Proteggi i dati di terze parti in conformità con la legge (ad es. GDPR)
- Seguire le normative sui controlli crittografici

AUDIT

- Organizza una revisione indipendente del tuo sistema di sicurezza cyber
- Garantire la conformità con le politiche o gli standard di sicurezza

STRUMENTI E METODI

RICERCA DESKTOP

- Analisi dei documenti aziendali
  - Strategia aziendale, Strategia aziendale, Diagrammi di flusso, Assegnazione ruoli,…
  - Raporti di valutazione del rischi precedenti
  - Inventario delle risorse
  - Analisi dei log, analisi degli eventi passati, report (compresi i report di audit)...
  - Rapporti sulla scansione delle vulnerabilità (Nessus, OpenVas)
- Fonti esterne
  - Analisi statistiche (ENISA, IBM/Ponemon, Verizon, Accenture, NetDilligence, McAffee, Semantec, Deloitte, PwC, ecc…)
  - Rapporti, bollettini dei centri di condivisione delle informazioni (ad es. CERT, ISACs).
- Aggregazione di fonti diversi:
  - Valore medio
  - Weighted function:
    - $X = \sum_{\forall i} w_i \times x_i$

PARLARE CON LA GENTE

- **Interviste**: discussioni individuali con le principali parti interessate sullo stato attuale della pratica (responsabili della sicurezza, risorse umane, proprietari delle risorse, ecc.)
- **Workshop**: discussioni di gruppo con le persone coinvolte nella valutazione del rischio
- **Metodo Delphi** : un metodo di previsione sistematico e interattivo che si basa sull'opinione presa in considerazione di diversi esperti
  - Gli esperti rispondono a un questionario (fornendo spiegazioni)
  - Le risposte sono segnalate in forma anonima ad altri (con spiegazioni)
  - Gli esperti rispondono nuovamente al questionario (correggendo le risposte)
  - Fermati a un criterio predefinito (ad esempio, numero fisso di giri) e viene utilizzato il punteggio medio o medina.

AGGREGAZIONE DI DATI DAI FONTI DIVERSI:

- Mediana

  {2,4,**5**,8,8}

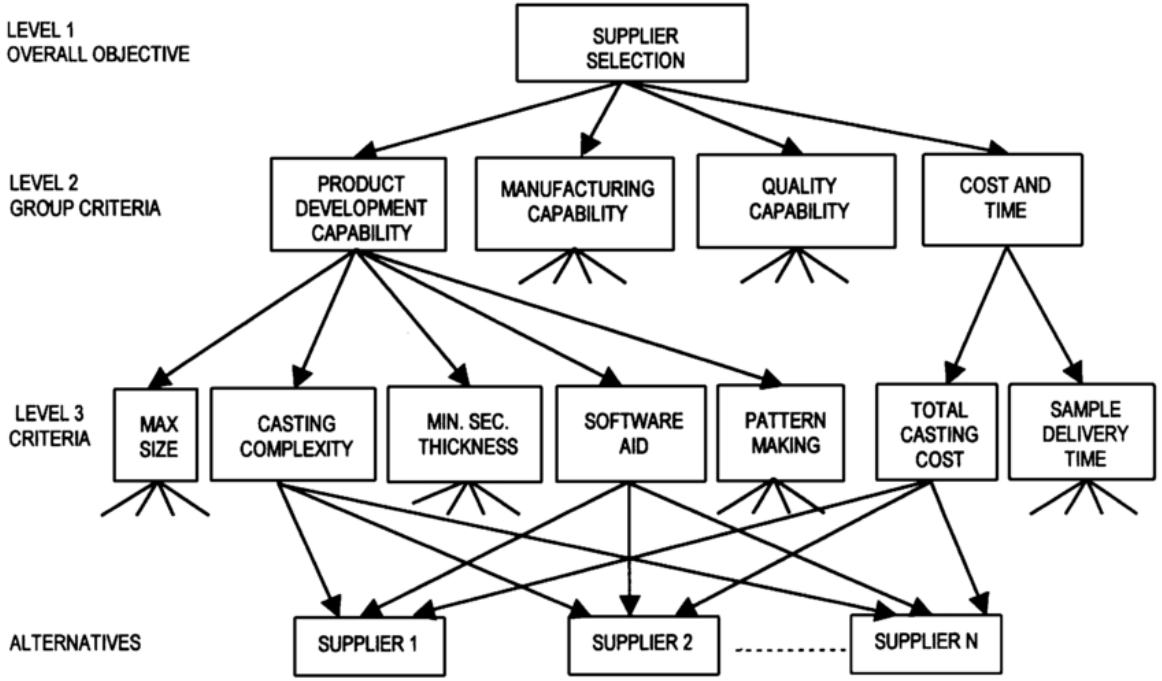
- Valore medio

$$X = \frac{1}{n}\sum_{i=1}^{n} x_i$$

- Weighted function:

$$X = \sum_{\forall i} w_i \times x_i$$

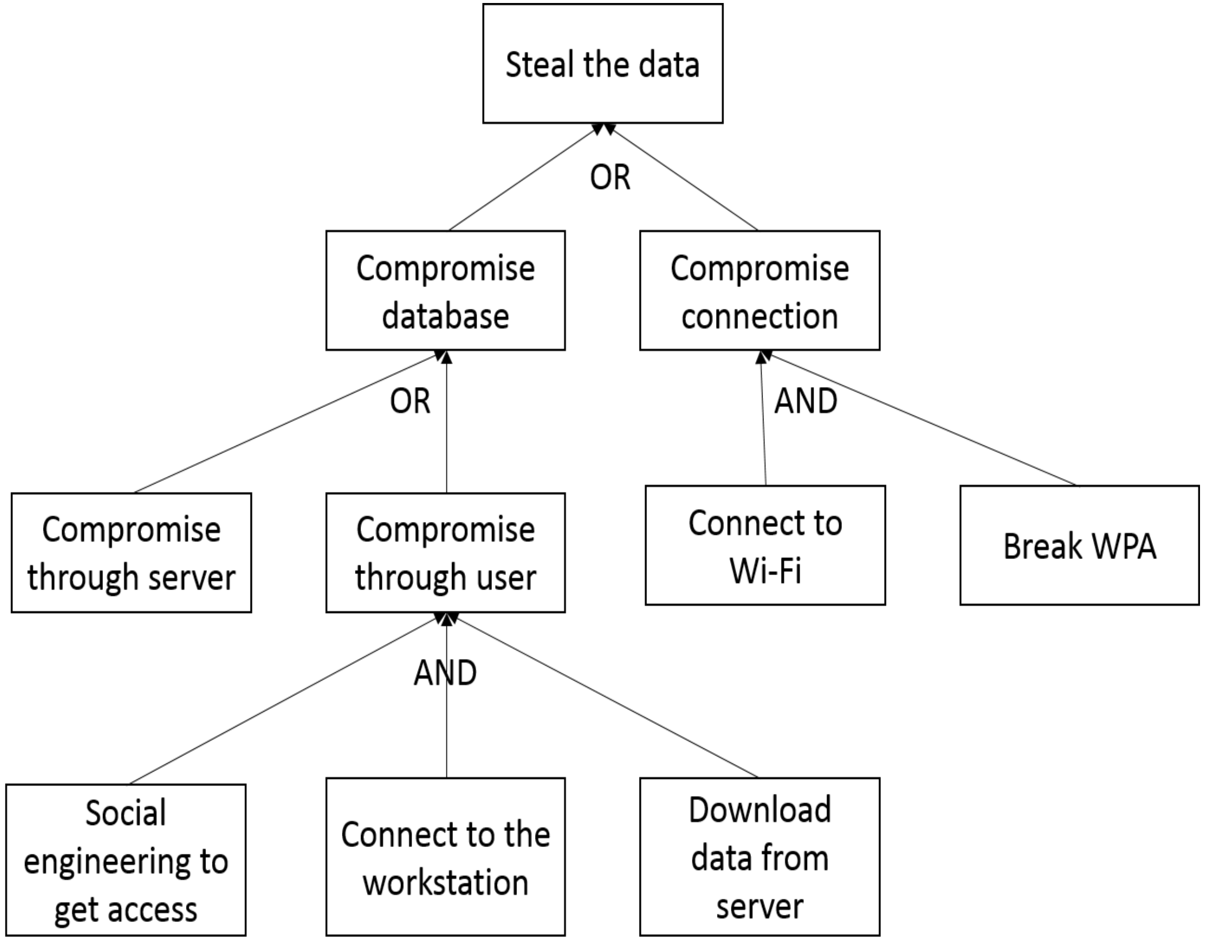
- Analytic Hierarchy Process (AHP)



ATTACK TREE

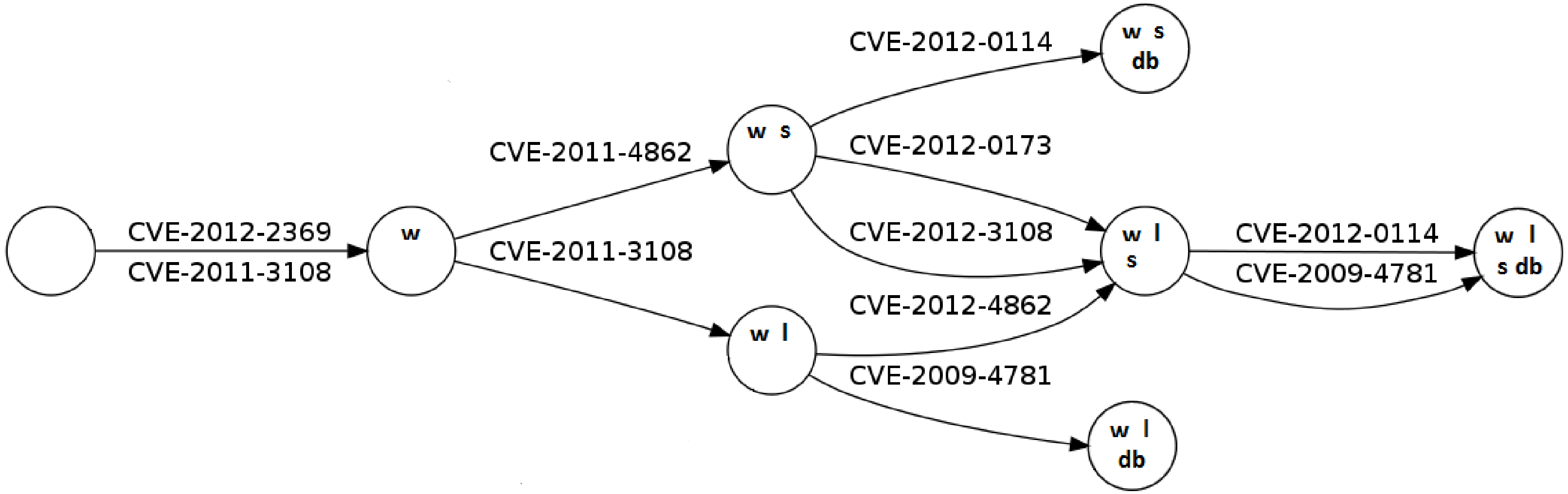
- Attach tree è una tecnica utile per un modo strutturato per analizzare e dettagliare le minacce

- Inizia con una possibile conseguenza indesiderata (nodo superiore)
- Suddividilo usando gli operatori AND e OR in passaggi più dettagliati
- Ripetere fino a raggiungere il livello di dettaglio richiesto.



ATTACK GRAPH

- Attack graph è una tecnica che mira a rappresentare tutti i percorsi (una sequenza di vulnerabilità esistenti da sfruttare) attraverso un sistema che un utente malintenzionato può seguire per raggiungere il suo obiettivo finale.
- Dopo la scansione delle vulnerabilità, lo strumento di creazione del attack graph li collega in un grafico basato sulle condizioni pre e post per ogni vulnerabilità rilevat



ANALISI E PONDERAZIONEDEL RISCHIO

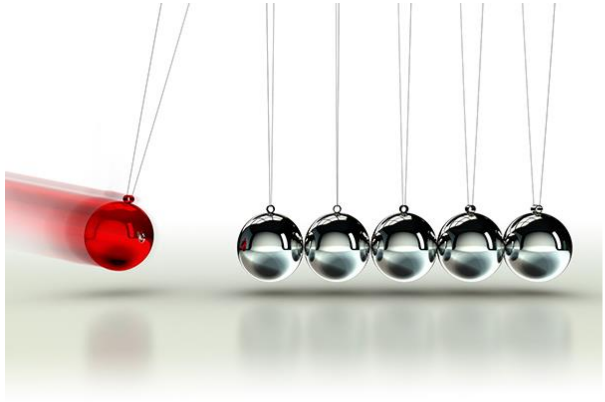
ANALISI DEL RISCHIO QUANTITATIVA O QUALITATIVA

- Quantitativo
  - Funziona con valori reali!
  - Le operazioni sui valori sono definite.
  - Fornire risultati monetari (adatti per ulteriori analisi e riutilizzo)
  - Difficile da usare
- Perdita – misurata in euro [dollari, tugrik, ecc.]
- Likelihood: valore reale positivo

- Qualitativo
  - Facile da applicare
  - Ampiamente usato
  - Ha bisogno della definizione di valore
  - Necessita della definizione delle operazioni
- Perdita – {very low, low, medium, high, very high}
- Likelihood – {very low, low, medium, high, very high}

ANALISI DEL RISCHIO. IMPATTO

- Una risorsa compromessa provoca la perdita.
  - L'impatto è stimato come una perdita attesa da un singolo evento di minaccia
- Tenere in considerazione:
  - Interruzione delle attività business
  - Perdita diretta
  - Violazione di una normativa
  - Violazione di un contratto
  - Perdita di reputazione
  - Perdita del cliente
  - Costo della notifica
  - Impatto sul personale/utente
  - Indagine/recupero perdita
  - Perdita di vantaggio competitivo
- Non dimenticare la dipendenza dalle risorse!



ANALISI DEL RISCHIO. IMPATTO

- Dal punto di vista della sicurezza è importante valutare le perdite dovute all'impatto su uno specifico aspetto della sicurezza:
  - Confidenzialità
  - Integrità
  - Disponibilità
- Potrebbe anche essere aggiunto
  - Responsabilità (non ripudio)

ANALISI DEL RISCHIO. LIKELIHOOD

- Likelihood = Esposizione × Probabilità[Successo]
  - Fonti di minaccia e contesto organizzativo
  - Controlli e vulnerabilità
  - Esperienza e statistiche

- L'esposizione è prevalentemente esterna
  - Interessato dalle tendenze globali e dal tipo di organizzazione
- La probabilità è per lo più interna
  - Colpito dalla tua protezione

STIMA DEL RISCHIO. CALCOLARE

- Formula generale:
  - Rischio = Likelihood × Perdita

- Minacce multiple (t) e assets (a):
  - Per asset: $Rischio_{CIA}^{a} = \sum_{\forall\, t} Likelihood^{t} \times Impact_{CIA}^{a}$
  - Per minaccia: $Rischio_{CIA}^{t} = \sum_{\forall\, a} Likelihood^{t} \times Impact_{CIA}^{a}$

RISK ESTIMATION. COMPUTE RISK. QUALITATIVE

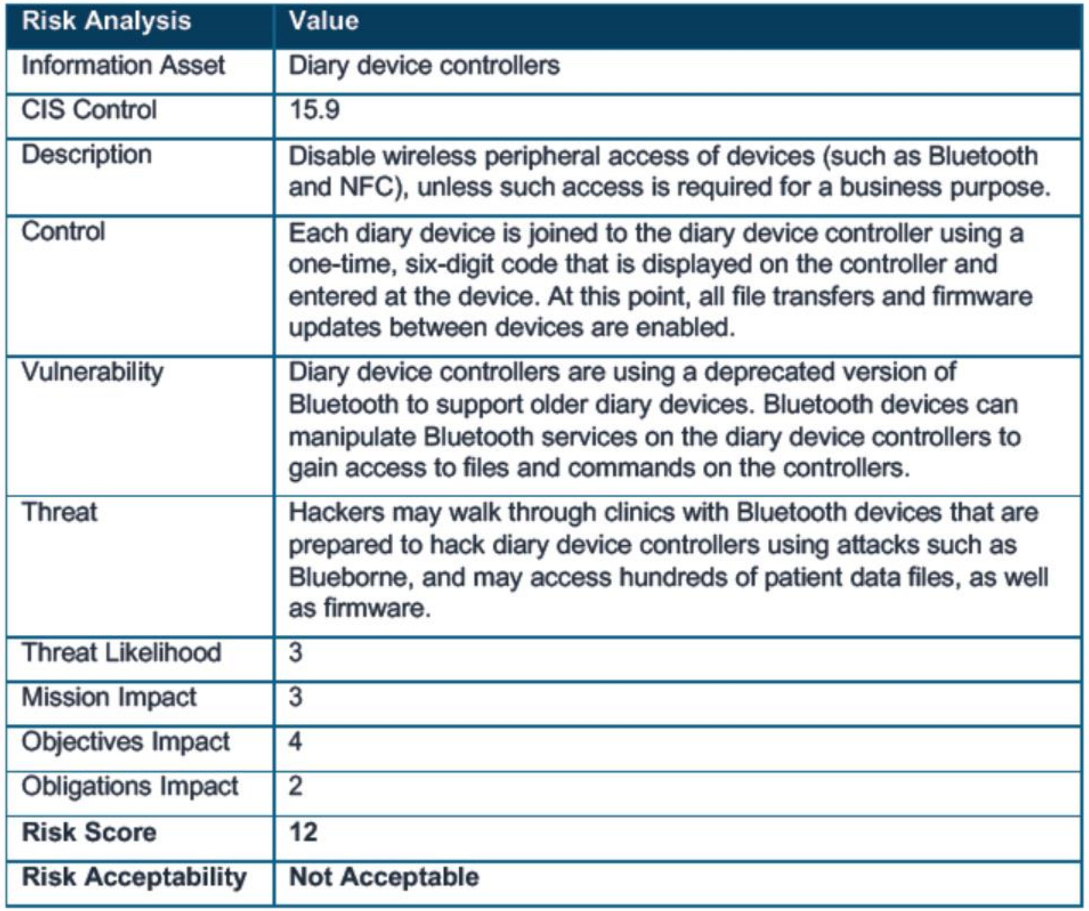
	Likelihood	**Very low**	**low**	**medium**	**high**	**Very high**
Perdita	**Very low**	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very high	4	5	6	7	8

PRIORITIZZARE I RISCHI

Assegnare priorità ai rischi in base a criteri di valutazione.

Minacce	Perdita	Likelihood	Rischio	Rank
Minaccia A	Very low	Very low	0	5
Minaccia B	Very high	Medium	6	1
Minaccia C	Low	Low	2	4
Minaccia D	Very low	High	4	2
Minaccia E	Medium	Low	3	3
Minaccia F	High	Low	4	2

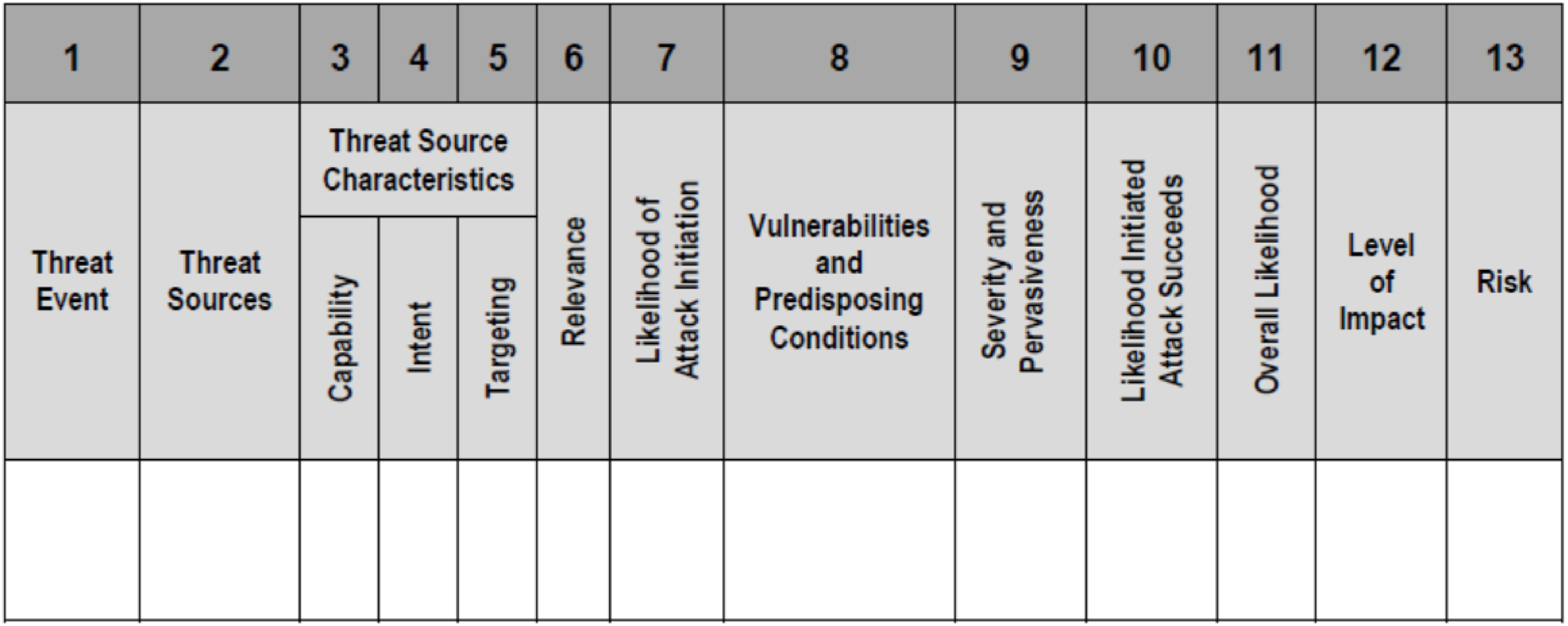
VALUTAZIONE DEL RISCHIO. ESEMPIO 1



Risk Analysis	Value
Information Asset	Diary device controllers
CIS Control	15.9
Description	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
Control	Each diary device is joined to the diary device controller using a one-time, six-digit code that is displayed on the controller and entered at the device. At this point, all file transfers and firmware updates between devices are enabled.
Vulnerability	Diary device controllers are using a deprecated version of Bluetooth to support older diary devices. Bluetooth devices can manipulate Bluetooth services on the diary device controllers to gain access to files and commands on the controllers.
Threat	Hackers may walk through clinics with Bluetooth devices that are prepared to hack diary device controllers using attacks such as Blueborne, and may access hundreds of patient data files, as well as firmware.
Threat Likelihood	3
Mission Impact	3
Objectives Impact	4
Obligations Impact	2
Risk Score	**12**
Risk Acceptability	**Not Acceptable**

[CIS Risk Assessment Method]

VALUTAZIONE DEL RISCHIO. ESEMPIO 2



1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

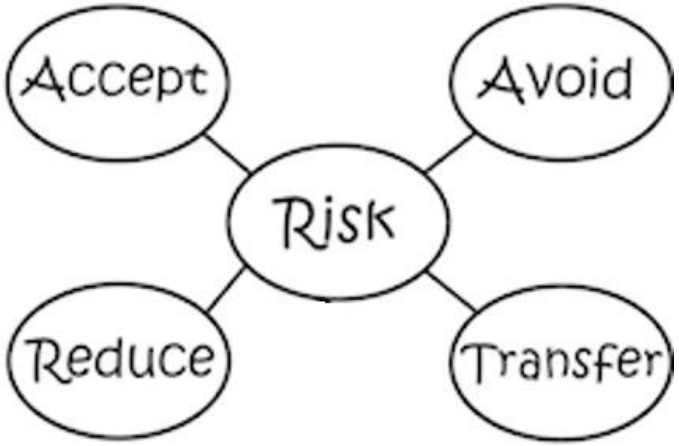
[NIST 800-30 rev 1. Guide for Conducting Risk Assessments]

73

TREATMENTO DEL RISCHIO

TRATTAMENTO DEL RISCHIO

- Evitamento del rischio
  - non svolgere attività rischiose
- Mitigazione del rischio (riduzione)
  - Prevenire/ridurre il likelihood o la perdita di minac
- Trasferimento del rischio
  - Assicurazione e outsourcing
- Accettazione del rischio (ritenzione/tolleranza)
  - Allora… ok.



TRATTAMENTO DEL RISCHIO. RIDUZIONE

- Il rischio può essere ridotto in 3 modi:

- Ridurre l'esposizione alle minacce
    - Molto difficile!
    - Non irritare le gente.

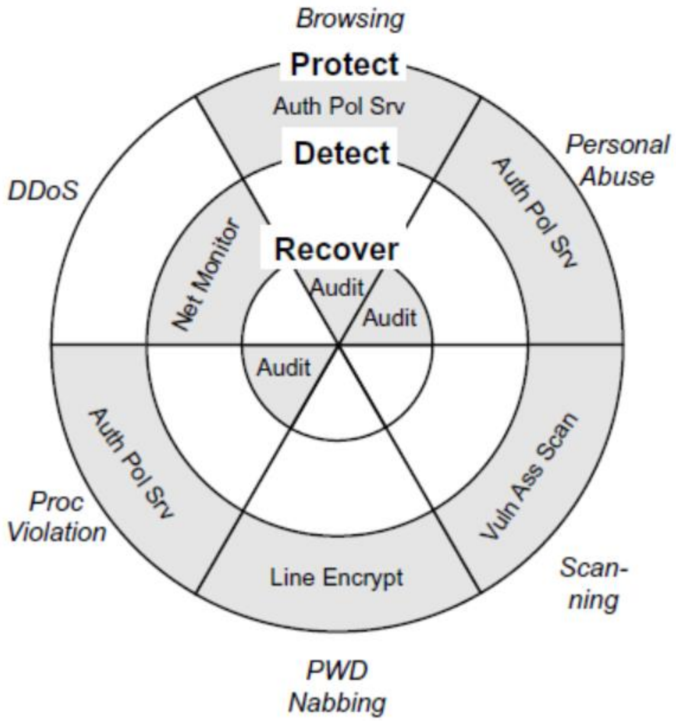
- Ridurre la probabilità di minaccia
    - Protezione da malware, protezione della rete, crittografia, gestione degli incidenti

- Ridurre l'impatto delle minacce
    - Piano di continuità operativa, Back-up, Gestione degli incidenti

TRATTAMENTO DEL RISCHIO. RIDUZIONE

- Difesa in ampiezza contro difesa in profondità
  - Livello di rete
    - Perimetro, reti, nodi finali

- Livello di sicurezza:
  - Prevenire, rilevare, monitorare, recuperare



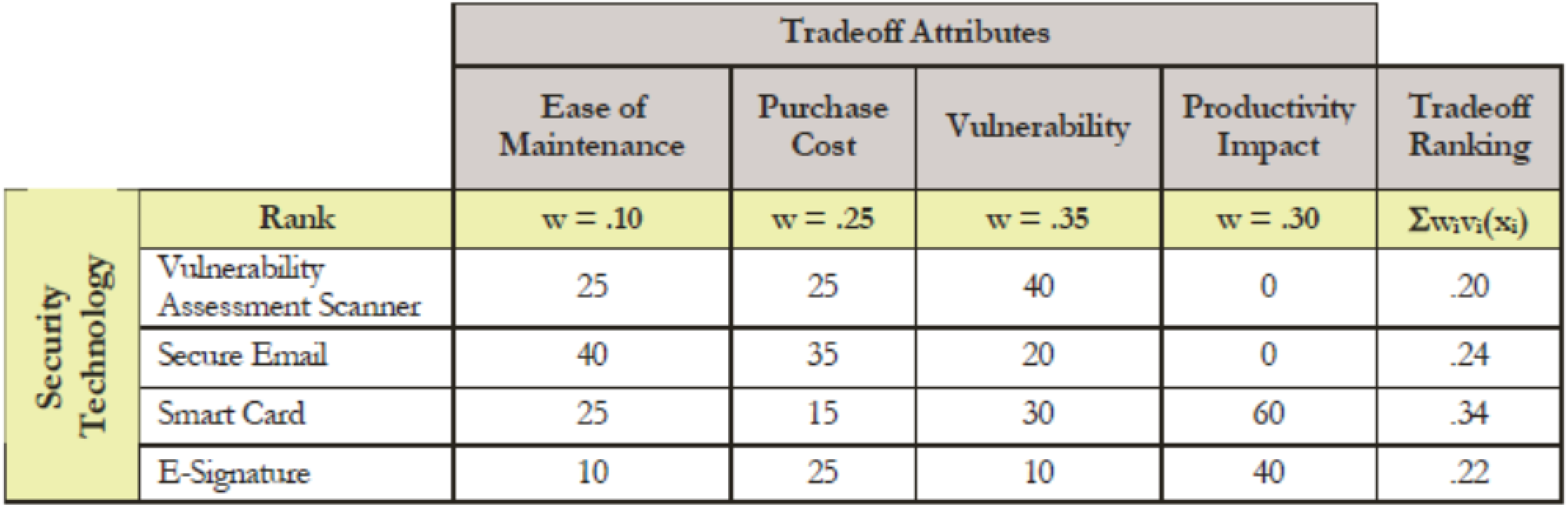
- S. Butler "Security attribute evaluation method: a cost-benefit approach". International Conference on Software Engineering, 2002

TRATTAMENTO DEL RISCHIO. COST-BENEFIT ANALYSIS

- Cost benefit analysis
  - $Benefit = Risk_{before} - Risk_{after} - Cost$
- Return on (security) investment
  - $RO(S)I = \frac{Risk_{before} - Risk_{after}}{Cost}$
  - Greedy approach

- Scelte multiple? Possibile soluzione: soluzione a un problema simile a knapsack problem:
  - Selezionare una serie di possibili controlli per
    1. Riduci al minimo il rischio
    2. Mantieni i costi entro il budget

RISK TREATMENT. TRADE-OFF ANALYSIS. SEMI-QUANTITATIVE



		Tradeoff Attributes				
		Ease of Maintenance	Purchase Cost	Vulnerability	Productivity Impact	Tradeoff Ranking
Security Technology	Rank	w = .10	w = .25	w = .35	w = .30	$\Sigma w_i v_i(x_i)$
	Vulnerability Assessment Scanner	25	25	40	0	.20
	Secure Email	40	35	20	0	.24
	Smart Card	25	15	30	60	.34
	E-Signature	10	25	10	40	.22

- S. Butler "Security attribute evaluation method: a cost-benefit approach". International Conference on Software Engineering, 2002

TRATTAMENTO DEL RISCHIO. TRASFERIMENTO DEL RISCHIO

- Spostare l'attività a un'altra entità (responsabile della gestione del rischio)
  - Sicurezza gestita
  - Cloud
  - Sviluppo in outsourcing
- Ma è difficile trasferire la responsabilità

- Assicurazione
  - Acquista un'assicurazione per coprire quei rischi che non puoi accettare

PERCHÉ L'ASSICURAZIONE CYBER?

- L'assicurazione cyber è apparsa perché:
  - La vulnerabilità è aumentata a causa dell'espansione della tecnologia dell'informazione
  - Le minacce cyber causano grandi rischi aziendali
  - La mitigazione del rischio non elimina completamente il rischio
  - Gli approcci dei gestori del rischio devono essere integrati
- Benefici previsti:
  - Livellamento delle perdite
  - Servire come indicatore della qualità della protezione
  - Incentivo a investire in sicurezza
  - Aumento del benessere sociale
  - Provocare la comparsa di standard di sicurezza avanzati

TRATTAMENTO DEL RISCHIO. EVITAMENTO DEL RISCHIO

1. Cerca di ridurre il rischio
2. Prova a trasferirlo
3. Se il rischio è ancora troppo alto per accettarlo…
4. Chiudere l'attività soggetta a questo rischio.

- Per esempio,
  - non utilizzare un sistema cloud (ad esempio, se non hai le competenze per configurarlo correttamente) o
  - non esternalizzare la codifica a sviluppatori sconosciuti

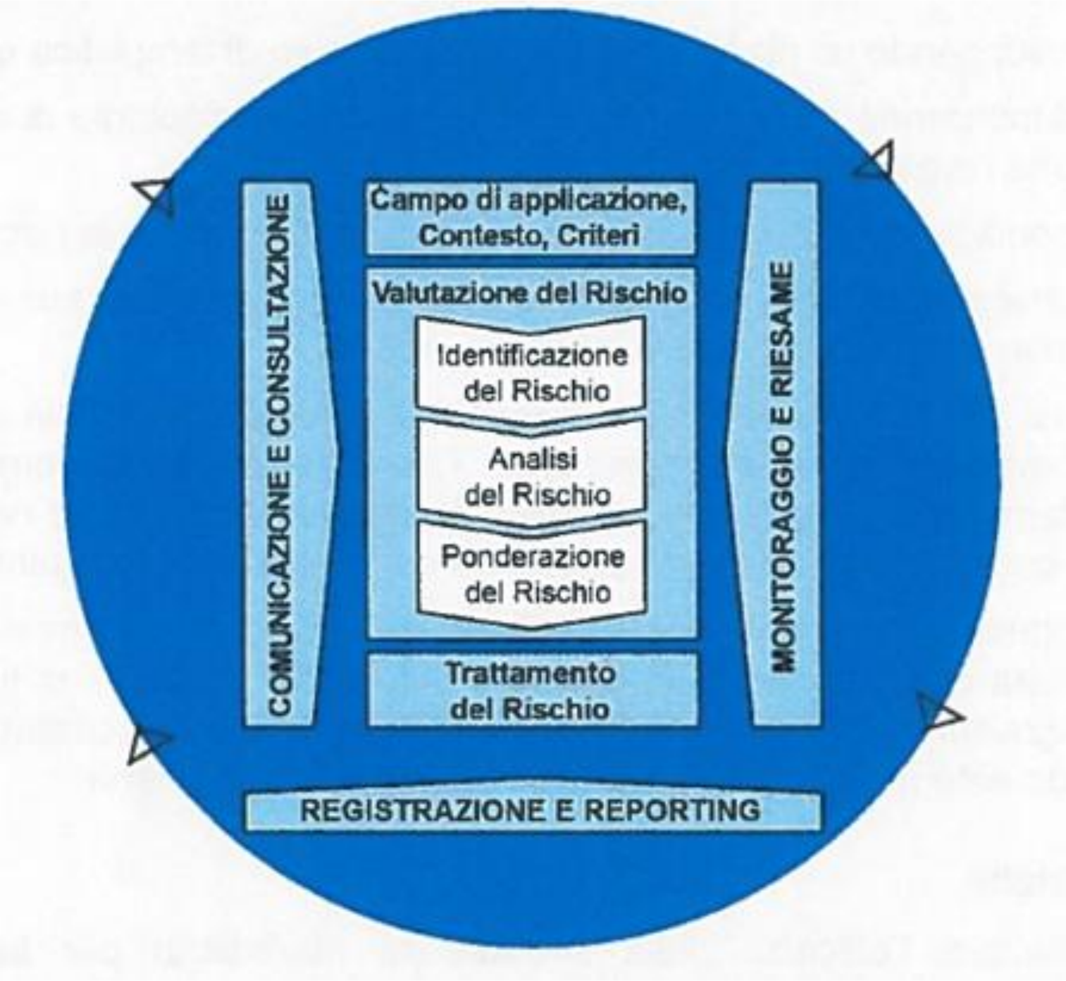
TRATTAMENTO DEL RISCHIO. ACCETTAZIONE DEL RISCHIO

- Opzione predefinita, ma devi essere consapevole di questa decisione
- Guidato da criteri di accettazione
- Possiamo essere coperti dall'autoassicurazione

- Se non puoi accettare il rischio, ripianifica il piano di trattamento del rischio

GESTIONE DEL RISCHIO. ALTRE ATTIVITÀ

- Comunicazione e Consultazione
  - Comunicare con le parti interessate
  - Consultare esperti esterni
- Monitoraggio e riesame
  - Monitorare i valori definiti
  - Esaminare regolarmente i risultati della valutazione del rischio (o quando vengono rilevati errori gravi)
- Registrazione e reporting
  - Registrare i risultati per l'uso futuro
  - Segnalare i risultati della valutazione del rischio


COMUNICAZIONE E CONSULTAZIONE
Campo di applicazione, Contesto, Criteri
Valutazione del Rischio
Identificazione del Rischio
Analisi del Rischio
Ponderazione del Rischio
Trattamento del Rischio
MONITORAGGIO E RIESAME
REGISTRAZIONE E REPORTING

CONCLUSIONE

CONCLUSIONE

- La valutazione del rischio è una pratica importante per gestione della sicurezza di un sistema cyber

- La valutazione del rischio richiede:
  - Buona pianificazione
  - Tempo
  - Sforzo
  - Buona conoscenza del sistema cyber
  - Ottima conoscenza della sicurezza cyber
  - Esperienza nella gestione del rischio

- Ci sono altri modi per trattare i rischi
  - Non solo riduzione del rischio

DOMANDE?

This course is based on the knowledge obtained in the scope of the following EU projects:

SPARTA MEDINA

MEDINA

Automation-based Certification for Cloud Services in Europe

Dr. Jesus Luna Garcia

Robert Bosch GmbH, Germany

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

Agenda

- Why (again) certification?
- Basic concepts
- H2020 MEDINA in a Nutshell
- AI and the future of certification

Why (again) certification?

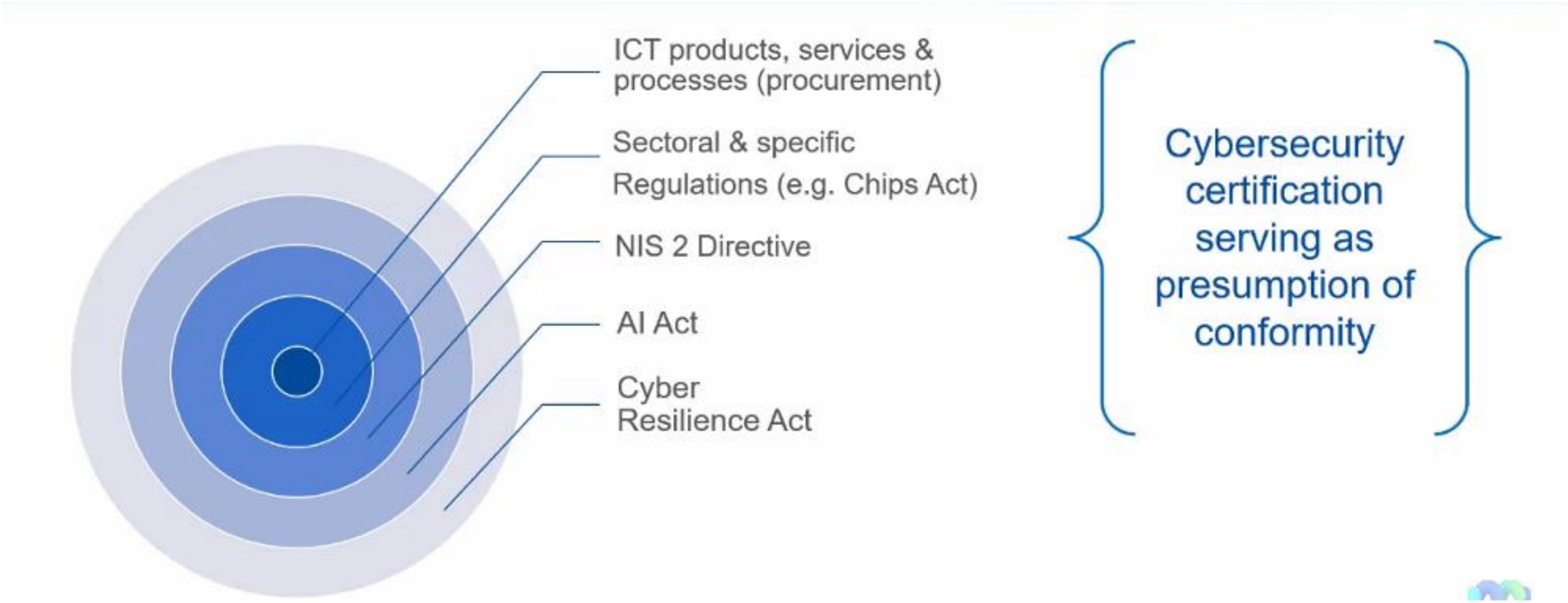
Cybersecurity Deja-Vu

UPC Openclass

20.10.2023

Cybersecurity Certification – the „new“ EU Silver Bullet?

- The role of cybersecurity certification is getting more prominent, whereas relevant EU-Regulations consider it as a mandatory requirement.



ICT products, services & processes (procurement)

Sectoral & specific Regulations (e.g. Chips Act)

NIS 2 Directive

AI Act

Cyber Resilience Act

Cybersecurity certification serving as presumption of conformity

Borrowed from ENISA's presentation during Cert WS (12.2022)

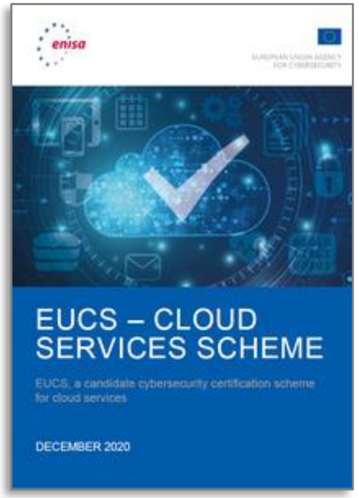
Certification “Made in the EU”

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation **EU-wide cybersecurity certification schemes** in order to:
  - provide an EU-wide cybersecurity baseline (requirements, audit methods)
  - enable customers to make risk-based decisions about cybersecurity
  - ***enable continuous cybersecurity compliance***
- ENISA (EU Cybersecurity Agency) nominated as responsible for developing the new EU-certification schemes.

What is being prepared by ENISA?

MEDINA

- Three EUCSA-derived certification schemes are under preparation by ENISA:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - **EUCS - Cybersecurity Certification Scheme for Cloud Services** → BOSCH
  - EU5G - Cybersecurity Certification Scheme for 5G
- …but more are expected to come (e.g., AI and IoT).
- How the (certification) future looks like?



enisa

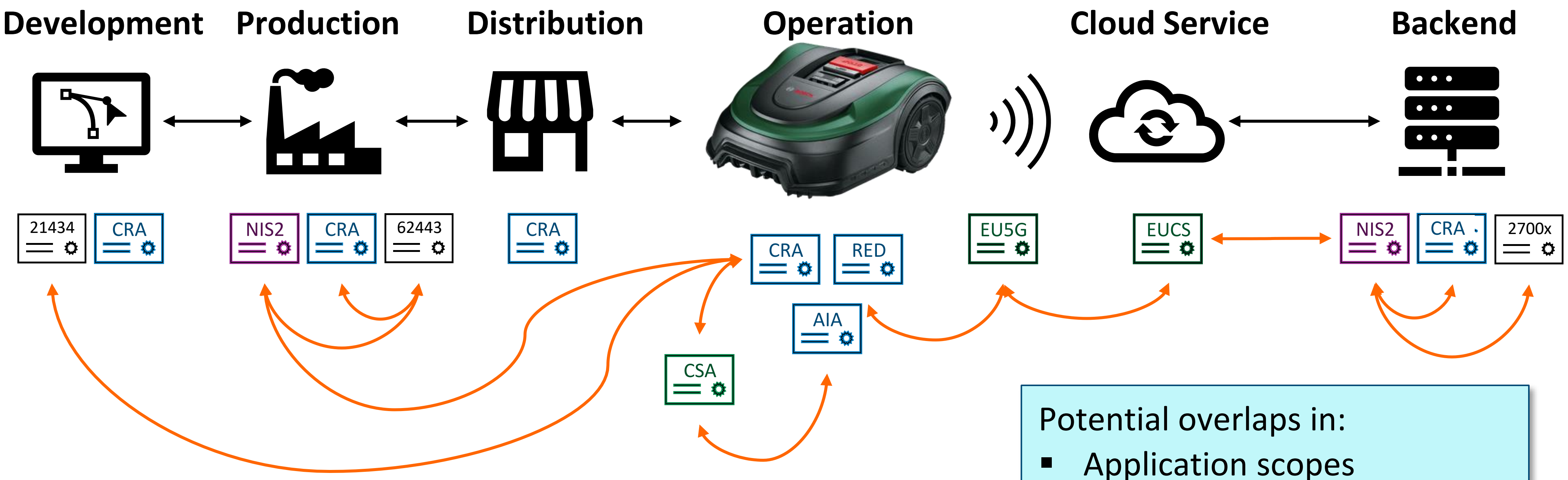
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

Real-world example: Bosch Indego



XYZ Product regulation

XYZ Infrastructure regulation

XYZ Certification scheme

XYZ Other

Potential overlaps in:

- Application scopes
- Security requirements
- Reporting obligations
- Evidence provisions
- Classifications etc.

$ ping audience

- Please open https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh

And feel free to share your opinion on the topic! 3 mins

Únase en

slido.com

#9795 9089

MEDINA

Basic Concepts

Introducing the EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

UPC Openclass

20.10.2023

Basics: Terminology

MEDINA

- **Conformity Assessment**: demonstration that specified requirements are fulfilled.
- **Certification:** the provision by an independent body (3rd party) of written assurance (a certificate) that the product, service or system in question is conformant.

Certification is about assurance! Per-se, being certified doesn’t mean it’s secure.

Basics: Purpose and Scope

- Purpose:
  - Certification can be a useful tool to add credibility, by demonstrating that the Target Of Evaluation (TOE) meets the expectations (in terms of requirements) of customers.
- Scope (TOE) of Certification:
  - Process: ISMS, CSMS, etc.
  - Products: Firewalls, encryption devices, smart home appliance, automotive components, etc.
  - Service: Single sign-on, cloud services, etc.

Basics: EUCS at a glance

- ENISA started the development of EUCS early 2020.
  - <u>Estimated</u> GoLive Q1/2024
- Basic features:
  - Standards based (German C5, French SecNumCloud)
  - Focus on Cloud Services (e.g., SQL, VM, Web Apps), not Cloud Service Providers (e.g., AWS, Azure, GCP)
  - Introduces compositional certification
  - Defines three levels of assurance *(see next slide)*
  - Introduces automation for assessments *(see next slide)*

Basics: Levels of Assurance in EUCS

MEDINA

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment driven
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** risks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

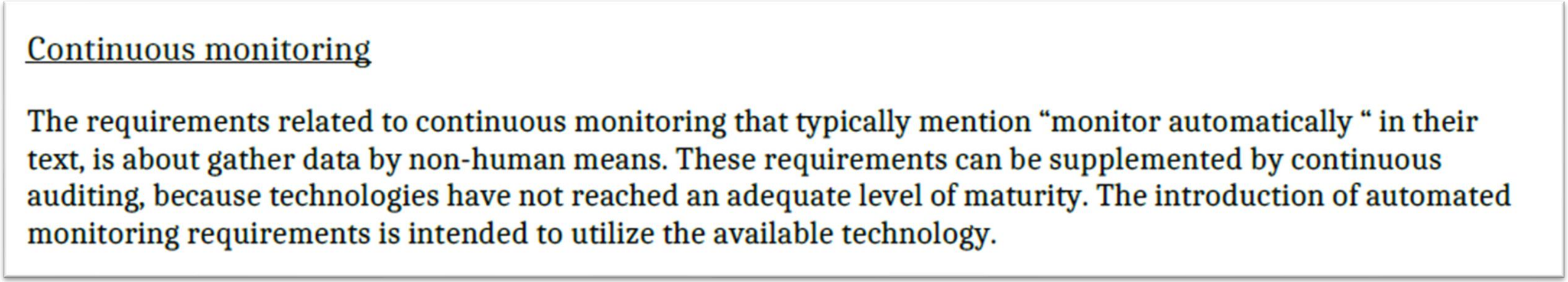
‘high’ level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

Basics: Continuous Monitoring in EUCS

- From 6th WD of EUCS1 specification (CEN CENELEC)

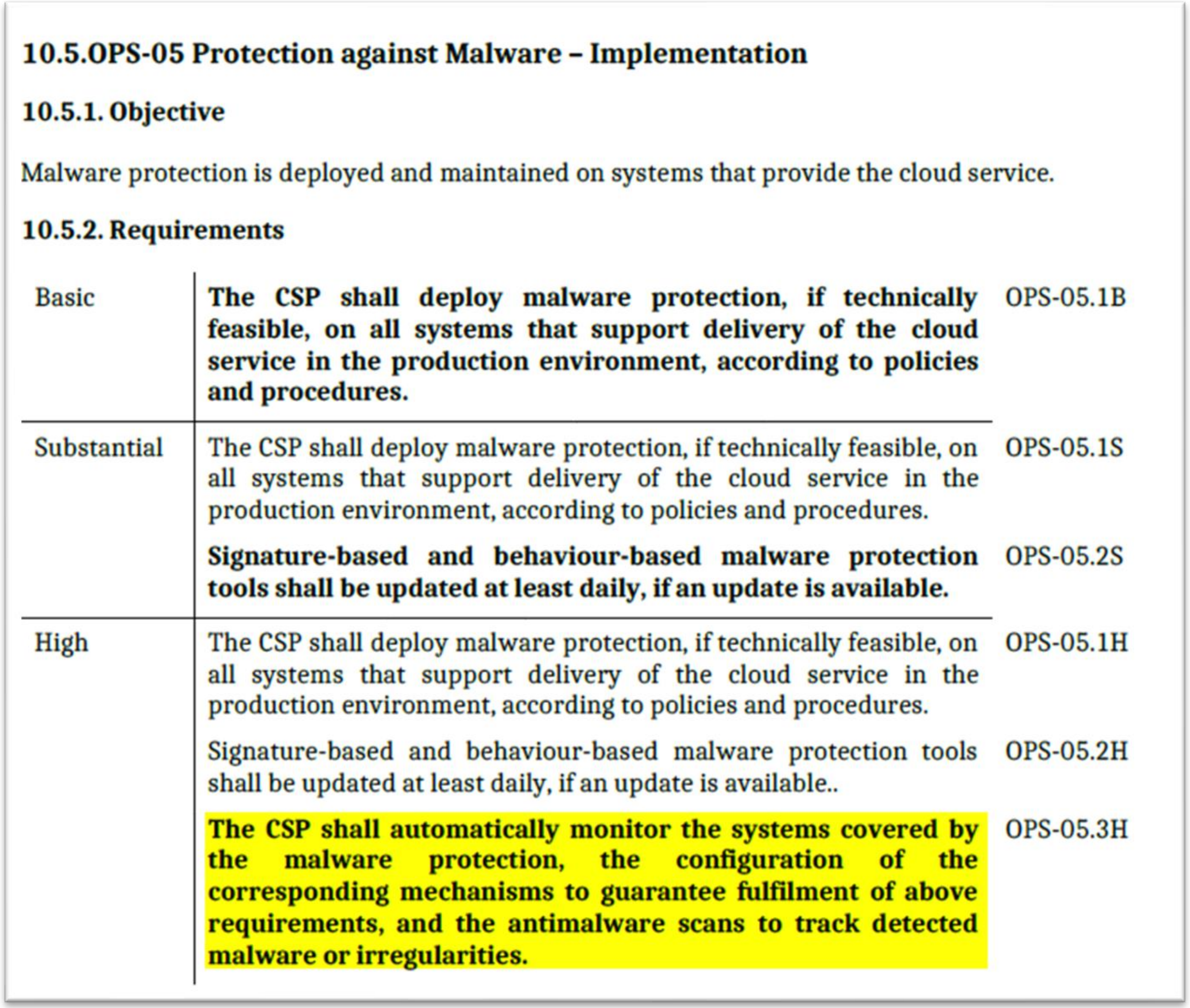


Continuous monitoring

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

Basics: Continuous Monitoring in EUCS

- “High” assurance requirement related to “continuous monitoring” (based on 6th WD from CEN CENELEC)



10.5.OPS-05 Protection against Malware – Implementation

10.5.1. Objective

Malware protection is deployed and maintained on systems that provide the cloud service.

10.5.2. Requirements

Basic	**The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.**	OPS-05.1B
Substantial	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.	OPS-05.1S
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available.	OPS-05.2S
High	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.	OPS-05.1H
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available..	OPS-05.2H
	The CSP shall automatically monitor the systems covered by the malware protection, the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.	OPS-05.3H

$ ping audience

- Please open https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh

And feel free to share your opinion on the topic! 3 mins

Únase en

slido.com

#9795 9089

MEDINA

H2020 MEDINA in a Nutshell

Paving the road towards EUCS

UPC Openclass

20.10.2023

Why MEDINA?

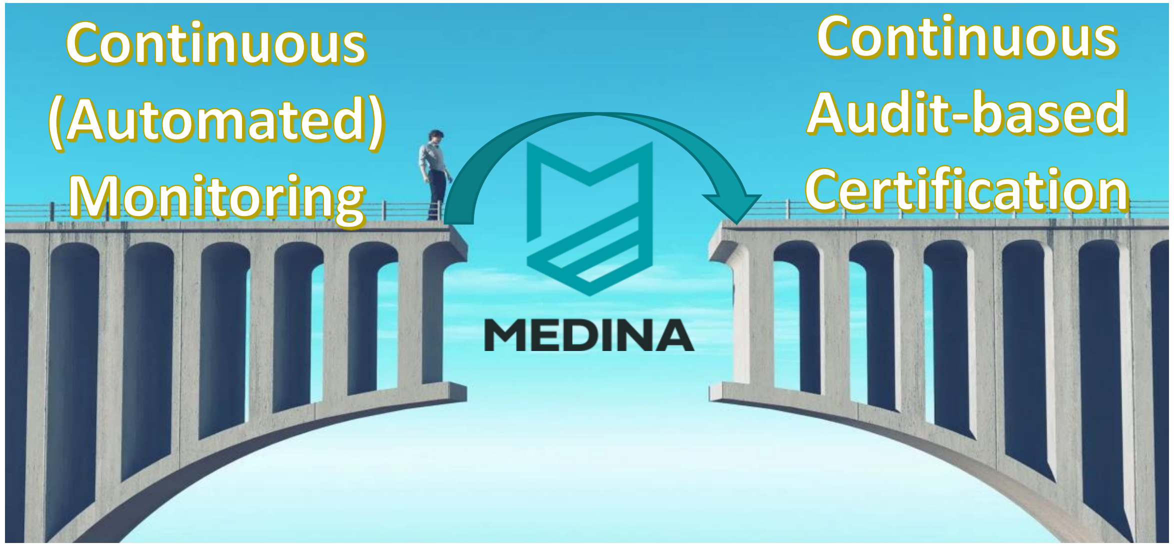
MEDINA

- The implementation of “continuous monitoring” brings some challenges to Cloud Service Providers, but also to auditors assessing those requirements.
  - Preliminary analysis documented in our whitepaper.
- How to approach EUCS-Continuous, and further develop it towards *continuous (automated) certification*?

Mission

Provision of a **Security framework and tools** for achieving a **continuous audit-based certification**, through **trustworthy evidence-management methods.**

- MEDINA primarily focuses on the **EUCS requirements for High Assurance**, where some degree of continuous (automated) monitoring is needed.
- However, the MEDINA framework can be **extended to other EUCS requirements** at the substantial level, or even to **similar certification schemes** (e.g., BSI C5).


Continuous (Automated) Monitoring
MEDINA
Continuous Audit-based Certification

Who’s Who in MEDINA?

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€

Estonia
Latvia
Lithuania
Denmark
Belarus
Ireland
United Kingdom
Netherlands
Poland
Germany
Belgium
Luxembourg
Czechia
Slovakia
Ukraine
Austria
Hungary
Moldova
France
Liechtenstein
Switzerland
Slovenia
Romania
Croatia
Serbia
Monaco
San Marino
Italy
Montenegro
Bulgaria
Andorra
North Macedonia
Spain
Albania
Portugal
Greece
Malta

tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft®

Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Challenges and Approaches

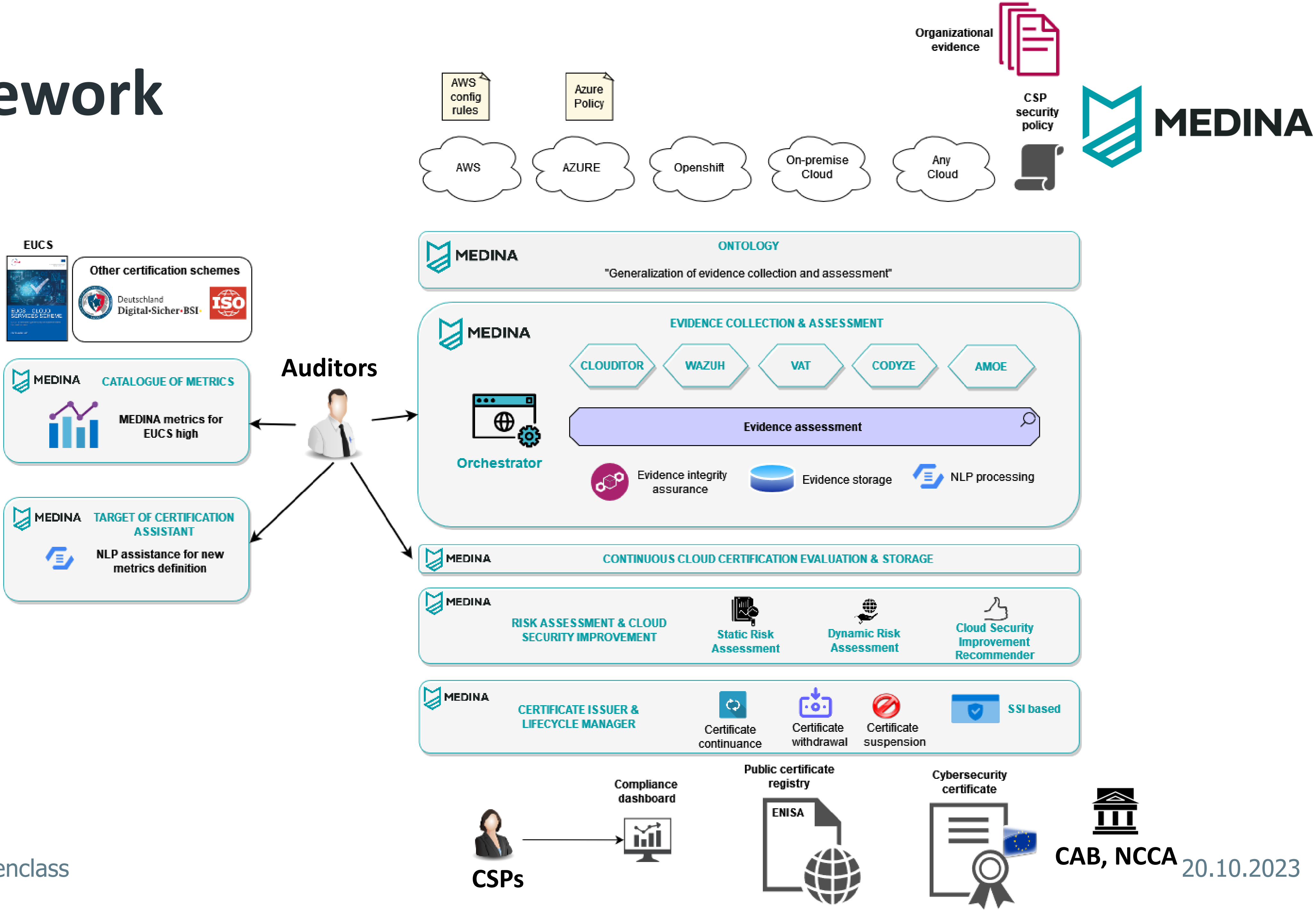
Topic	Approach (Keywords)
Automation of compliance assessments	• Assessment based on machine-readable EUCS metrics • CSP-neutral / -native technical evidence collectors • NLP for assessing security policies (e.g., PDF)
Trustworthy evidence management	• Blockchain-based evidence vault • RBAC authorization model
Certificate management	• Risk-based automation of certificate life-cycle • Backtracking/visualization of non-compliances • SSI enabled (selective disclosure of attributes) • Connection to ENISA Certification Website (wip)
Standardization	• EUCS: CEN CENELEC EUCS1 • Metrics: ISO/IEC 27004, NIST SP 800-55rev2 • Automation: NIST OSCAL, ETSI CYBER

Expected Benefits

MEDINA

- **Guidance** on the implementation of the controls, compliance **metrics and evidences** to be collected
- Support for **automatic compliance assessment** of EUCS and **other certification schemes**
- Ease the effort of **managing** (trustworthy) evidences in EUCS
- Standardization and awareness to pave the road for **continuous certification** (in particular with **Regulators in the EU and US**)

Framework



Organizational evidence

AWS config rules

Azure Policy

CSP security policy

MEDINA

AWS

AZURE

Openshift

On-premise Cloud

Any Cloud

EUCS

Other certification schemes

Deutschland Digital•Sicher•BSI•

ISO

MEDINA ONTOLOGY

"Generalization of evidence collection and assessment"

MEDINA EVIDENCE COLLECTION & ASSESSMENT

CLOUDITOR

WAZUH

VAT

CODYZE

AMOE

Orchestrator

Evidence assessment

Evidence integrity assurance

Evidence storage

NLP processing

Auditors

MEDINA CATALOGUE OF METRICS

MEDINA metrics for EUCS high

MEDINA TARGET OF CERTIFICATION ASSISTANT

NLP assistance for new metrics definition

MEDINA CONTINUOUS CLOUD CERTIFICATION EVALUATION & STORAGE

MEDINA RISK ASSESSMENT & CLOUD SECURITY IMPROVEMENT

Static Risk Assessment

Dynamic Risk Assessment

Cloud Security Improvement Recommender

MEDINA CERTIFICATE ISSUER & LIFECYCLE MANAGER

Certificate continuance

Certificate withdrawal

Certificate suspension

SSI based

Compliance dashboard

Public certificate registry

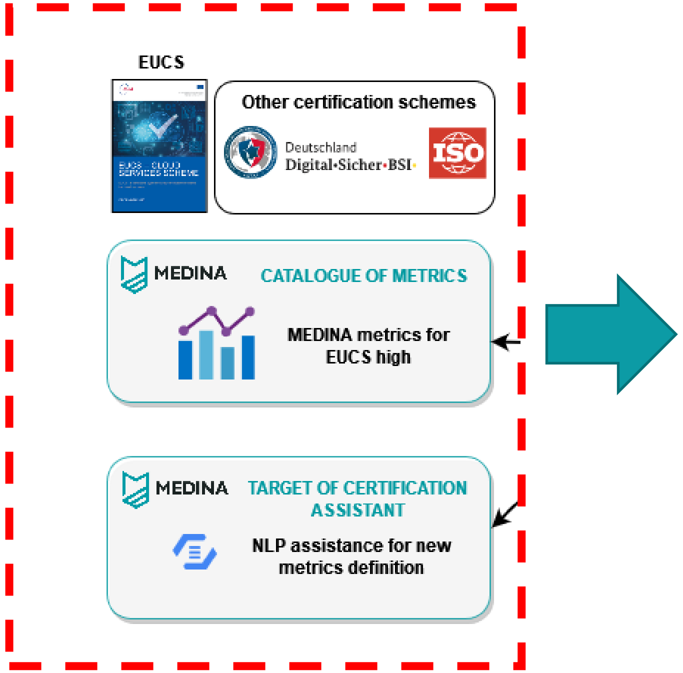
ENISA

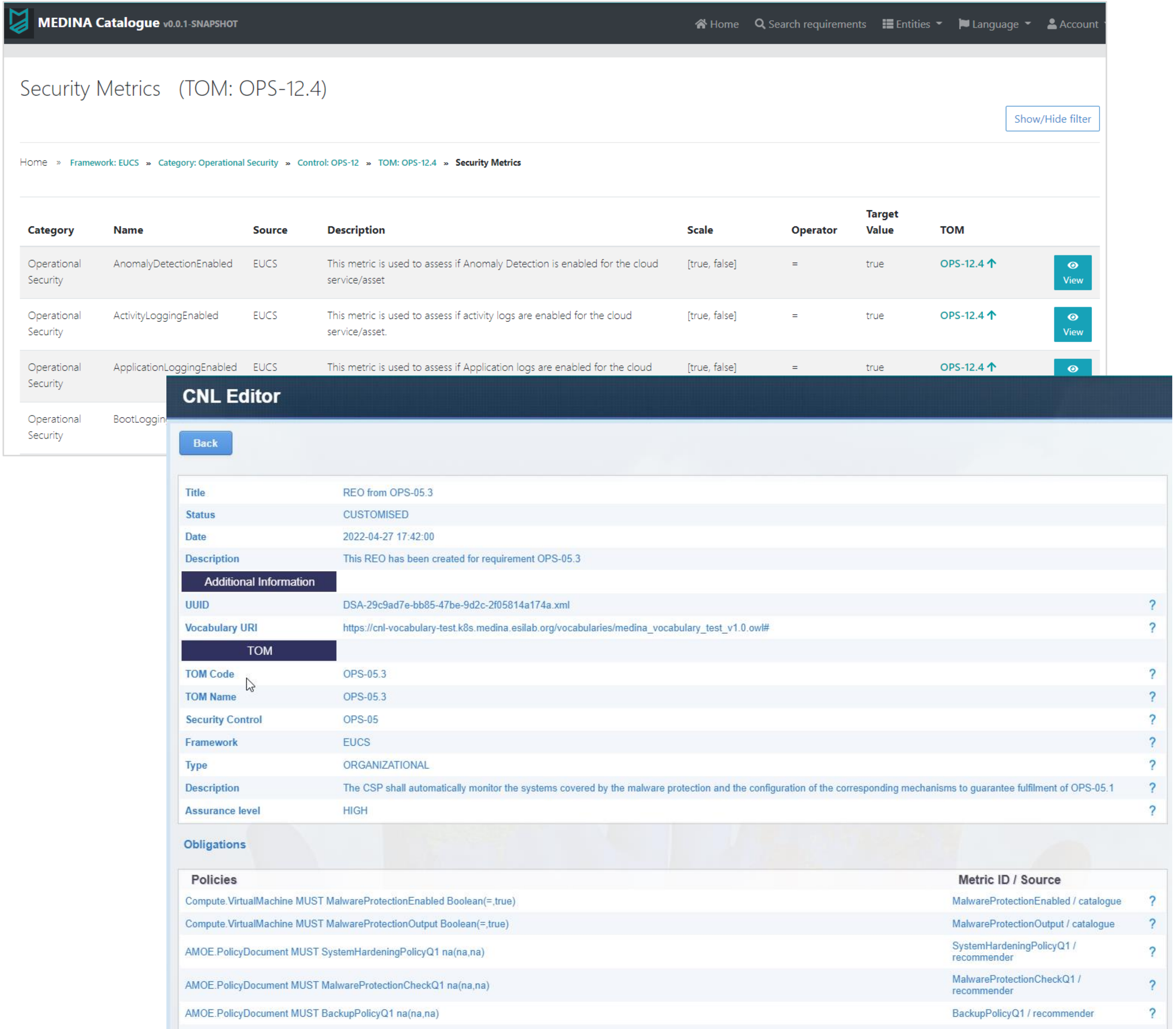
Cybersecurity certificate

CSPs

CAB, NCCA

ToE Initialization


EUCS
Other certification schemes
Deutschland Digital·Sicher·BSI·
ISO
MEDINA
CATALOGUE OF METRICS
MEDINA metrics for EUCS high
MEDINA
TARGET OF CERTIFICATION ASSISTANT
NLP assistance for new metrics definition



Security Metrics (TOM: OPS-12.4)

Home » Framework: EUCS » Category: Operational Security » Control: OPS-12 » TOM: OPS-12.4 » Security Metrics

Category	Name	Source	Description	Scale	Operator	Target Value	TOM	
Operational Security	AnomalyDetectionEnabled	EUCS	This metric is used to assess if Anomaly Detection is enabled for the cloud service/asset	[true, false]	=	true	OPS-12.4	View
Operational Security	ActivityLoggingEnabled	EUCS	This metric is used to assess if activity logs are enabled for the cloud service/asset.	[true, false]	=	true	OPS-12.4	View
Operational Security	ApplicationLoggingEnabled	EUCS	This metric is used to assess if Application logs are enabled for the cloud	[true, false]	=	true	OPS-12.4	
Operational Security	BootLoggin							

CNL Editor

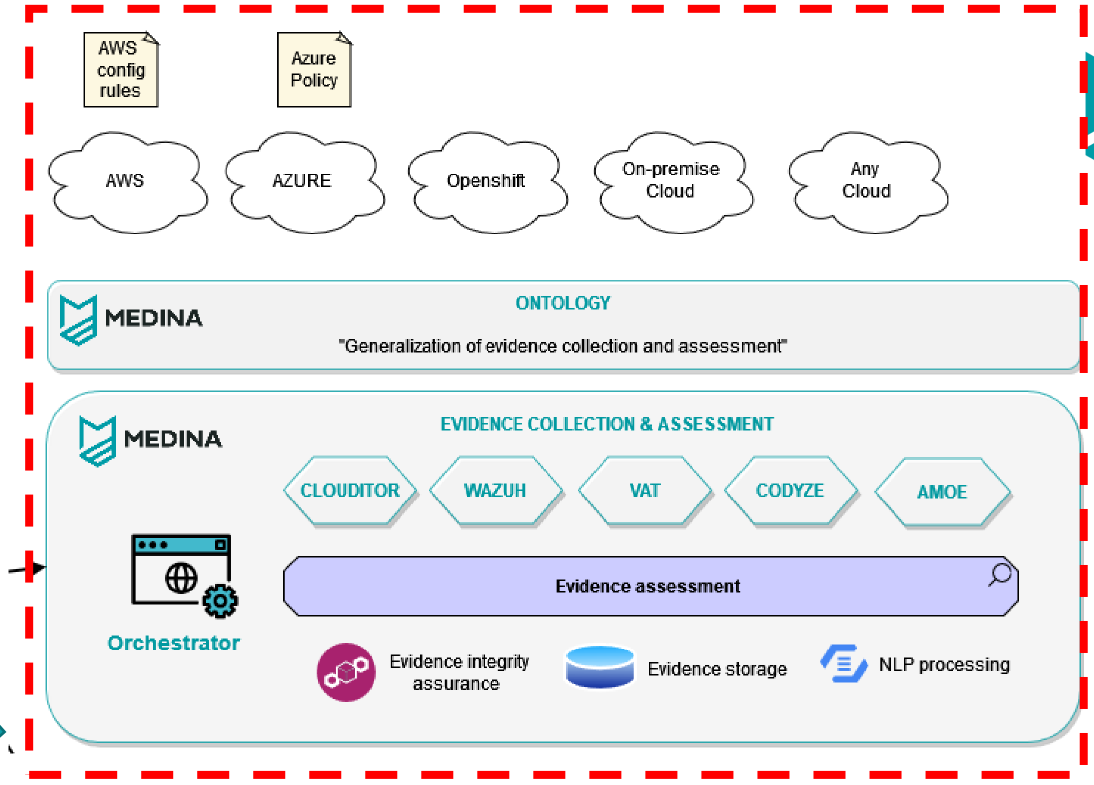
Title	REO from OPS-05.3	
Status	CUSTOMISED	
Date	2022-04-27 17:42:00	
Description	This REO has been created for requirement OPS-05.3	
Additional Information		
UUID	DSA-29c9ad7e-bb85-47be-9d2c-2f05814a174a.xml	?
Vocabulary URI	https://cnl-vocabulary-test.k8s.medina.esilab.org/vocabularies/medina_vocabulary_test_v1.0.owl#	?
TOM		
TOM Code	OPS-05.3	?
TOM Name	OPS-05.3	?
Security Control	OPS-05	?
Framework	EUCS	?
Type	ORGANIZATIONAL	?
Description	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	?
Assurance level	HIGH	?

Obligations

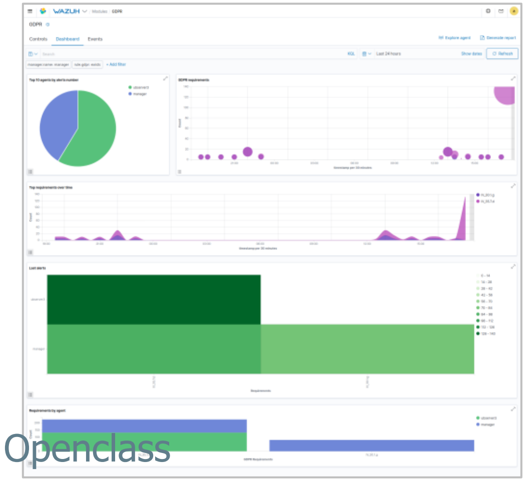
Policies	Metric ID / Source	
Compute.VirtualMachine MUST MalwareProtectionEnabled Boolean(=,true)	MalwareProtectionEnabled / catalogue	?
Compute.VirtualMachine MUST MalwareProtectionOutput Boolean(=,true)	MalwareProtectionOutput / catalogue	?
AMOE.PolicyDocument MUST SystemHardeningPolicyQ1 na(na,na)	SystemHardeningPolicyQ1 / recommender	?
AMOE.PolicyDocument MUST MalwareProtectionCheckQ1 na(na,na)	MalwareProtectionCheckQ1 / recommender	?
AMOE.PolicyDocument MUST BackupPolicyQ1 na(na,na)	BackupPolicyQ1 / recommender	?

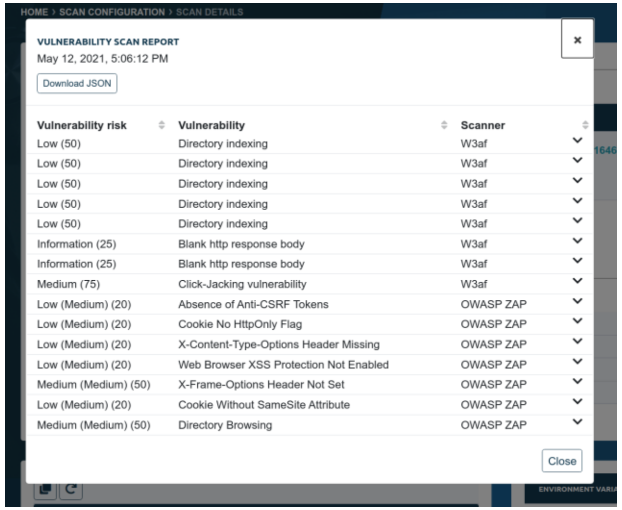
Ev. Collection

MEDINA



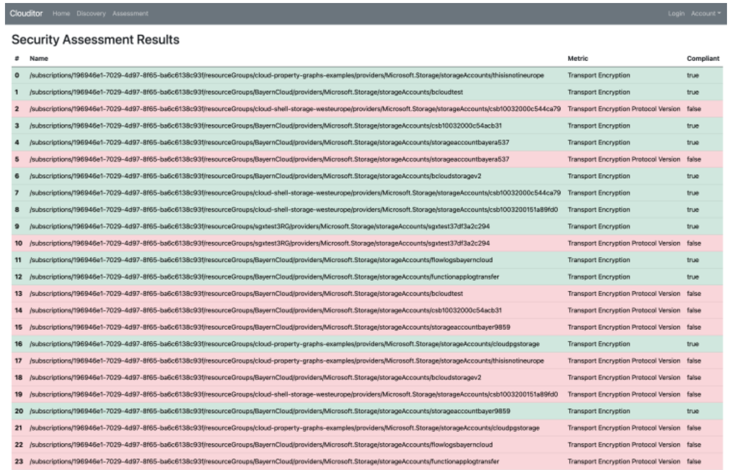
Technical evidence collectors





VULNERABILITY SCAN REPORT
May 12, 2021, 5:06:12 PM

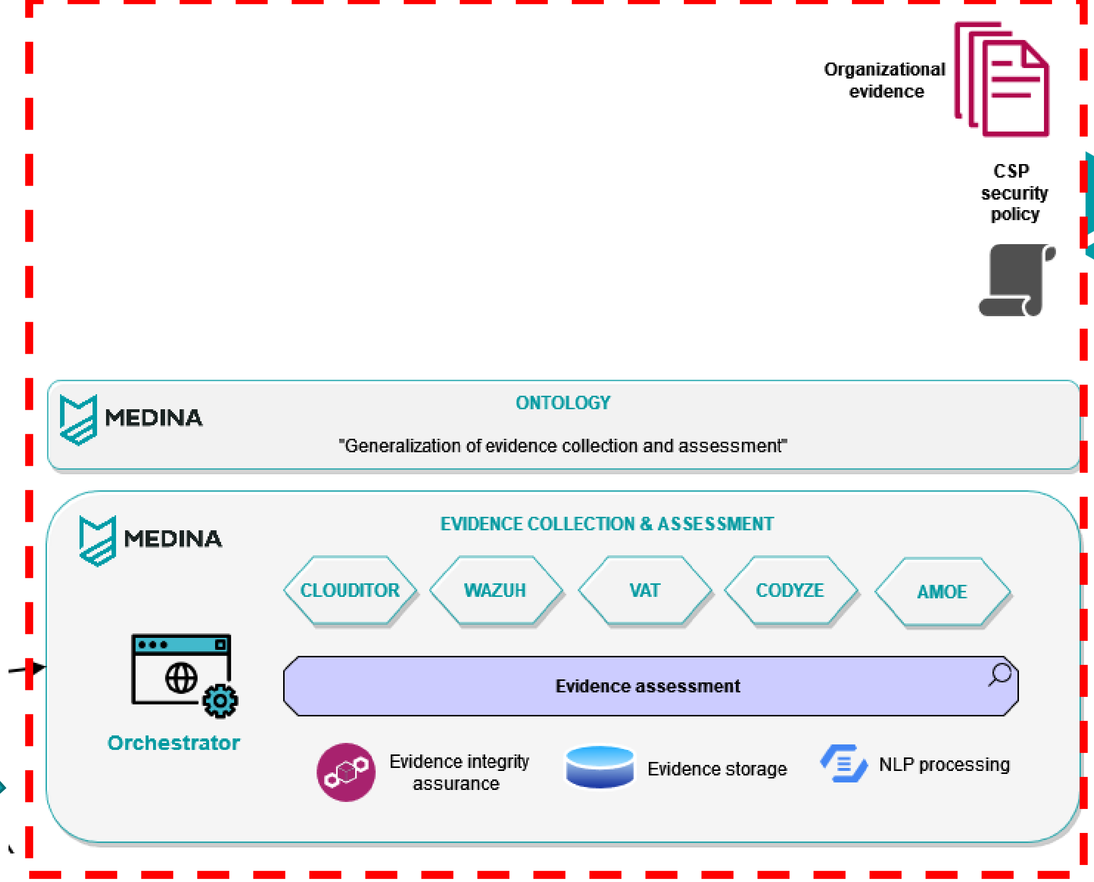
Vulnerability risk	Vulnerability	Scanner
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Information (25)	Blank http response body	W3af
Information (25)	Blank http response body	W3af
Medium (75)	Click-Jacking vulnerability	W3af
Low (Medium) (20)	Absence of Anti-CSRF Tokens	OWASP ZAP
Low (Medium) (20)	Cookie No HttpOnly Flag	OWASP ZAP
Low (Medium) (20)	X-Content-Type-Options Header Missing	OWASP ZAP
Low (Medium) (20)	Web Browser XSS Protection Not Enabled	OWASP ZAP
Medium (Medium) (50)	X-Frame-Options Header Not Set	OWASP ZAP
Low (Medium) (20)	Cookie Without SameSite Attribute	OWASP ZAP
Medium (Medium) (50)	Directory Browsing	OWASP ZAP



Security Assessment Results

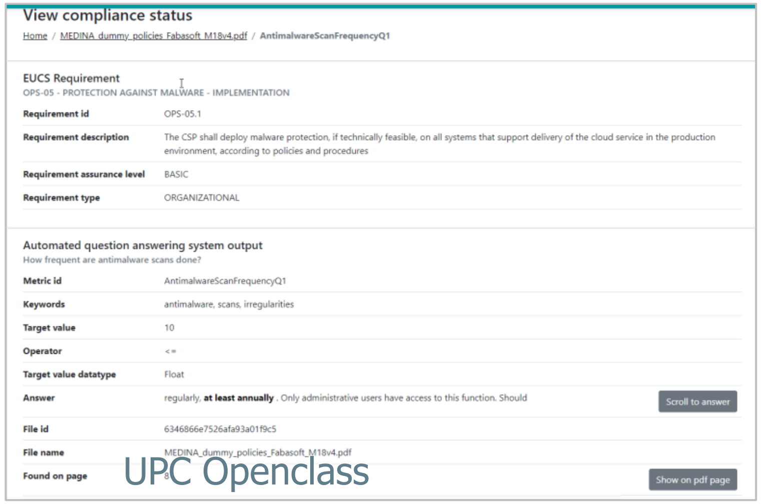
#	Name	Metric	Compliant
0	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/thisisnotineurope	Transport Encryption	true
1	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudtest	Transport Encryption	true
2	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb10032000c544ca79	Transport Encryption Protocol Version	false
3	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/csb10032000c54acb31	Transport Encryption	true
4	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayera537	Transport Encryption	true
5	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayera537	Transport Encryption Protocol Version	false
6	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudstoragev2	Transport Encryption	true
7	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb10032000c544ca79	Transport Encryption	true
8	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb1003200151a89fd0	Transport Encryption	true
9	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/sgxtest3RG/providers/Microsoft.Storage/storageAccounts/sgxtest37df3a2c294	Transport Encryption	true
10	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/sgxtest3RG/providers/Microsoft.Storage/storageAccounts/sgxtest37df3a2c294	Transport Encryption Protocol Version	false
11	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/flowlogsbayerncloud	Transport Encryption	true
12	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/functionapplogtransfer	Transport Encryption	true
13	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudtest	Transport Encryption Protocol Version	false
14	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/csb10032000c54acb31	Transport Encryption Protocol Version	false
15	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayer9859	Transport Encryption Protocol Version	false
16	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/cloudpgstorage	Transport Encryption	true
17	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/thisisnotineurope	Transport Encryption Protocol Version	false
18	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudstoragev2	Transport Encryption Protocol Version	false
19	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb1003200151a89fd0	Transport Encryption Protocol Version	false
20	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayer9859	Transport Encryption	true
21	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/cloudpgstorage	Transport Encryption Protocol Version	false
22	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/flowlogsbayerncloud	Transport Encryption Protocol Version	false
23	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/functionapplogtransfer	Transport Encryption Protocol Version	false

Ev. Collection



MEDINA

NLP-evidence collectors



View compliance status

Home / MEDINA_dummy_policies_Fabasoft_M18v4.pdf / AntimalwareScanFrequencyQ1

EUCS Requirement

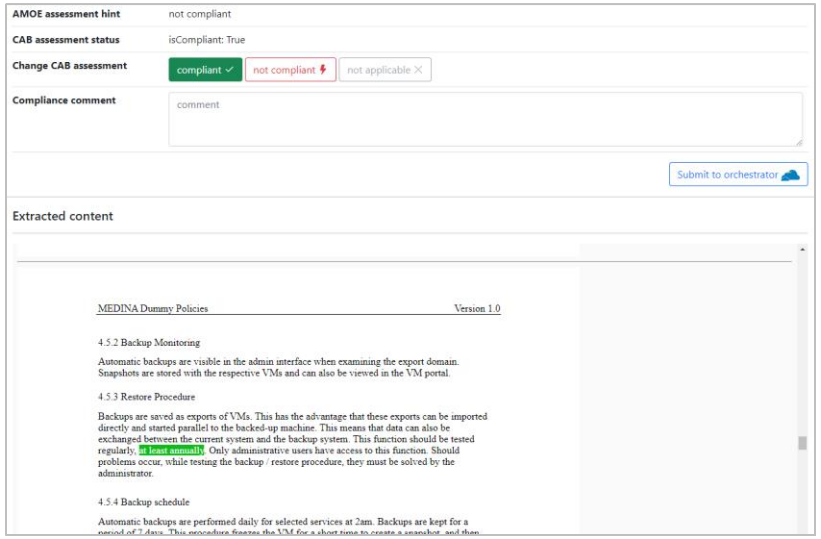
OPS-05 - PROTECTION AGAINST MALWARE - IMPLEMENTATION

Requirement id	OPS-05.1
Requirement description	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures
Requirement assurance level	BASIC
Requirement type	ORGANIZATIONAL

Automated question answering system output

How frequent are antimalware scans done?

Metric id	AntimalwareScanFrequencyQ1
Keywords	antimalware, scans, irregularities
Target value	10
Operator	<=
Target value datatype	Float
Answer	regularly, **at least annually** . Only administrative users have access to this function. Should
File id	6346866e7526afa93a01f9c5
File name	MEDINA_dummy_policies_Fabasoft_M18v4.pdf
Found on page	8



AMOE assessment hint	not compliant
CAB assessment status	isCompliant: True
Change CAB assessment	compliant ✓ not compliant not applicable ✕
Compliance comment	comment

Extracted content

MEDINA Dummy Policies Version 1.0

4.5.2 Backup Monitoring

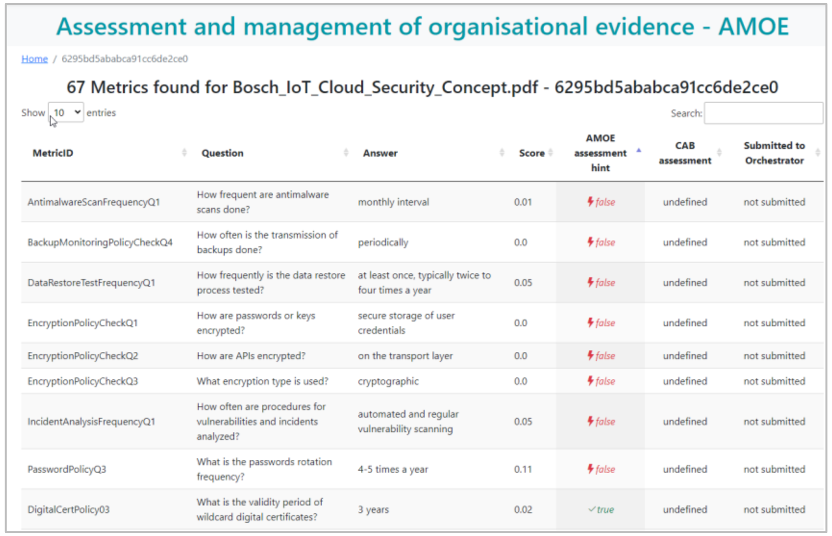
Automatic backups are visible in the admin interface when examining the export domain. Snapshots are stored with the respective VMs and can also be viewed in the VM portal.

4.5.3 Restore Procedure

Backups are saved as exports of VMs. This has the advantage that these exports can be imported directly and started parallel to the backed-up machine. This means that data can also be exchanged between the current system and the backup system. This function should be tested regularly, at least annually. Only administrative users have access to this function. Should problems occur, while testing the backup / restore procedure, they must be solved by the administrator.

4.5.4 Backup schedule

Automatic backups are performed daily for selected services at 2am. Backups are kept for a period of 7 days. This procedure freezes the VM for a short time to create a snapshot, and then



Assessment and management of organisational evidence - AMOE

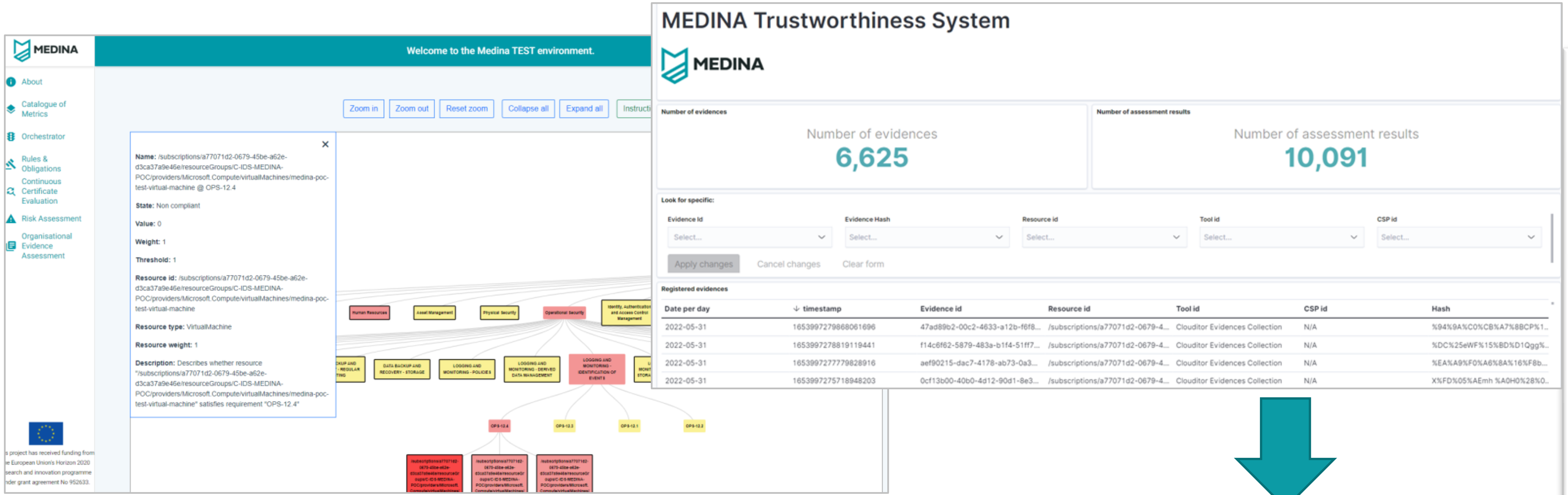
Home / 6295bd5ababca91cc6de2ce0

67 Metrics found for Bosch_IoT_Cloud_Security_Concept.pdf - 6295bd5ababca91cc6de2ce0

Show 10 entries Search:

MetricID	Question	Answer	Score	AMOE assessment hint	CAB assessment	Submitted to Orchestrator
AntimalwareScanFrequencyQ1	How frequent are antimalware scans done?	monthly interval	0.01	false	undefined	not submitted
BackupMonitoringPolicyCheckQ4	How often is the transmission of backups done?	periodically	0.0	false	undefined	not submitted
DataRestoreTestFrequencyQ1	How frequently is the data restore process tested?	at least once, typically twice to four times a year	0.05	false	undefined	not submitted
EncryptionPolicyCheckQ1	How are passwords or keys encrypted?	secure storage of user credentials	0.0	false	undefined	not submitted
EncryptionPolicyCheckQ2	How are APIs encrypted?	on the transport layer	0.0	false	undefined	not submitted
EncryptionPolicyCheckQ3	What encryption type is used?	cryptographic	0.0	false	undefined	not submitted
IncidentAnalysisFrequencyQ1	How often are procedures for vulnerabilities and incidents analyzed?	automated and regular vulnerability scanning	0.05	false	undefined	not submitted
PasswordPolicyQ3	What is the passwords rotation frequency?	4-5 times a year	0.11	false	undefined	not submitted
DigitalCertPolicy03	What is the validity period of wildcard digital certificates?	3 years	0.02	✓ true	undefined	not submitted

Cert. Management



MEDINA

Welcome to the Medina TEST environment.

- About
- Catalogue of Metrics
- Orchestrator
- Rules & Obligations
- Continuous Certificate Evaluation
- Risk Assessment
- Organisational Evidence Assessment

Zoom in | Zoom out | Reset zoom | Collapse all | Expand all | Instructi

Name: /subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine @ OPS-12.4

State: Non compliant

Value: 0

Weight: 1

Threshold: 1

Resource id: /subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine

Resource type: VirtualMachine

Resource weight: 1

Description: Describes whether resource "/subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine" satisfies requirement "OPS-12.4"

s project has received funding from
ie European Union's Horizon 2020
search and innovation programme
nder grant agreement No 952633.

MEDINA Trustworthiness System

MEDINA

Number of evidences

Number of evidences
6,625

Number of assessment results

Number of assessment results
10,091

Look for specific:

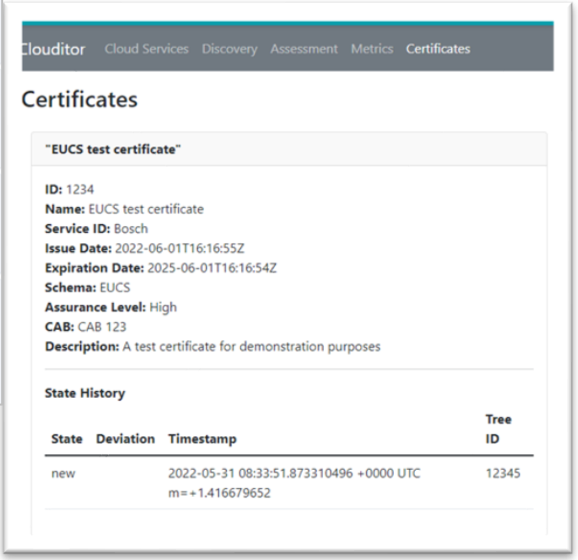
Evidence Id: Select... | Evidence Hash: Select... | Resource id: Select... | Tool id: Select... | CSP id: Select...

Apply changes | Cancel changes | Clear form

Registered evidences

Date per day	↓ timestamp	Evidence id	Resource id	Tool id	CSP id	Hash
2022-05-31	1653997279868061696	47ad89b2-00c2-4633-a12b-f6f8...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%94%9A%C0%CB%A7%8BCP%1...
2022-05-31	1653997278819119441	f14c6f62-5879-483a-b1f4-51ff7...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%DC%25eWF%15%BD%D1Qgg%...
2022-05-31	1653997277779828916	aef90215-dac7-4178-ab73-0a3...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%EA%A9%F0%A6%8A%16%F8b...
2022-05-31	1653997275718948203	0cf13b00-40b0-4d12-90d1-8e3...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	X%FD%05%AEmh %A0H0%28%0...

MEDINA



Clouditor | Cloud Services | Discovery | Assessment | Metrics | Certificates

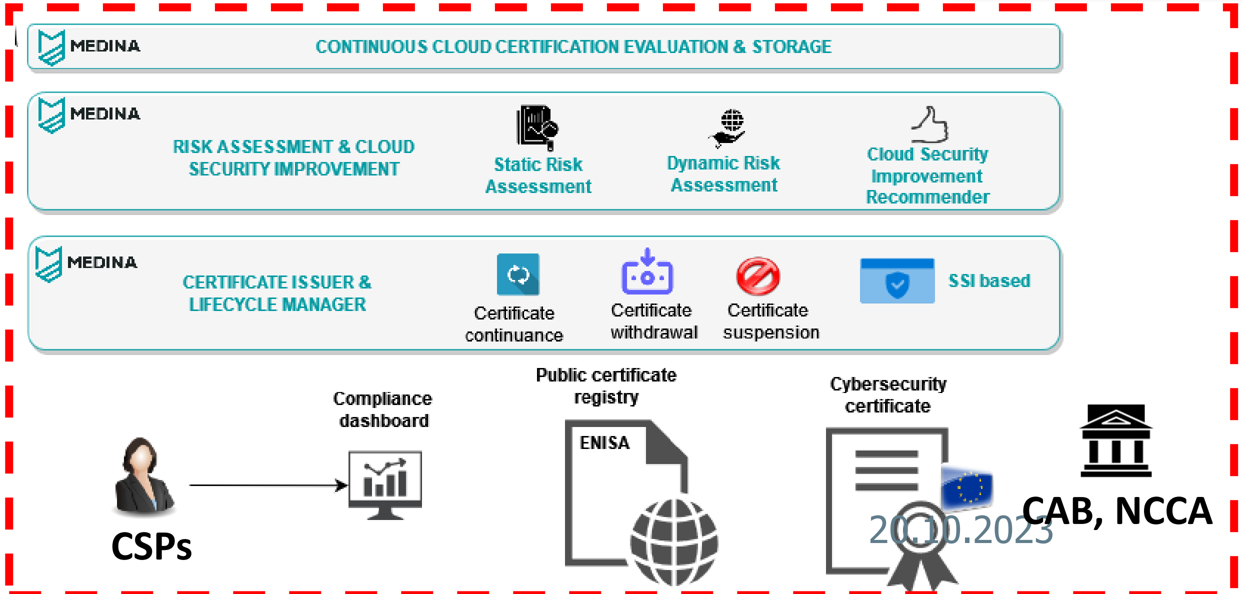
Certificates

"EUCS test certificate"

ID: 1234
Name: EUCS test certificate
Service ID: Bosch
Issue Date: 2022-06-01T16:16:55Z
Expiration Date: 2025-06-01T16:16:54Z
Schema: EUCS
Assurance Level: High
CAB: CAB 123
Description: A test certificate for demonstration purposes

State History

State	Deviation	Timestamp	Tree ID
new		2022-05-31 08:33:51.873310496 +0000 UTC m=+1.416679652	12345



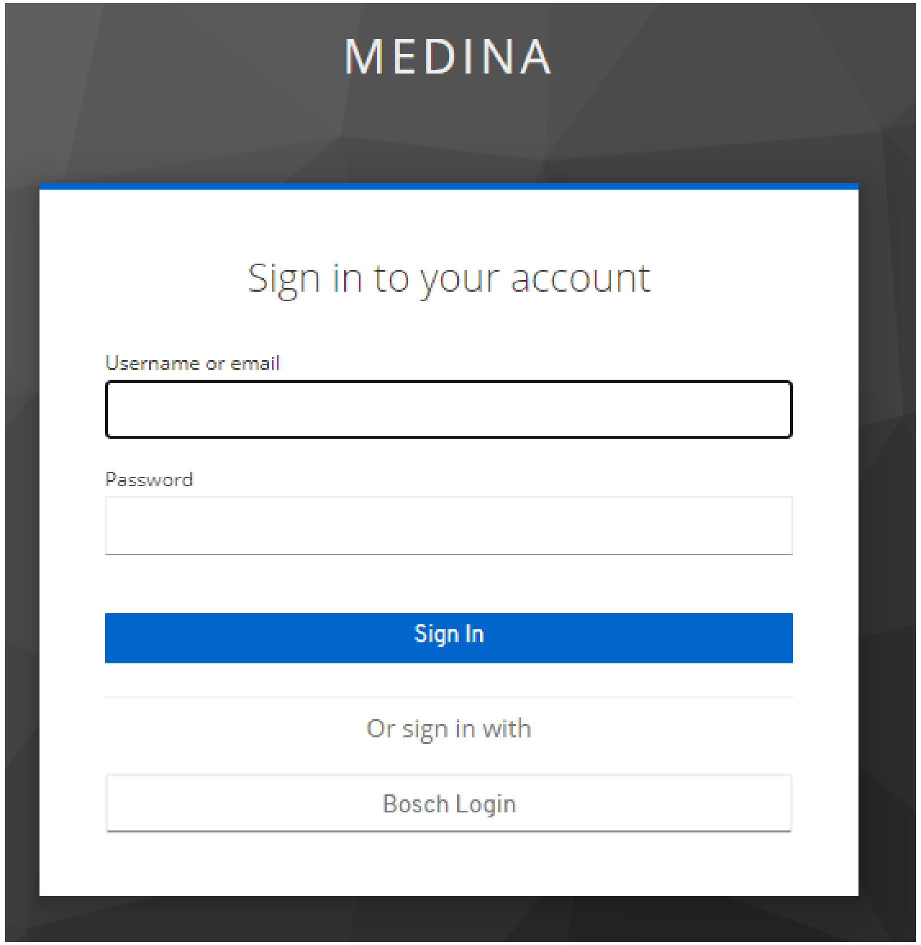
MEDINA — CONTINUOUS CLOUD CERTIFICATION EVALUATION & STORAGE

MEDINA — RISK ASSESSMENT & CLOUD SECURITY IMPROVEMENT: Static Risk Assessment; Dynamic Risk Assessment; Cloud Security Improvement Recommender

MEDINA — CERTIFICATE ISSUER & LIFECYCLE MANAGER: Certificate continuance; Certificate withdrawal; Certificate suspension; SSI based

Demo

MEDINA



MEDINA

Sign in to your account

Username or email

Password

Or sign in with

MEDINA

Summary

Life after MEDINA and enter COBALT

Summary

MEDINA

- MEDINA aims to facilitate adoption of EUCS, specifically for automated monitoring, while paving the road for continuous certification.
- Most of the proposed framework has been developed and integrated.
- Strong synergies have been built with relevant stakeholders in academia, industry, and standardization.
- Ongoing focus on integration, validation, and sustainability activities until the end of the project (Oct-2023).

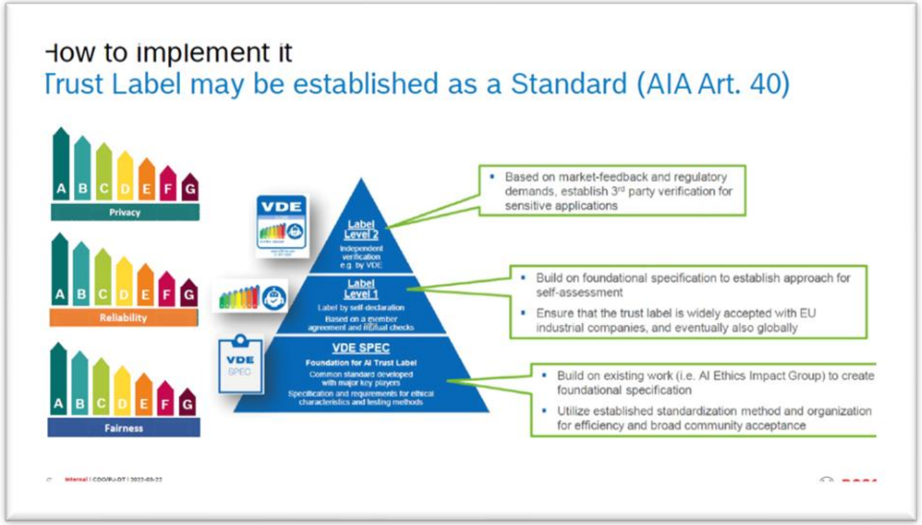
What Comes After MEDINA?

MEDINA

- Despite the interest of contacted stakeholders, a major challenge is about “productizing” the MEDINA framework.
  - Ongoing discussions with the EC’s “exploitation booster”
- Sadly, a relevant show-stopper for automation is on the Regulator-side.
  - Synergies and collaborations are expected to last well-beyond MEDINA’s lifetime
- Where else can be leveraged MEDINA’s framework?

Horizon EU – COBALT (2024 – 2026)

- Goal: extend the MEDINA framework to achieve continuous (automated) cybersecurity certification for **AI-enabled systems and Quantum Computing**.
- Pan-European consortium (DE, GR, ES, BE, FR, RO, CY) including Robert Bosch GmbH, UPC, Fraunhofer, ECSO, Red Alert Labs, and TüV Süd.
- Topics:
  - Automation of cybersecurity assessments (e.g., AIShield)
  - Cybersecurity metrics for compliance
  - Dynamic risk management
  - Protection of collected “evidence”
  - Compositional certification (e.g., cloud + AI)
  - Standardization and Regulation (alignment, influence)



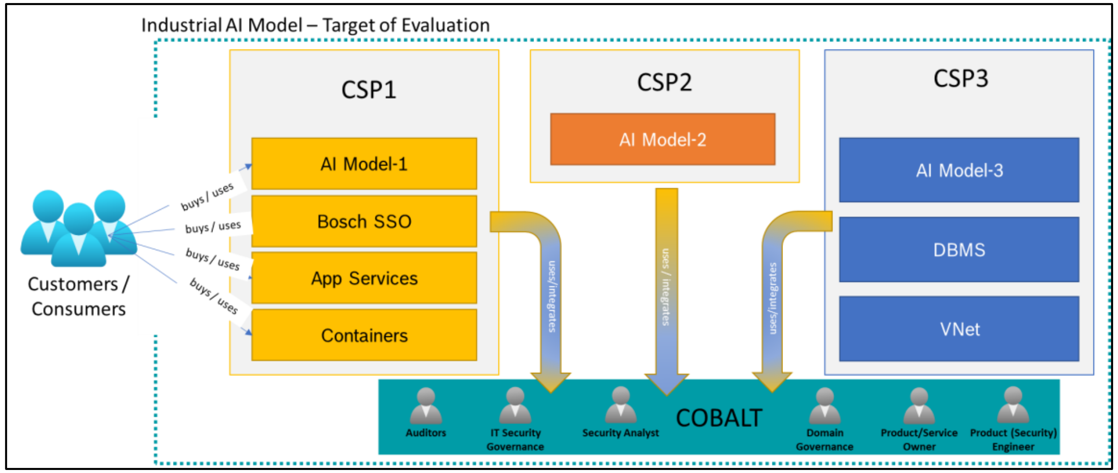
Ⅎow to implement it
Ⱶrust Label may be established as a Standard (AIA Art. 40)

- Based on market-feedback and regulatory demands, establish 3rd party verification for sensitive applications

- Build on foundational specification to establish approach for self-assessment
- Ensure that the trust label is widely accepted with EU industrial companies, and eventually also globally

- Build on existing work (i.e. AI Ethics Impact Group) to create foundational specification
- Utilize established standardization method and organization for efficiency and broad community acceptance

A B C D E F G
Privacy
A B C D E F G
Reliability
A B C D E F G
Fairness
VDE
Label Level 2
Independent verification e.g. by VDE
Label Level 1
Label by self-declaration
Based on a member agreement and mutual checks
VDE SPEC
Foundation for AI Trust Label
Common standard developed with major key players
Specification and requirements for ethical characteristics and testing methods
VDE SPEC
Internal | CDO/PJ-DT | 2022-03-22



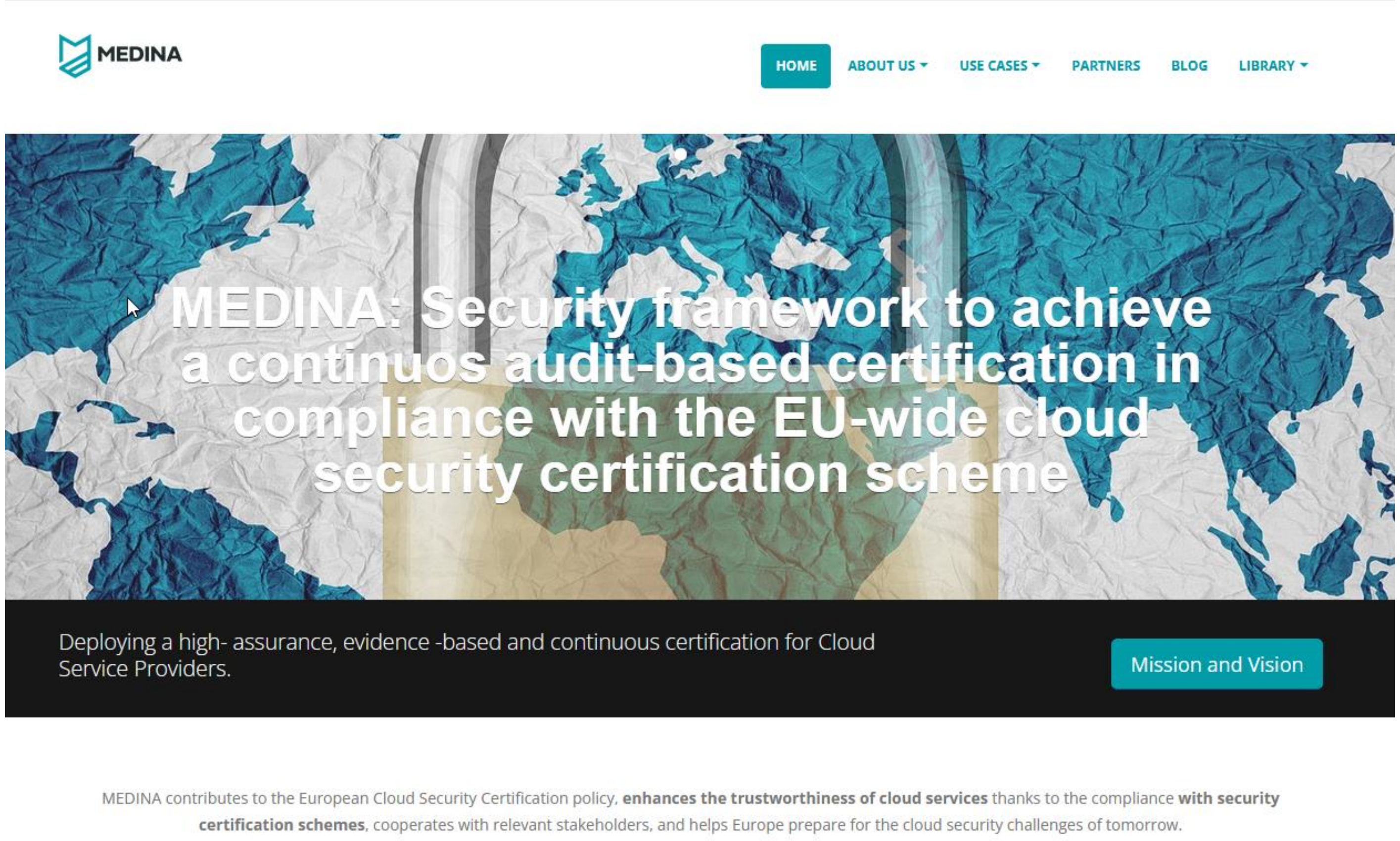
To certify or not to certify AI security? These are the open questions

- Is “AI certification” an enabler/synonym for “AI trustworthiness”?
- The AI perimeter to certify:
  - AI definition is a moving target,
  - Which AI components in an AI system shall be certified (AI software, model, training dataset, processes…)?
- Which AI attributes fall within the scope in terms of security properties?
  - Integrity (prevent attackers from degrading AI models and AI model functionality), Availability (stop attackers from interfering with normal operation of AI models), Confidentiality of sensitive data.
  - Other risks e.g. ethical risks or safety risks (relationships)
  - Explainability
- When AI certification is **really** needed? According to the EU’s AI Act (draft), criticality of AI in its context of application.

ENISA
AI CYBERSECURITY CONFERENCE
7 June, Brussels
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Further Reading

- Further details are available in our public reporting (deliverables) at https://medina-project.eu/public-deliverables
- Communication materials are available at https://medina-project.eu/communication-materials
- Framework demonstrator https://www.youtube.com/watch?v=fRFE61GZ3ZY



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

Your feedback

- Please open https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh

And feel free to share your opinion on the topic!

Únase en

slido.com

#9795 9089

MEDINA

Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com

MEDINA

Paving the road towards continuous audit-based certification for cloud services in Europe

Dr. Jesus Luna Garcia

Robert Bosch GmbH, Germany

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

Agenda

MEDINA

- Why (again) certification?
- Basic concepts
- H2020 MEDINA in a Nutshell
- Summary

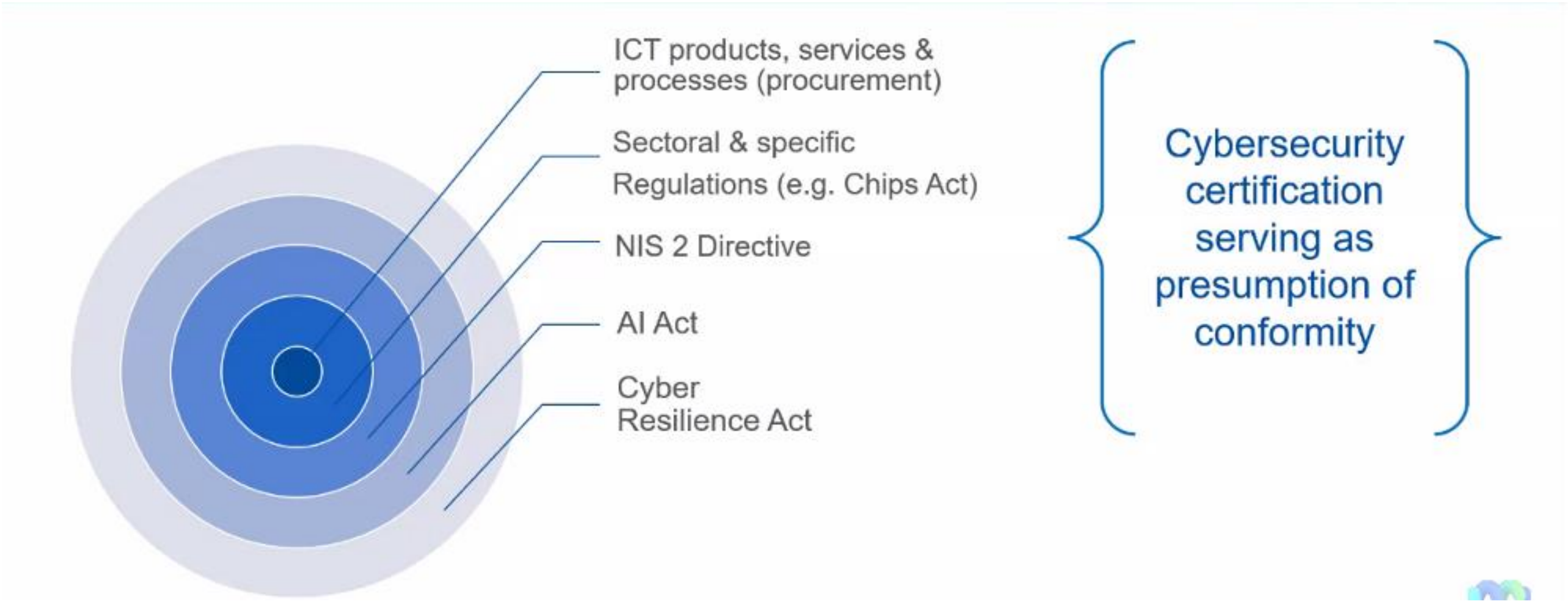
Why (again) certification?

Cybersecurity Deja-Vu

Created with dream.ai

Cybersecurity Certifications – the „new“ EU Silver Bullet (?)

- The role of cybersecurity certification is getting more prominent, whereas relevant EU-Regulations consider it as a mandatory requirement.


ICT products, services & processes (procurement)
Sectoral & specific Regulations (e.g. Chips Act)
NIS 2 Directive
AI Act
Cyber Resilience Act
Cybersecurity certification serving as presumption of conformity

Borrowed from ENISA's presentation during Cert WS (12.2022)

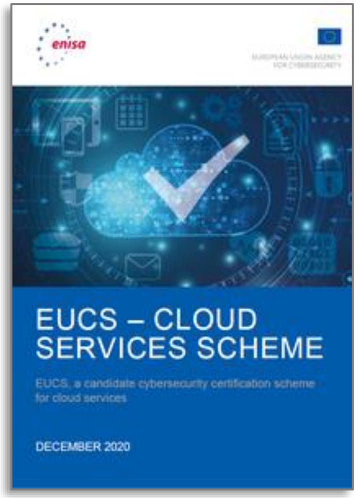
Certification “Made in the EU”

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation **EU-wide cybersecurity certification schemes** in order to:
  - provide an EU-wide cybersecurity baseline (requirements, audit methods)
  - enable customers to make risk-based decisions about cybersecurity
  - ***enable continuous cybersecurity compliance***
- ENISA (EU Cybersecurity Agency) nominated as responsible for developing the new EU-certification schemes.

What is being prepared by ENISA?

MEDINA

- Three EUCSA-derived certification schemes are under preparation by ENISA:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - **EUCS - Cybersecurity Certification Scheme for Cloud Services** → BOSCH
  - EU5G - Cybersecurity Certification Scheme for 5G
- …but more are expected to come (e.g., AI and IoT).
- How the (certification) future looks like?



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

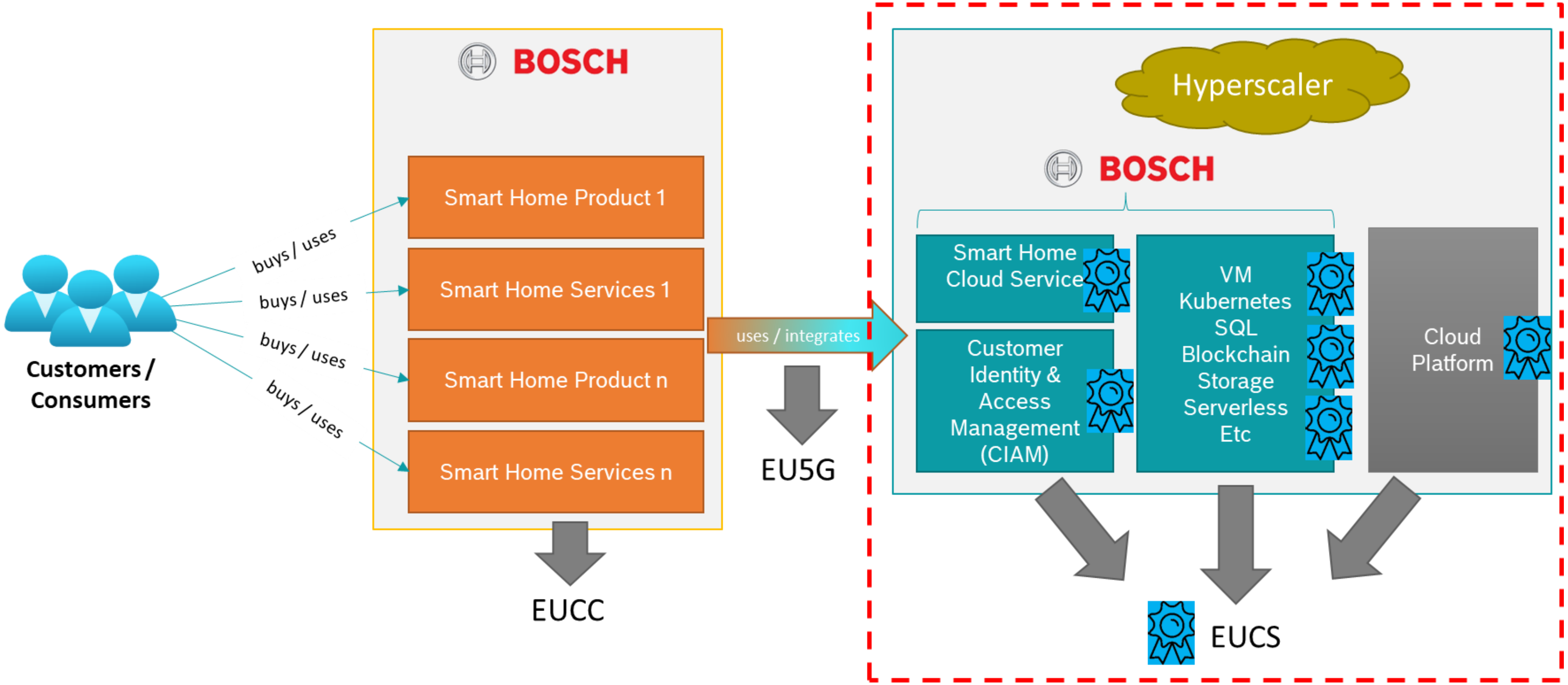
EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

Target Picture

MEDINA



$ ping audience.necs

- Let’s have some fun ☺
- Please open https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh

And feel free to share your opinion on the topic! 3 mins

Join at

slido.com

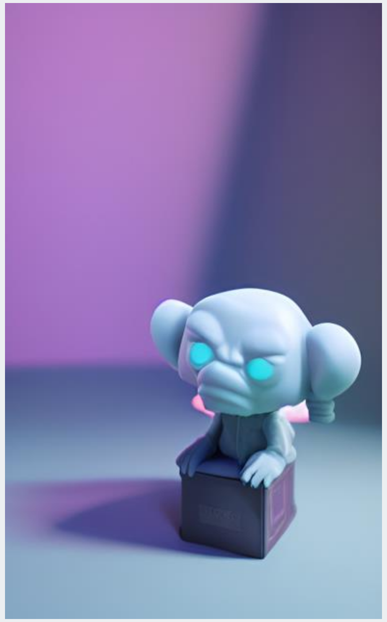
#9795 9089

MEDINA

Basic Concepts

Introducing the EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

Created with dream.ai



NeCS WS 2023

20.10.2023

Basics: Terminology

- **Conformity Assessment**: demonstration that specified requirements are fulfilled.
- **Certification:** the provision by an independent body (3rd party) of written assurance (a certificate) that the product, service or system in question is conformant.

- Certification is about assurance! Per-se, being certified doesn't mean it's secure.

Basics: Purpose and Scope

- Purpose:
  - Certification can be a useful tool to add credibility, by demonstrating that the Target Of Evaluation (TOE) meets the expectations (in terms of requirements) of customers.
- Scope (TOE) of Certification:
  - Process: ISMS, CSMS, etc.
  - Products: Firewalls, encryption devices, smart home appliance, automotive components, etc.
  - Service: Single sign-on, cloud services, etc.

Basics: EUCS at a glance

- ENISA started the development of EUCS early 2020.
  - Estimated GoLive Q1/2024
- Basic features:
  - Standards based (German C5, French SecNumCloud)
  - Focus on Cloud Services (e.g., SQL, VM, Web Apps), not Cloud Service Providers (e.g., AWS, Azure, GCP)
  - Introduces compositional certification
  - Defines three levels of assurance *(see next slide)*
  - Introduces automation for assessments *(see next slide)*

Basics: Levels of Assurance in EUCS

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment driven
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** risks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

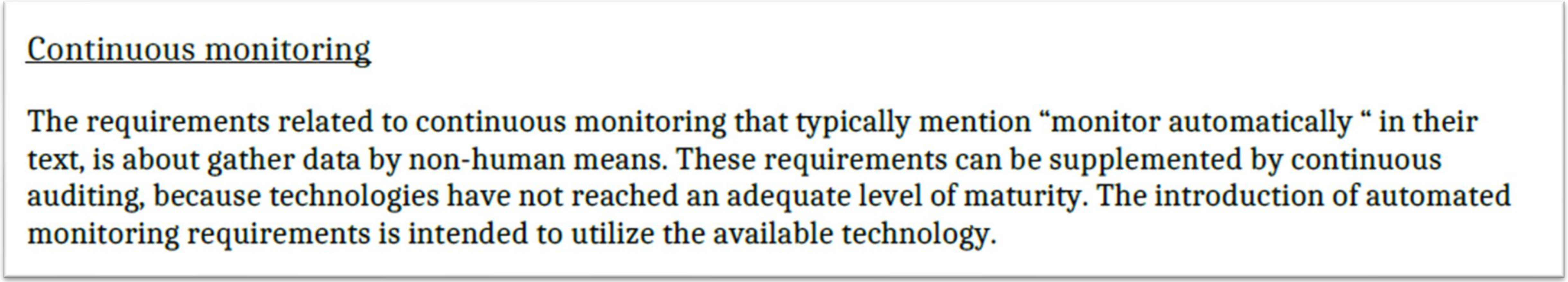
‘high’ level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

Basics: Continuous Monitoring in EUCS

- From 6th WD of EUCS1 specification (CEN CENELEC)

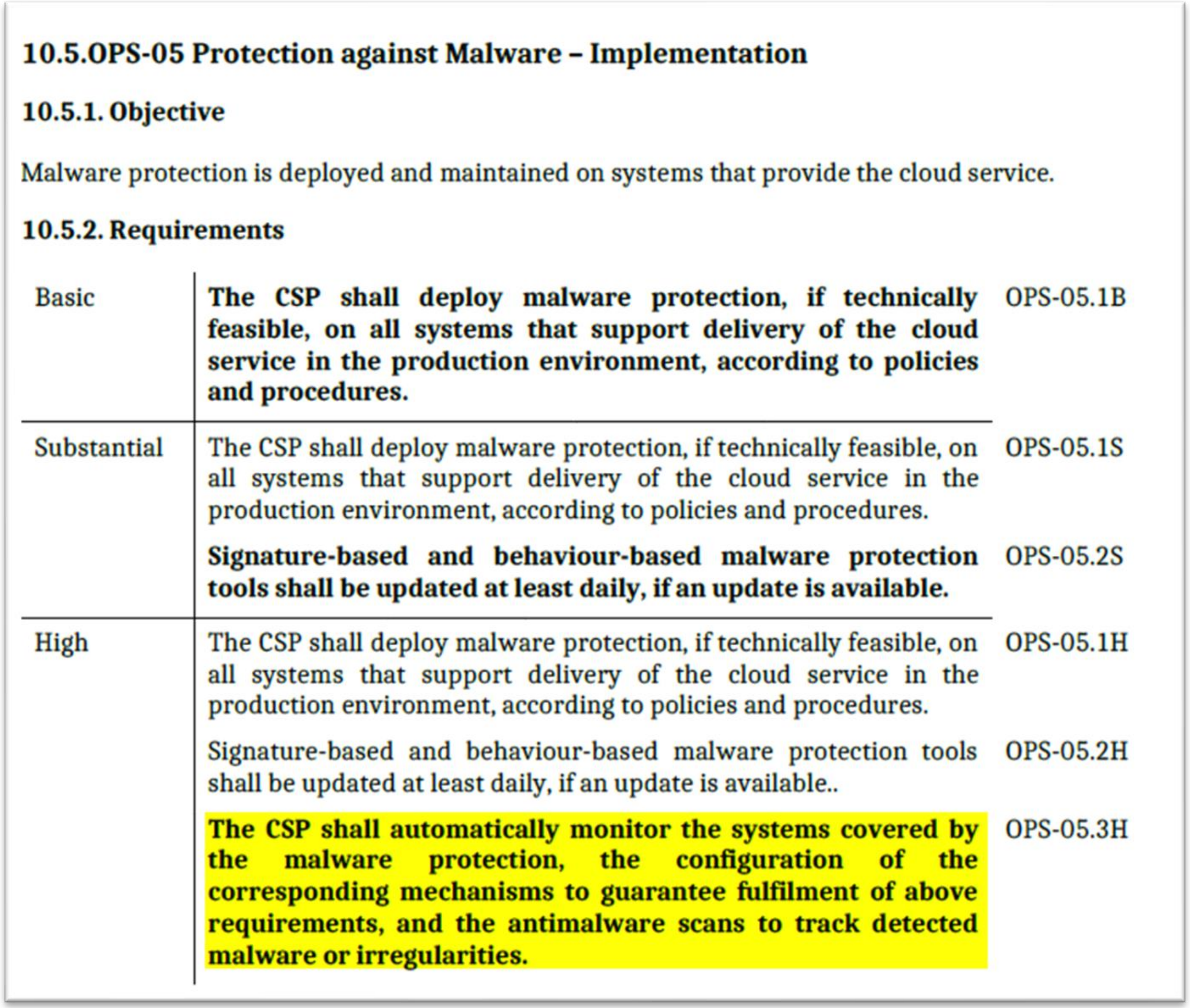


Continuous monitoring

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

Basics: Continuous Monitoring in EUCS

- “High” assurance requirement related to “continuous monitoring” (based on 6th WD from CEN CENELEC)



10.5.OPS-05 Protection against Malware – Implementation

10.5.1. Objective

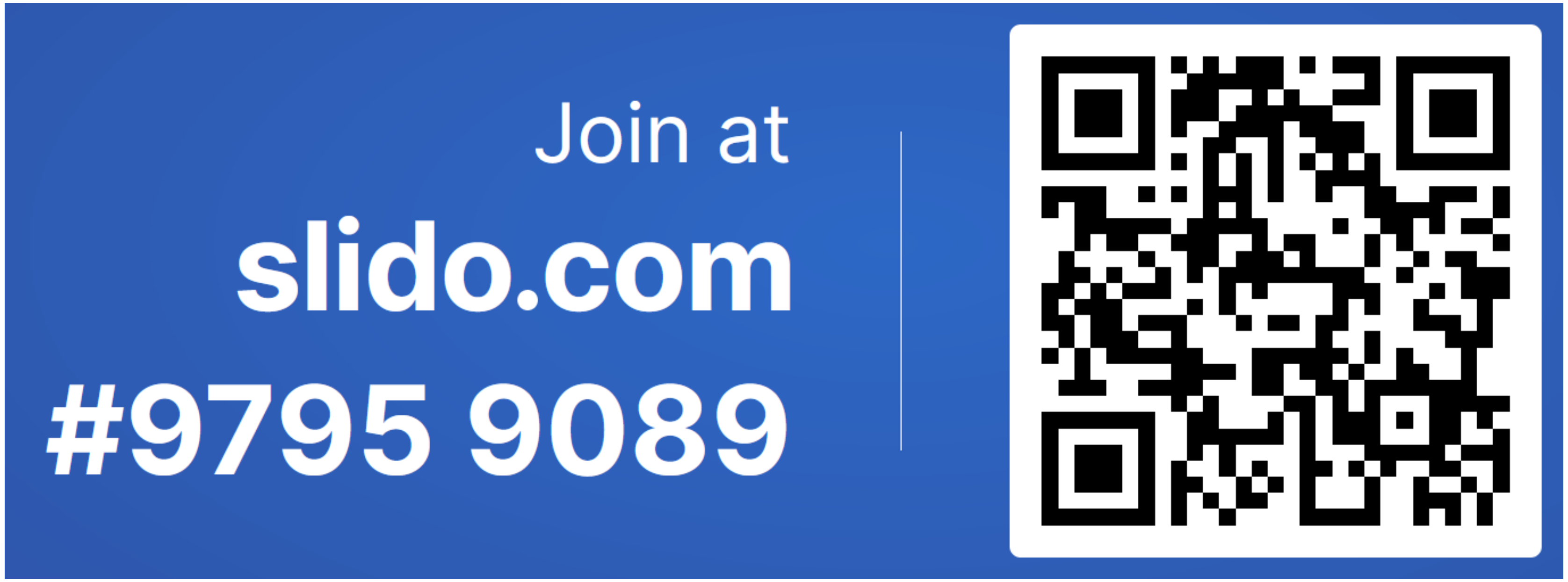
Malware protection is deployed and maintained on systems that provide the cloud service.

10.5.2. Requirements

Basic	**The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.**	OPS-05.1B
Substantial	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.	OPS-05.1S
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available.	OPS-05.2S
High	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.	OPS-05.1H
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available..	OPS-05.2H
	The CSP shall automatically monitor the systems covered by the malware protection, the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.	OPS-05.3H

$ ping audience.necs

- Do we really need EUCS?
  - Share your opinion! 3 mins https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh



Join at

slido.com

#9795 9089

H2020 MEDINA in a Nutshell

Paving the road towards EUCS

Created with dream.ai

NeCS WS 2023

20.10.2023

Why MEDINA?

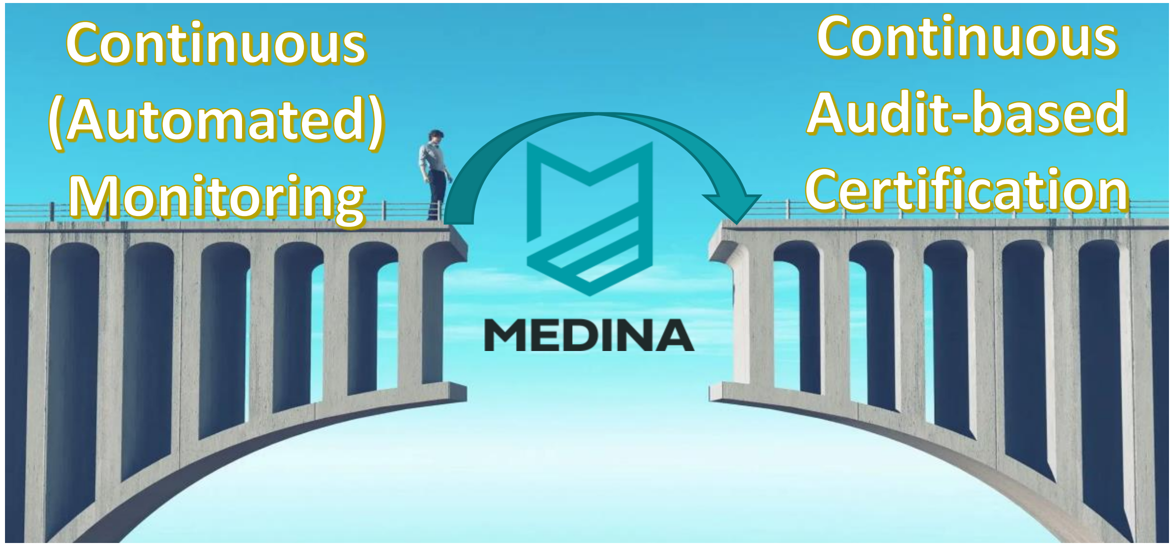
MEDINA

- The implementation of “continuous monitoring” brings some challenges to Cloud Service Providers, but also to auditors assessing those requirements.
  - Preliminary analysis documented in our whitepaper.
- How to approach EUCS-Continuous, and further develop it towards *continuous (automated) certification*?

Mission

- Provision of a **Security framework and tools** for achieving a **continuous audit-based certification**, through **trustworthy evidence-management methods.**

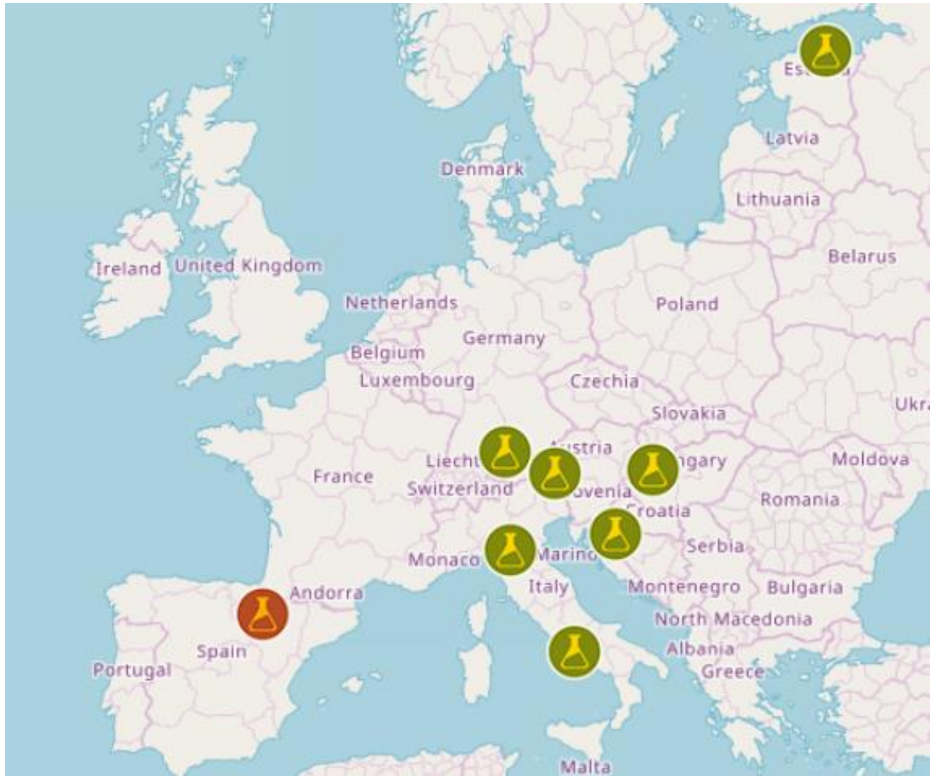
  - MEDINA primarily focuses on the **EUCS requirements for High Assurance**, where some degree of continuous (automated) monitoring is needed.
  - However, the MEDINA framework can be **extended to other EUCS requirements** at the substantial level, or even to **similar certification schemes** (e.g., BSI C5).


Continuous (Automated) Monitoring
MEDINA
Continuous Audit-based Certification

Who's Who in MEDINA?

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€



tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft

Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Challenges and Approaches

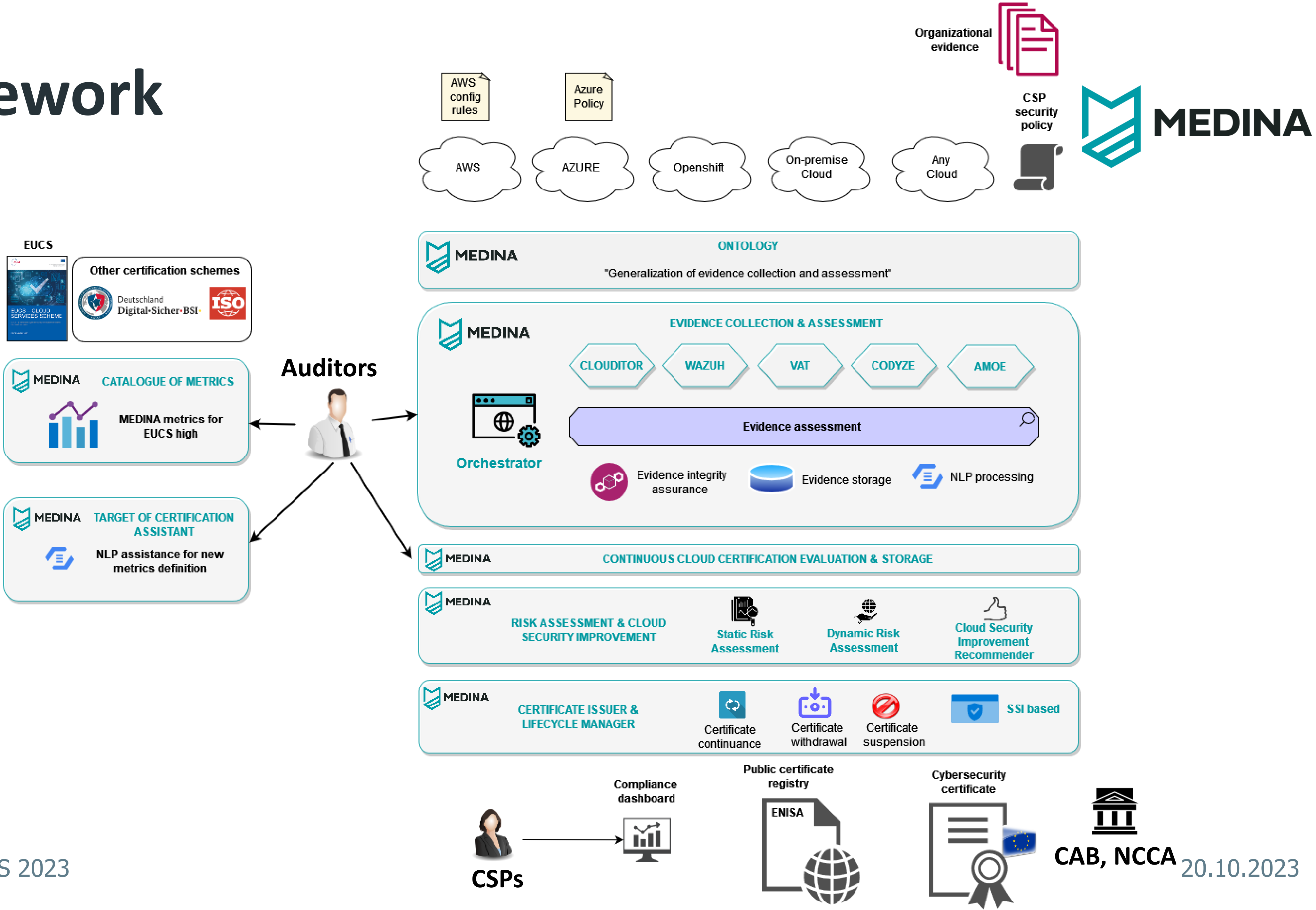
MEDINA

Existing Certifications	EUCS and MEDINA
Point in time certifications (e.g., once per-year)	Continuous certification based on automated monitoring
High costs and effort for certifying cloud services	NLP-driven automation to support audit processes (incl. evidence management)
Lack of transparency in assessed levels of security	Dynamic reporting provides different levels of details and transparency
High customization effort in commercial tools to support new schemes like EUCS	NLP-aided generation of automated assessments based on natural language requirements

Expected Benefits

- **Guidance** on the implementation of the controls, compliance **metrics and evidences** to be collected
- Support for **automatic compliance assessment** of EUCS and **other certification schemes**
- Ease the effort of **managing** (trustworthy) evidences in EUCS
- Standardization and awareness to pave the road for **continuous certification** (in particular with **Regulators in the EU and US**)

Framework



Organizational evidence

AWS config rules

Azure Policy

CSP security policy

AWS

AZURE

Openshift

On-premise Cloud

Any Cloud

MEDINA

EUCS

Other certification schemes

Deutschland Digital•Sicher•BSI•

ISO

MEDINA CATALOGUE OF METRICS

MEDINA metrics for EUCS high

Auditors

MEDINA TARGET OF CERTIFICATION ASSISTANT

NLP assistance for new metrics definition

MEDINA ONTOLOGY

"Generalization of evidence collection and assessment"

MEDINA EVIDENCE COLLECTION & ASSESSMENT

CLOUDITOR

WAZUH

VAT

CODYZE

AMOE

Orchestrator

Evidence assessment

Evidence integrity assurance

Evidence storage

NLP processing

MEDINA CONTINUOUS CLOUD CERTIFICATION EVALUATION & STORAGE

MEDINA RISK ASSESSMENT & CLOUD SECURITY IMPROVEMENT

Static Risk Assessment

Dynamic Risk Assessment

Cloud Security Improvement Recommender

MEDINA CERTIFICATE ISSUER & LIFECYCLE MANAGER

Certificate continuance

Certificate withdrawal

Certificate suspension

SSI based

Compliance dashboard

Public certificate registry

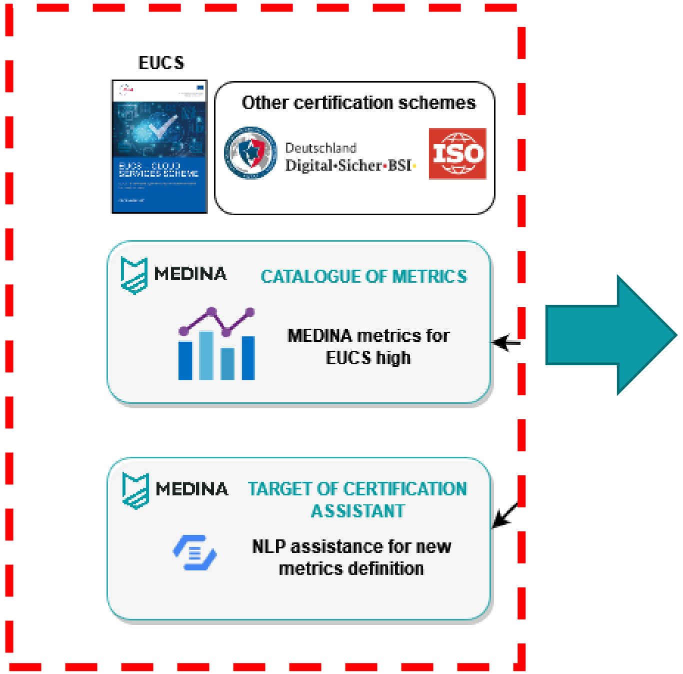
ENISA

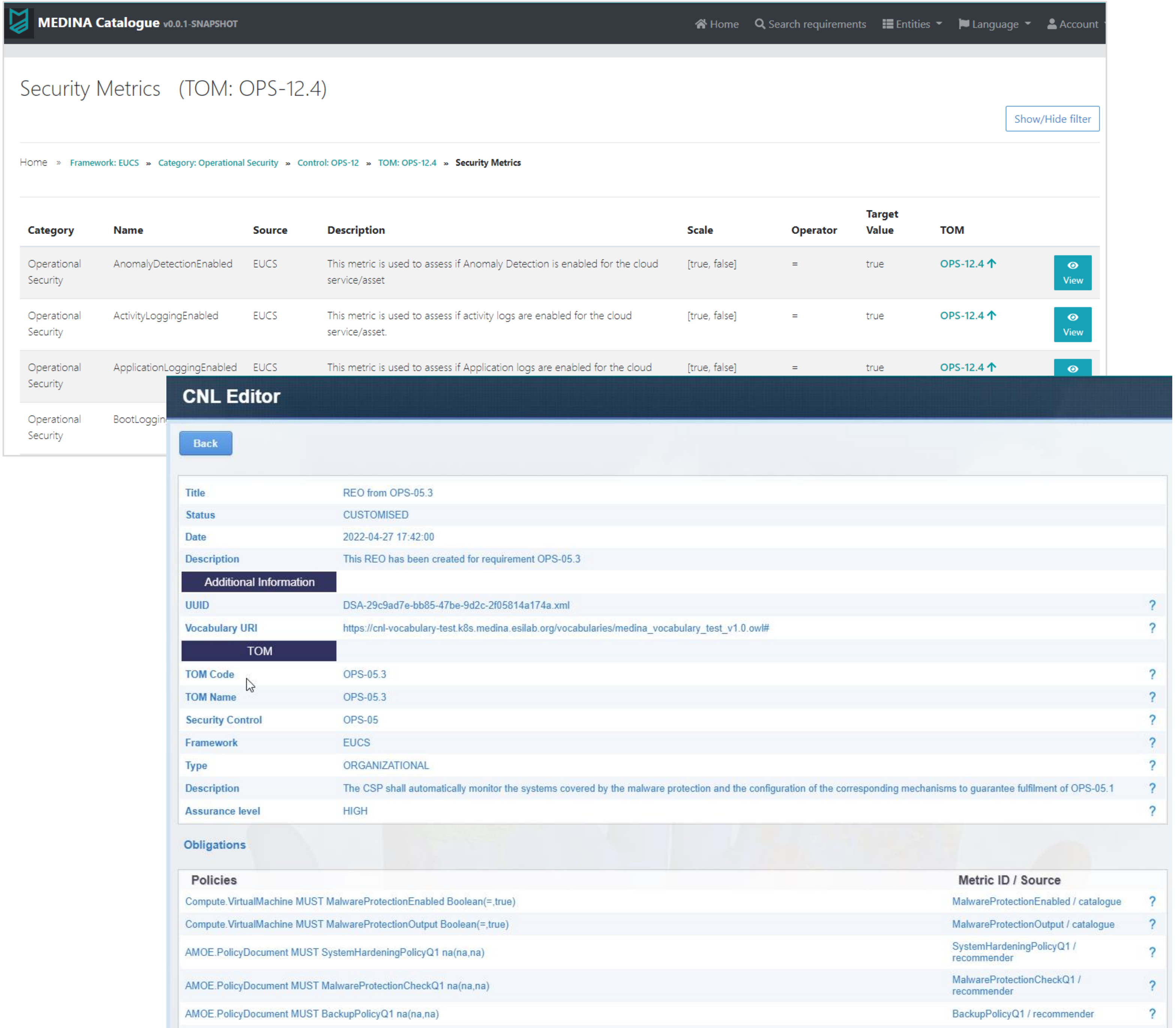
Cybersecurity certificate

CSPs

CAB, NCCA

ToE Initialization


EUCS
Other certification schemes
Deutschland Digital•Sicher•BSI•
ISO
MEDINA
CATALOGUE OF METRICS
MEDINA metrics for EUCS high
MEDINA
TARGET OF CERTIFICATION ASSISTANT
NLP assistance for new metrics definition



Security Metrics (TOM: OPS-12.4)

Home » Framework: EUCS » Category: Operational Security » Control: OPS-12 » TOM: OPS-12.4 » Security Metrics

Category	Name	Source	Description	Scale	Operator	Target Value	TOM	
Operational Security	AnomalyDetectionEnabled	EUCS	This metric is used to assess if Anomaly Detection is enabled for the cloud service/asset	[true, false]	=	true	OPS-12.4 ↑	View
Operational Security	ActivityLoggingEnabled	EUCS	This metric is used to assess if activity logs are enabled for the cloud service/asset.	[true, false]	=	true	OPS-12.4 ↑	View
Operational Security	ApplicationLoggingEnabled	EUCS	This metric is used to assess if Application logs are enabled for the cloud	[true, false]	=	true	OPS-12.4 ↑	
Operational Security	BootLoggin							

CNL Editor

Back

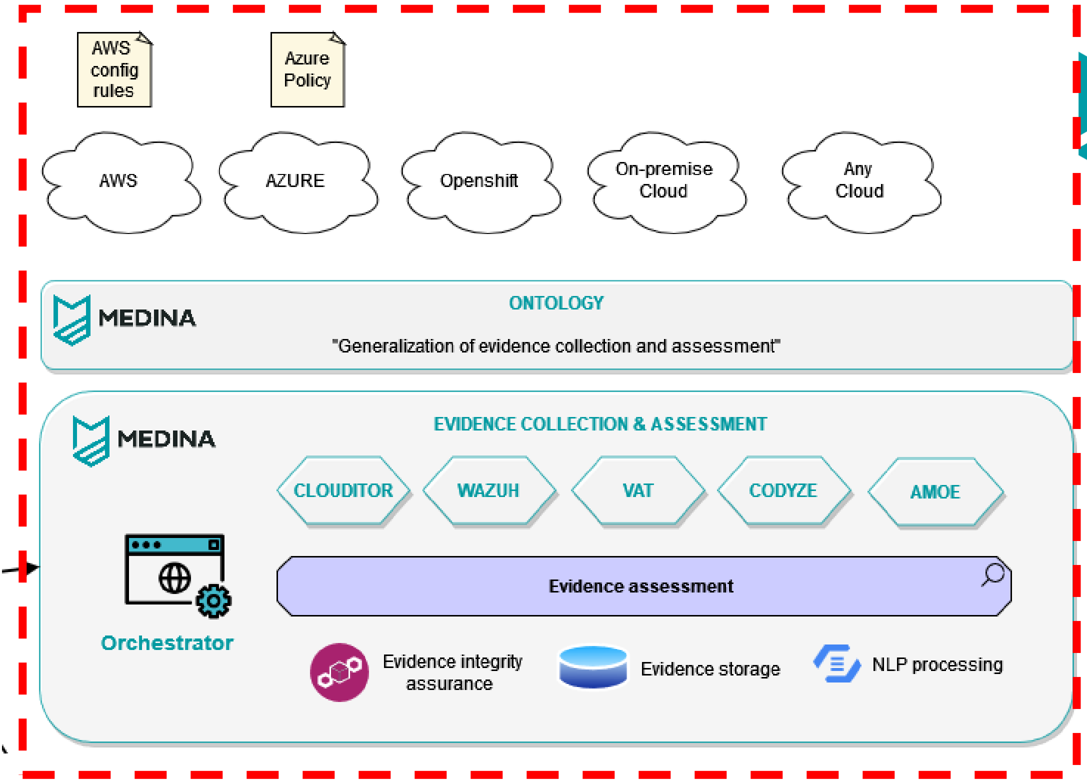
Title	REO from OPS-05.3
Status	CUSTOMISED
Date	2022-04-27 17:42:00
Description	This REO has been created for requirement OPS-05.3
Additional Information	
UUID	DSA-29c9ad7e-bb85-47be-9d2c-2f05814a174a.xml
Vocabulary URI	https://cnl-vocabulary-test.k8s.medina.esilab.org/vocabularies/medina_vocabulary_test_v1.0.owl#
TOM	
TOM Code	OPS-05.3
TOM Name	OPS-05.3
Security Control	OPS-05
Framework	EUCS
Type	ORGANIZATIONAL
Description	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
Assurance level	HIGH

Obligations

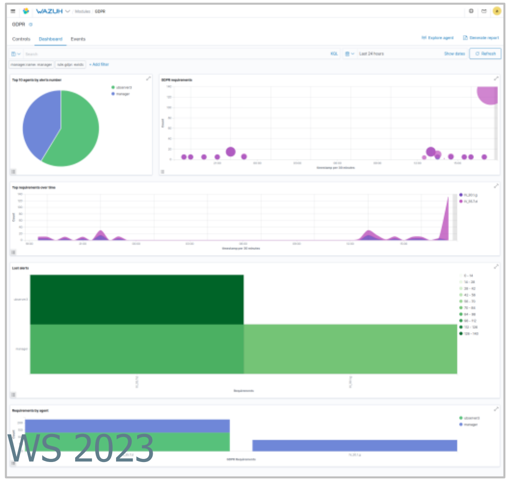
Policies	Metric ID / Source
Compute.VirtualMachine MUST MalwareProtectionEnabled Boolean(=,true)	MalwareProtectionEnabled / catalogue
Compute.VirtualMachine MUST MalwareProtectionOutput Boolean(=,true)	MalwareProtectionOutput / catalogue
AMOE.PolicyDocument MUST SystemHardeningPolicyQ1 na(na,na)	SystemHardeningPolicyQ1 / recommender
AMOE.PolicyDocument MUST MalwareProtectionCheckQ1 na(na,na)	MalwareProtectionCheckQ1 / recommender
AMOE.PolicyDocument MUST BackupPolicyQ1 na(na,na)	BackupPolicyQ1 / recommender

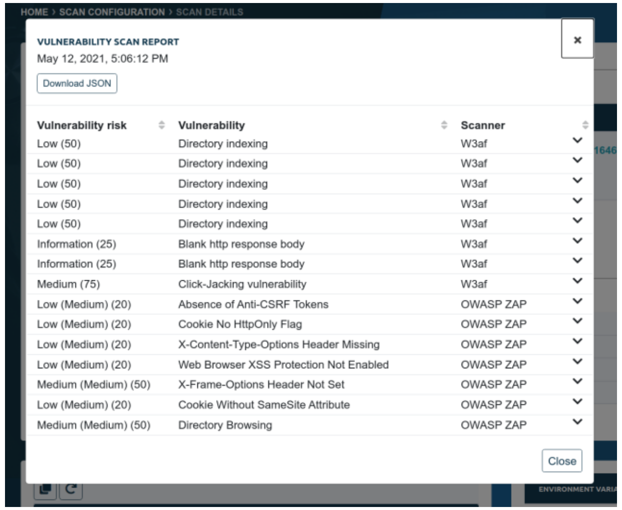
Ev. Collection

MEDINA



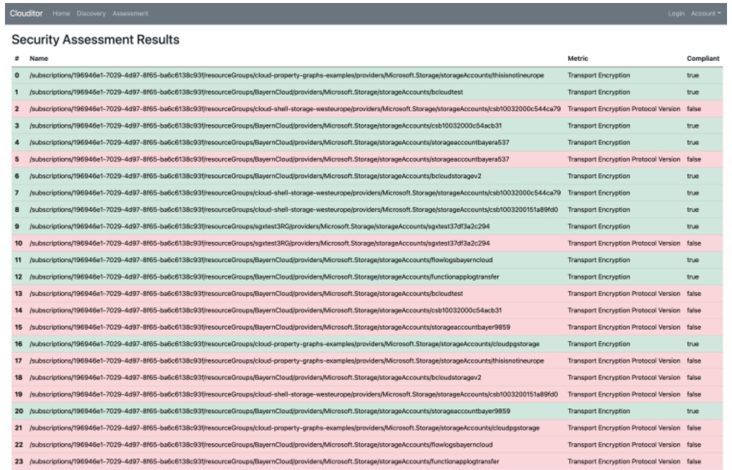
Technical evidence collectors





VULNERABILITY SCAN REPORT
May 12, 2021, 5:06:12 PM

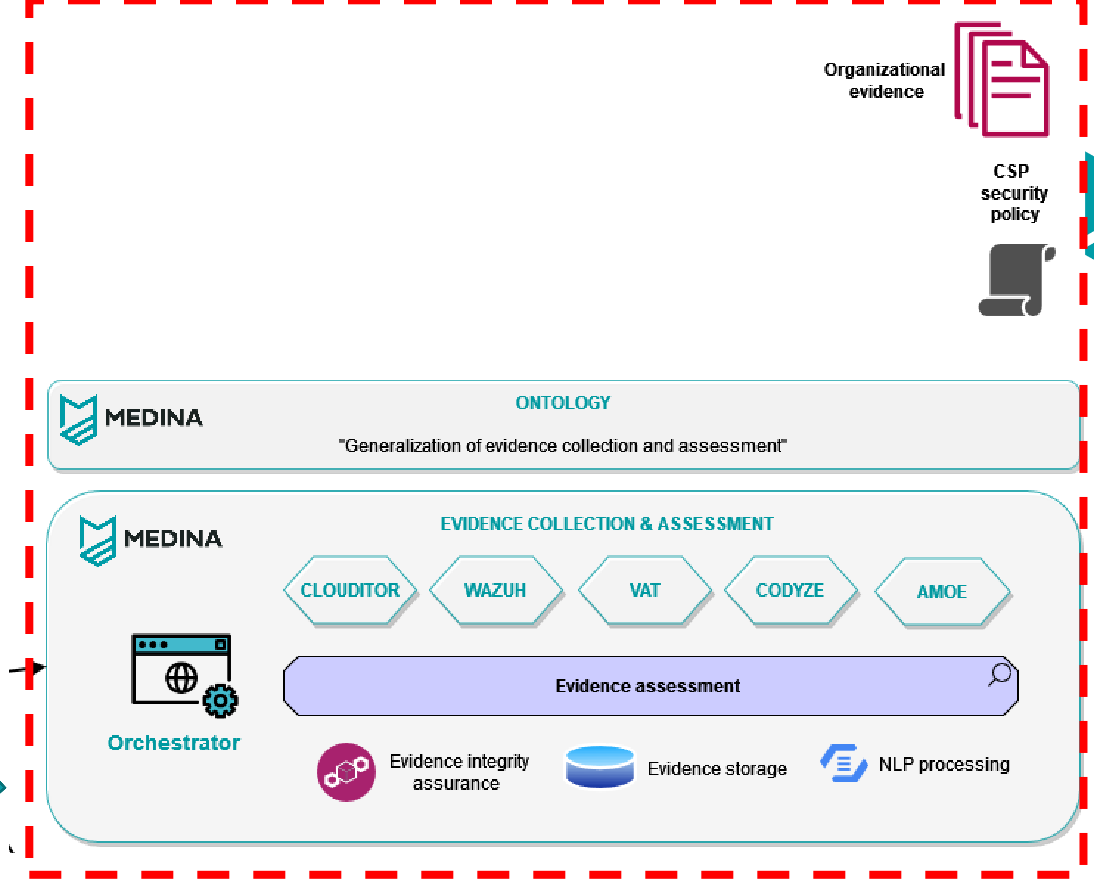
Vulnerability risk	Vulnerability	Scanner
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Low (50)	Directory indexing	W3af
Information (25)	Blank http response body	W3af
Information (25)	Blank http response body	W3af
Medium (75)	Click-Jacking vulnerability	W3af
Low (Medium) (20)	Absence of Anti-CSRF Tokens	OWASP ZAP
Low (Medium) (20)	Cookie No HttpOnly Flag	OWASP ZAP
Low (Medium) (20)	X-Content-Type-Options Header Missing	OWASP ZAP
Low (Medium) (20)	Web Browser XSS Protection Not Enabled	OWASP ZAP
Medium (Medium) (50)	X-Frame-Options Header Not Set	OWASP ZAP
Low (Medium) (20)	Cookie Without SameSite Attribute	OWASP ZAP
Medium (Medium) (50)	Directory Browsing	OWASP ZAP



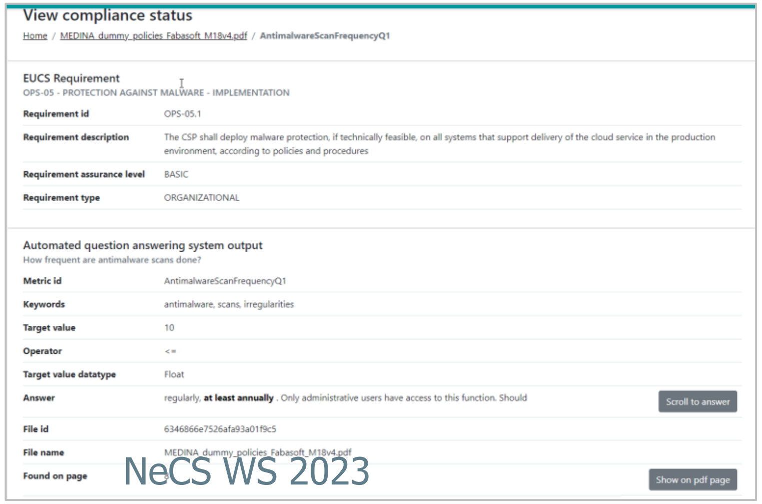
Security Assessment Results

#	Name	Metric	Compliant
0	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/thisisnotineurope	Transport Encryption	true
1	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudtest	Transport Encryption	true
2	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb10032000c544ca79	Transport Encryption Protocol Version	false
3	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/csb10032000c54acb31	Transport Encryption	true
4	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayera537	Transport Encryption	true
5	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayera537	Transport Encryption Protocol Version	false
6	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudstoragev2	Transport Encryption	true
7	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb10032000c544ca79	Transport Encryption	true
8	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb1003200151a89fd0	Transport Encryption	true
9	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/sgxtest3RG/providers/Microsoft.Storage/storageAccounts/sgxtest37df3a2c294	Transport Encryption	true
10	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/sgxtest3RG/providers/Microsoft.Storage/storageAccounts/sgxtest37df3a2c294	Transport Encryption Protocol Version	false
11	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/flowlogsbayerncloud	Transport Encryption	true
12	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/functionapplogtransfer	Transport Encryption	true
13	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudtest	Transport Encryption Protocol Version	false
14	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/csb10032000c54acb31	Transport Encryption Protocol Version	false
15	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayer9859	Transport Encryption Protocol Version	false
16	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/cloudpgstorage	Transport Encryption	true
17	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/thisisnotineurope	Transport Encryption Protocol Version	false
18	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/bcloudstoragev2	Transport Encryption Protocol Version	false
19	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-shell-storage-westeurope/providers/Microsoft.Storage/storageAccounts/csb1003200151a89fd0	Transport Encryption Protocol Version	false
20	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/storageaccountbayer9859	Transport Encryption	true
21	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/cloud-property-graphs-examples/providers/Microsoft.Storage/storageAccounts/cloudpgstorage	Transport Encryption Protocol Version	false
22	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/flowlogsbayerncloud	Transport Encryption Protocol Version	false
23	/subscriptions/196946e1-7029-4d97-8f65-ba6c6138c93f/resourceGroups/BayernCloud/providers/Microsoft.Storage/storageAccounts/functionapplogtransfer	Transport Encryption Protocol Version	false

Ev. Collection



NLP-evidence collectors



View compliance status

Home / MEDINA_dummy_policies_Fabasoft_M18v4.pdf / AntimalwareScanFrequencyQ1

EUCS Requirement

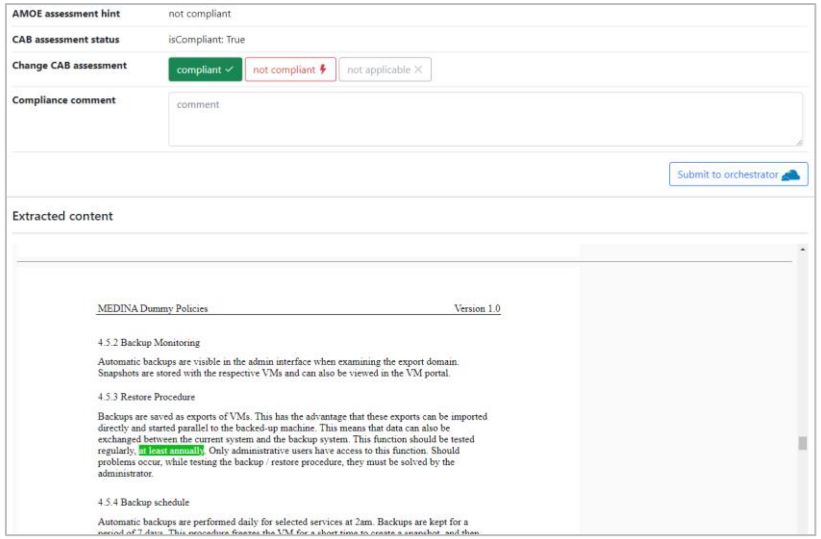
OPS-05 - PROTECTION AGAINST MALWARE - IMPLEMENTATION

Requirement id	OPS-05.1
Requirement description	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures
Requirement assurance level	BASIC
Requirement type	ORGANIZATIONAL

Automated question answering system output

How frequent are antimalware scans done?

Metric id	AntimalwareScanFrequencyQ1
Keywords	antimalware, scans, irregularities
Target value	10
Operator	<=
Target value datatype	Float
Answer	regularly, **at least annually** . Only administrative users have access to this function. Should
File id	6346866e7526afa93a01f9c5
File name	MEDINA_dummy_policies_Fabasoft_M18v4.pdf
Found on page	8



AMOE assessment hint	not compliant
CAB assessment status	isCompliant: True
Change CAB assessment	compliant ✓ not compliant ϟ not applicable ✕
Compliance comment	comment

Extracted content

MEDINA Dummy Policies Version 1.0

4.5.2 Backup Monitoring

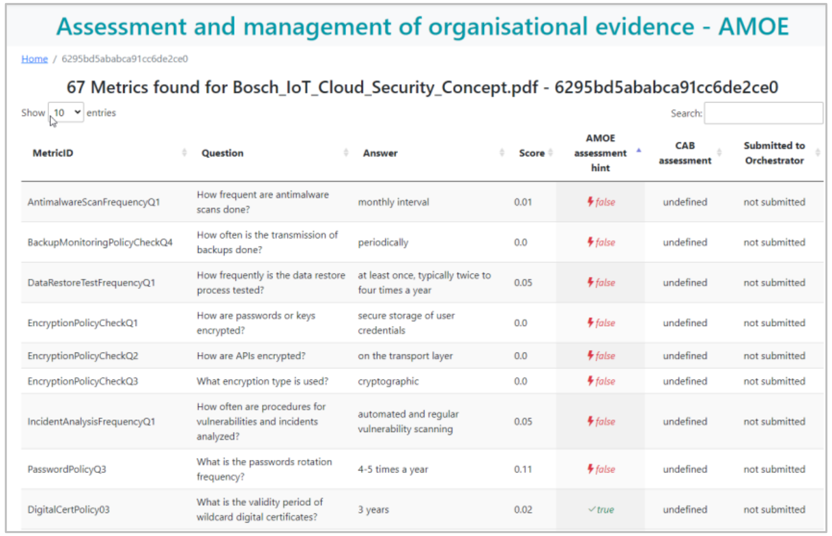
Automatic backups are visible in the admin interface when examining the export domain. Snapshots are stored with the respective VMs and can also be viewed in the VM portal.

4.5.3 Restore Procedure

Backups are saved as exports of VMs. This has the advantage that these exports can be imported directly and started parallel to the backed-up machine. This means that data can also be exchanged between the current system and the backup system. This function should be tested regularly, at least annually. Only administrative users have access to this function. Should problems occur, while testing the backup / restore procedure, they must be solved by the administrator.

4.5.4 Backup schedule

Automatic backups are performed daily for selected services at 2am. Backups are kept for a period of 7 days. This procedure freezes the VM for a short time to create a snapshot, and then



Assessment and management of organisational evidence - AMOE

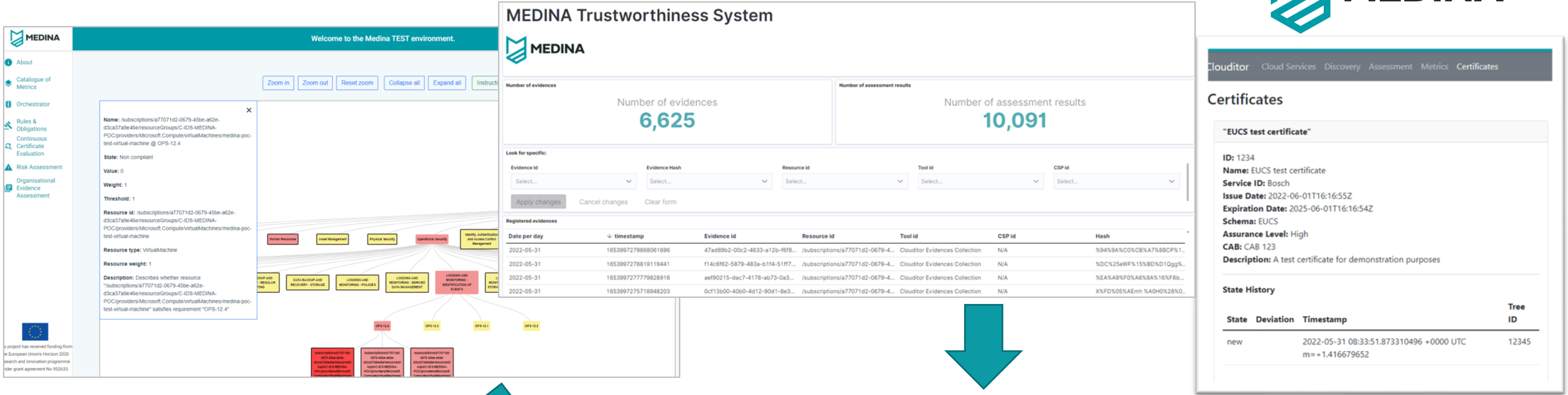
Home / 6295bd5ababca91cc6de2ce0

67 Metrics found for Bosch_IoT_Cloud_Security_Concept.pdf - 6295bd5ababca91cc6de2ce0

MetricID	Question	Answer	Score	AMOE assessment hint	CAB assessment	Submitted to Orchestrator
AntimalwareScanFrequencyQ1	How frequent are antimalware scans done?	monthly interval	0.01	ϟ false	undefined	not submitted
BackupMonitoringPolicyCheckQ4	How often is the transmission of backups done?	periodically	0.0	ϟ false	undefined	not submitted
DataRestoreTestFrequencyQ1	How frequently is the data restore process tested?	at least once, typically twice to four times a year	0.05	ϟ false	undefined	not submitted
EncryptionPolicyCheckQ1	How are passwords or keys encrypted?	secure storage of user credentials	0.0	ϟ false	undefined	not submitted
EncryptionPolicyCheckQ2	How are APIs encrypted?	on the transport layer	0.0	ϟ false	undefined	not submitted
EncryptionPolicyCheckQ3	What encryption type is used?	cryptographic	0.0	ϟ false	undefined	not submitted
IncidentAnalysisFrequencyQ1	How often are procedures for vulnerabilities and incidents analyzed?	automated and regular vulnerability scanning	0.05	ϟ false	undefined	not submitted
PasswordPolicyQ3	What is the passwords rotation frequency?	4-5 times a year	0.11	ϟ false	undefined	not submitted
DigitalCertPolicy03	What is the validity period of wildcard digital certificates?	3 years	0.02	✓ true	undefined	not submitted

Cert. Management

MEDINA



Name: /subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine @ OPS-12.4

State: Non compliant

Value: 0

Weight: 1

Threshold: 1

Resource id: /subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine

Resource type: VirtualMachine

Resource weight: 1

Description: Describes whether resource "/subscriptions/a77071d2-0679-45be-a62e-d3ca37a9e46e/resourceGroups/C-IDS-MEDINA-POC/providers/Microsoft.Compute/virtualMachines/medina-poc-test-virtual-machine" satisfies requirement "OPS-12.4"

s project has received funding from
e European Union's Horizon 2020
search and innovation programme
nder grant agreement No 952633.

MEDINA Trustworthiness System

MEDINA

Number of evidences

Number of evidences
6,625

Number of assessment results

Number of assessment results
10,091

Look for specific:

Evidence Id: Select...
Evidence Hash: Select...
Resource id: Select...
Tool id: Select...
CSP id: Select...

Apply changes · Cancel changes · Clear form

Registered evidences

Date per day	↓ timestamp	Evidence id	Resource id	Tool id	CSP id	Hash
2022-05-31	1653997279868061696	47ad89b2-00c2-4633-a12b-f6f8...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%94%9A%C0%CB%A7%8BCP%1...
2022-05-31	1653997278819119441	f14c6f62-5879-483a-b1f4-51ff7...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%DC%25eWF%15%BD%D1Qgg%...
2022-05-31	1653997277779828916	aef90215-dac7-4178-ab73-0a3...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	%EA%A9%F0%A6%8A%16%F8b...
2022-05-31	1653997275718948203	0cf13b00-40b0-4d12-90d1-8e3...	/subscriptions/a77071d2-0679-4...	Clouditor Evidences Collection	N/A	X%FD%05%AEmh %A0H0%28%0...

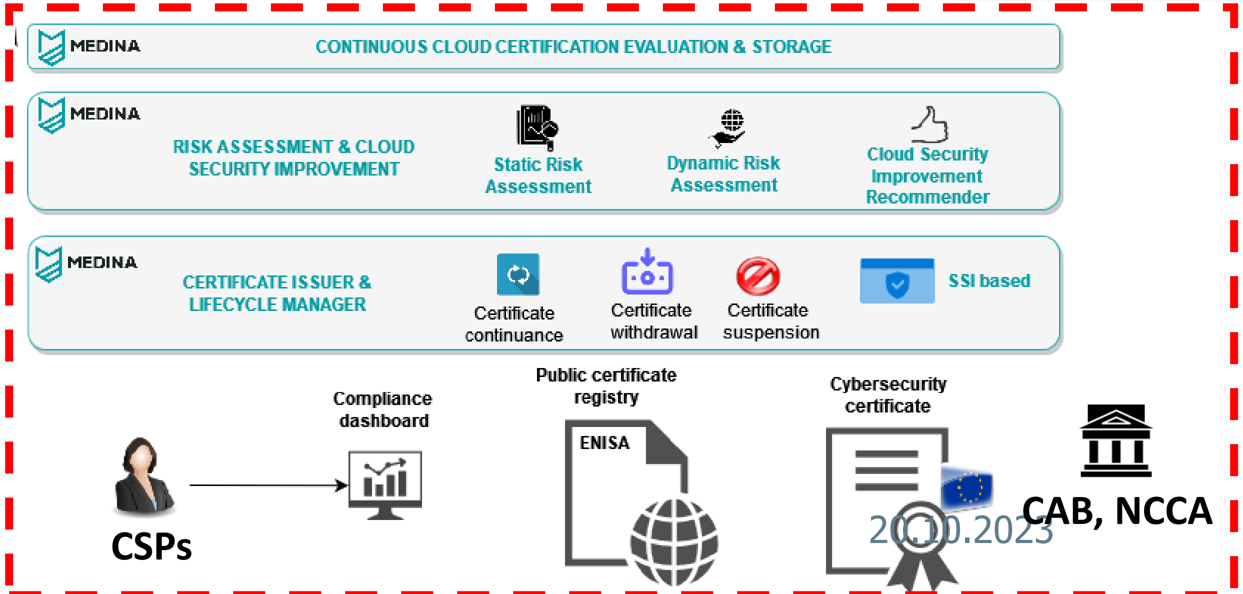
Certificates

"EUCS test certificate"

ID: 1234
Name: EUCS test certificate
Service ID: Bosch
Issue Date: 2022-06-01T16:16:55Z
Expiration Date: 2025-06-01T16:16:54Z
Schema: EUCS
Assurance Level: High
CAB: CAB 123
Description: A test certificate for demonstration purposes

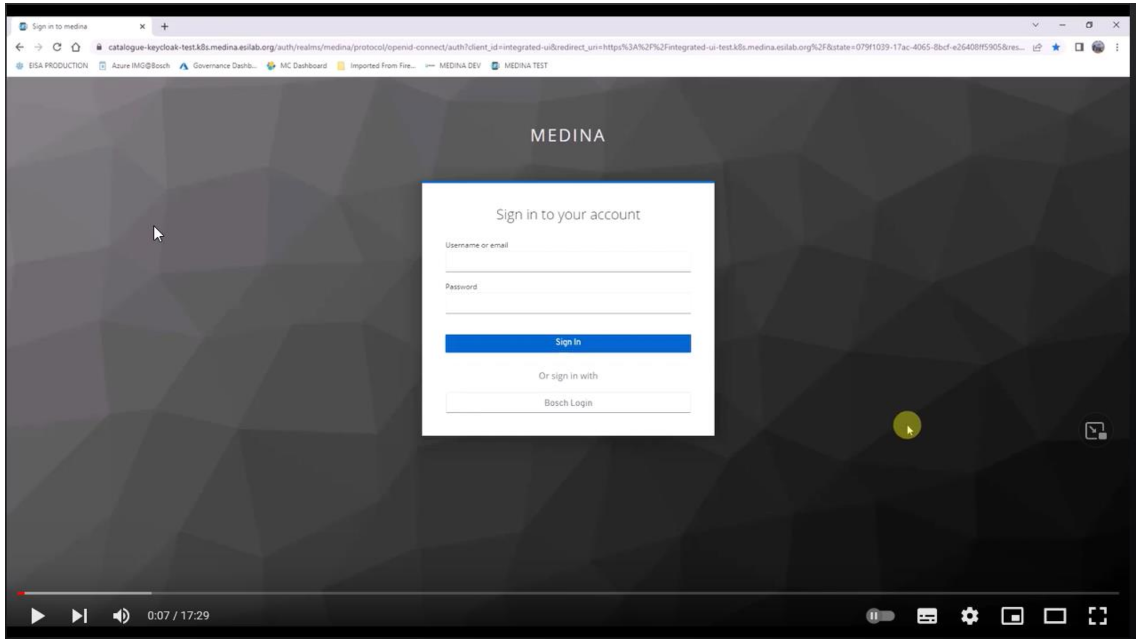
State History

State	Deviation	Timestamp	Tree ID
new		2022-05-31 08:33:51.873310496 +0000 UTC m=+1.416679652	12345



MEDINA
CONTINUOUS CLOUD CERTIFICATION EVALUATION & STORAGE
MEDINA
RISK ASSESSMENT & CLOUD SECURITY IMPROVEMENT
Static Risk Assessment
Dynamic Risk Assessment
Cloud Security Improvement Recommender
MEDINA
CERTIFICATE ISSUER & LIFECYCLE MANAGER
Certificate continuance
Certificate withdrawal
Certificate suspension
SSI based
Compliance dashboard
Public certificate registry
ENISA
Cybersecurity certificate
CSPs
CAB, NCCA

Initial Prototype Available



catalogue-keycloak-test.k8s.medina.esilab.org/auth/realms/medina/protocol/openid-connect/auth?client_id=integrated-ui&redirect_uri=https%3A%2F%2Fintegrated-ui-test.k8s.medina.esilab.org%2F&state=079f1039-17ac-4065-8bcf-e26408ff5905&res...

Summary

Life after MEDINA

Created with dream.ai

Summary

- MEDINA aims to facilitate adoption of EUCS, specifically for automated monitoring, while paving the road for continuous certification.
- Most of the proposed framework has been developed and integrated.
- Strong synergies have been built with relevant stakeholders in academia, industry, and standardization.
- Ongoing focus on integration, validation, and sustainability activities until the end of the project (Oct-2023).

What Comes After MEDINA?

- Despite the interest of contacted stakeholders, a major challenge is about “productizing” the MEDINA framework.
  - Ongoing discussions with the EC’s “exploitation booster”
- Sadly, a relevant show-stopper for automation is on the Regulator-side.
  - Synergies and collaborations are expected to last well-beyond MEDINA’s lifetime
- Where else can be leveraged MEDINA’s framework?
  - A few words about AI trustworthiness ☺

Realizing an AI Trustworthiness framework

- Defining AI trustworthiness:
  - Lack of consensus on what AI trustworthiness means.
  - Some proposals go well beyond cybersecurity (e.g., transparency, fairness, accountability).
  - Others add cybersecurity as a dimension of either robustness, reliability, or safety.

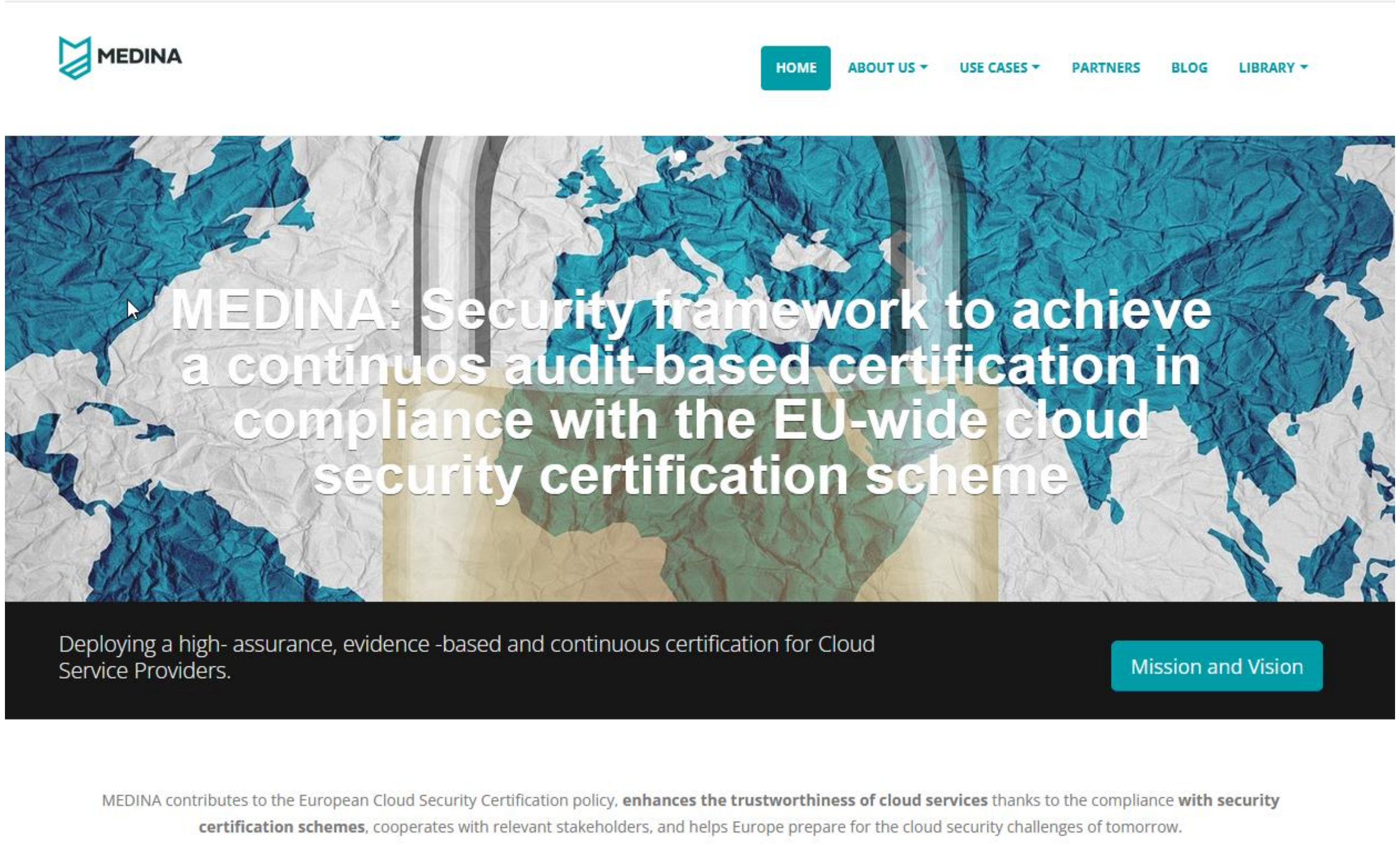
- Risk management framework for AI:
  - Based on the notion/dimensions of “trustworthiness”.
  - What makes *special* an AI-RMF?
  - How to *measure* risk in an AI system (quantitative/qualitat ive)?

- Conformance assessments:
  - Also depend on the notion of trustworthiness ☺
  - 3rd party certification vs Self-issued Assessment of Conformity.
  - Which requirements to assess?
  - Holistic perspective (e.g., including cloud platform, edge).
  - *Continuous (automated)* vs Point-in-time assessments.
  - Standard-based (although no standards are available).

Further Reading

MEDINA

- Further details are available in our public reporting (deliverables) at https://medina-project.eu/public-delivera
- Communication materials are available at https://medina-project.eu/communication-materials



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

Share your feedback about MEDINA – and enjoy your dinner!

https://app.sli.do/event/uwZdcw6TJgAVYUKz1Vznfh

Join at

slido.com

#9795 9089

MEDINA

Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com

ASSESSING THE TRUSTWORTHINESS OF AI SYTEMS

DR. JESUS LUNA GARCIA
CYBERSECURITY GOVERNANCE – AI AND CLOUD

ROBERT BOSCH GMBH (GERMANY)

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

BOSCH

Agenda

1. Background
2. Challenges
3. Work in Progress

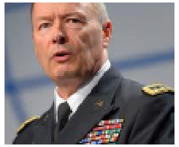
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

Background

AIoT – the broken promise of trust and cybersecurity

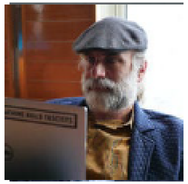
- AI-enabled IoT systems (AIoT) are an ever-growing global market.
  - We refer not only to AI embedded into IoT devices, but also to AI-enabled (cloud) services for IoT.
- Parallel to its growth, consumer trust in AIoT systems has shaken since several years.
  - Recognized cybersecurity experts starting to consider it as a lost cause.
- What shall we (i.e., research, industry, policy makers, …) do to bring back trust to AIoT systems? What does it mean “trustworthiness” in AI?

“Unsecurable”
Chris Inglis (2010), Former Deputy Director National Security Agency



“Indefensible”
Gen. Keith Alexander (2011), Former Director NSA und Commander of the United States Cyber Command

“Hopeless”
Ron Rivest (2012), Co-Inventor of RSA-Crypto Systems, Turing Award (2002)

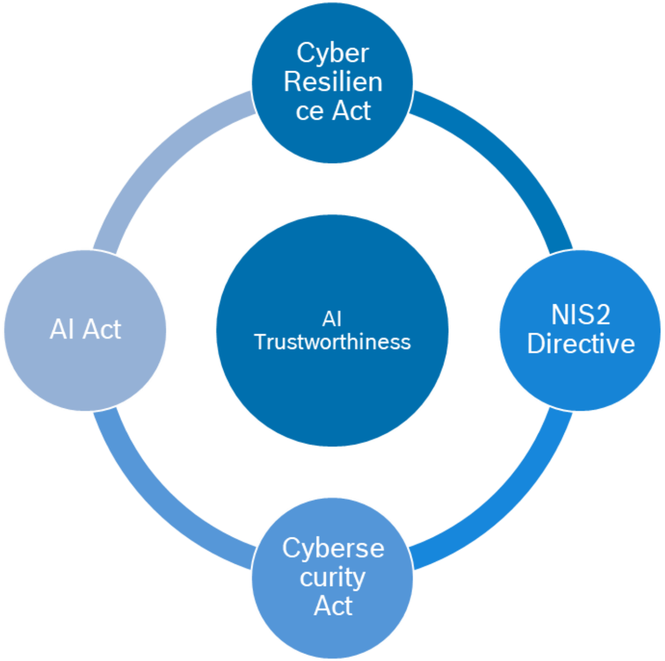


“Lousy IoT Security”
Bruce Schneier (2019) Writer, fellow and lecturer at Harvard's Kennedy School, board member of Electronic Frontier Foundation

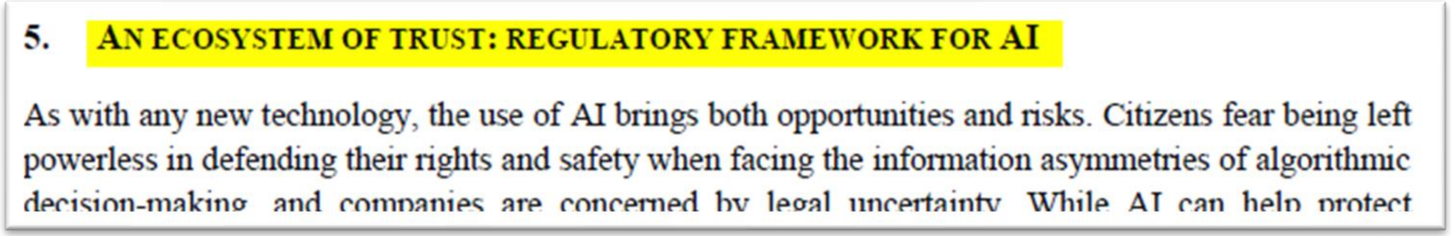
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 952633

Background

E.g., EU legislation support towards AIoT Trustworthiness



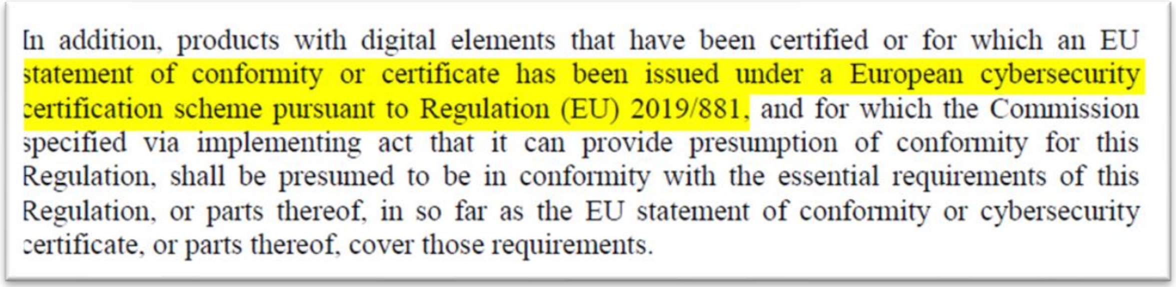
High Level Expert Group on AI



5. AN ECOSYSTEM OF TRUST: REGULATORY FRAMEWORK FOR AI

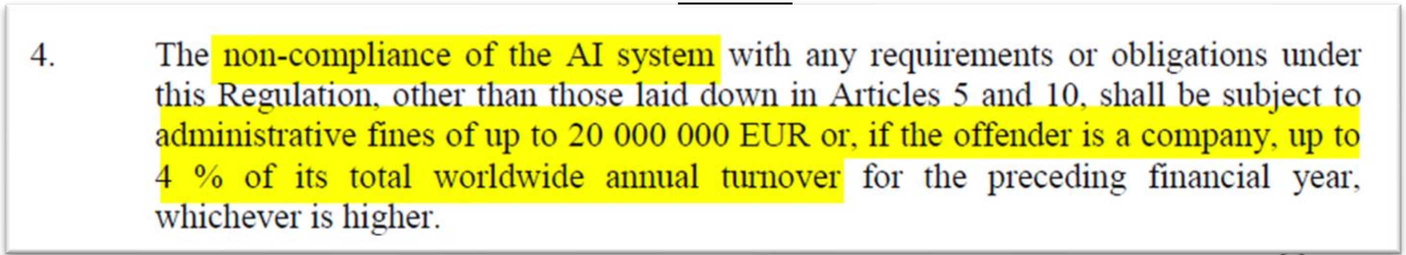
As with any new technology, the use of AI brings both opportunities and risks. Citizens fear being left powerless in defending their rights and safety when facing the information asymmetries of algorithmic decision-making, and companies are concerned by legal uncertainty. While AI can help protect

Cyber Resilience Act



In addition, products with digital elements that have been certified or for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881, and for which the Commission specified via implementing act that it can provide presumption of conformity for this Regulation, shall be presumed to be in conformity with the essential requirements of this Regulation, or parts thereof, in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.

AI Act



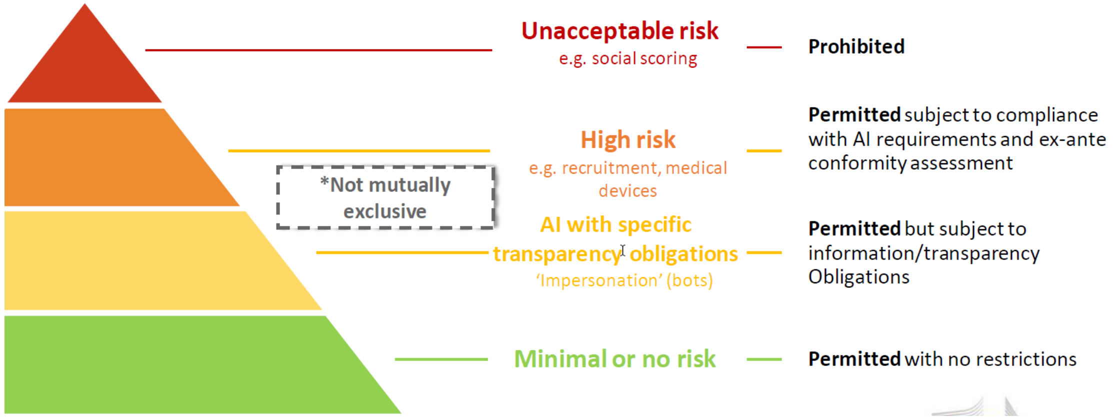
4. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

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

Background

What do these Regulations imply for the industry?

Risk Based



Unacceptable risk e.g. social scoring — **Prohibited**

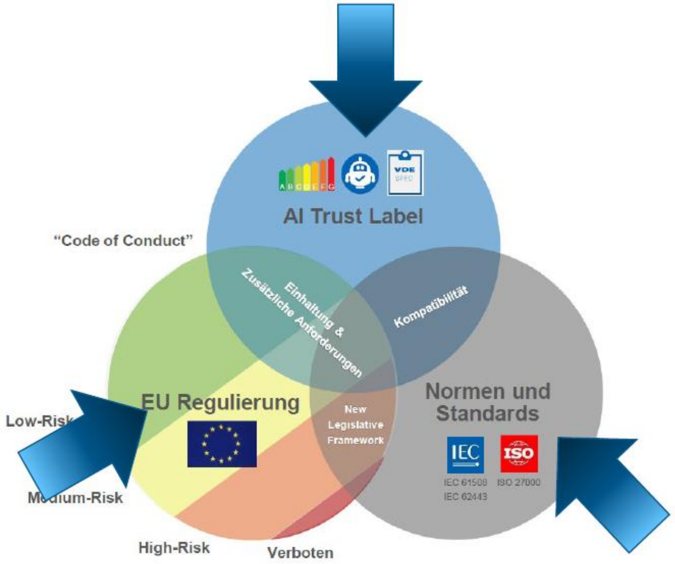
High risk e.g. recruitment, medical devices — **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

*Not mutually exclusive

AI with specific transparency obligations 'Impersonation' (bots) — **Permitted** but subject to information/transparency Obligations

Minimal or no risk — **Permitted** with no restrictions

Conformant



…and of course, we need to define what "trustworthiness" means for AI systems ☺

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

Challenges (or at least some of these)

Realizing an AI Trustworthiness framework

- Defining AI trustworthiness:
  - Lack of consensus on what AI trustworthiness means.
  - Some proposals go well beyond cybersecurity (e.g., transparency, fairness, accountability).
  - Others add cybersecurity as a dimension of either robustness, reliability, or safety.

- Risk management framework for AI:
  - Based on the notion/dimensions of "trustworthiness".
  - What makes *special* an AI-RMF?
  - How to *measure* risk in an AI system (quantitative/qualitative)?

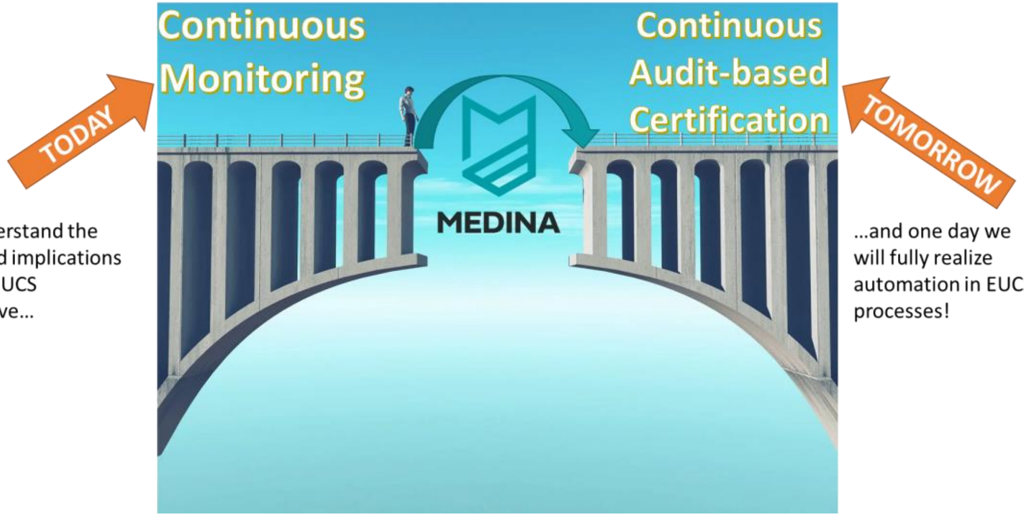
- Conformance assessments:
  - Also depend on the notion of trustworthiness ☺
  - 3rd party certification vs Self-issued Assessment of Conformity.
  - Which requirements to assess?
  - Holistic perspective (e.g., including cloud platform, edge).
  - *Continuous (automated)* vs Point-in-time assessments.
  - Standard-based (although no standards are available).

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

Work in Progress

Paving the road to AI trustworthiness

- Strong collaborations with ENISA and US NIST on topics related to AI cybersecurity, RMF, and certification.
- Active participation in relevant standardization activities (e.g., ISO/IEC, and German BSI).
- H2020 MEDINA on continuous cybersecurity certification.
- Active scouting in upcoming EU calls (e.g., DIGITAL).
- Major efforts to further develop Bosch’s AIShield.
- Certification-by-design ☺



Let’s understand the real-world implications from an EUCS perspective…

…and one day we will fully realize automation in EUCS processes!

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

Thanks!

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

MEDINA

From Continuous Monitoring to Continuous Cloud Cybersecurity Certification

Dr. Jesus Luna Garcia

Robert Bosch GmbH, Germany

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

Agenda

MEDINA

- Background
- H2020 MEDINA Overview
- Initial Results
- Summary

Background

EU Cybersecurity Act (EUCSA)

EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

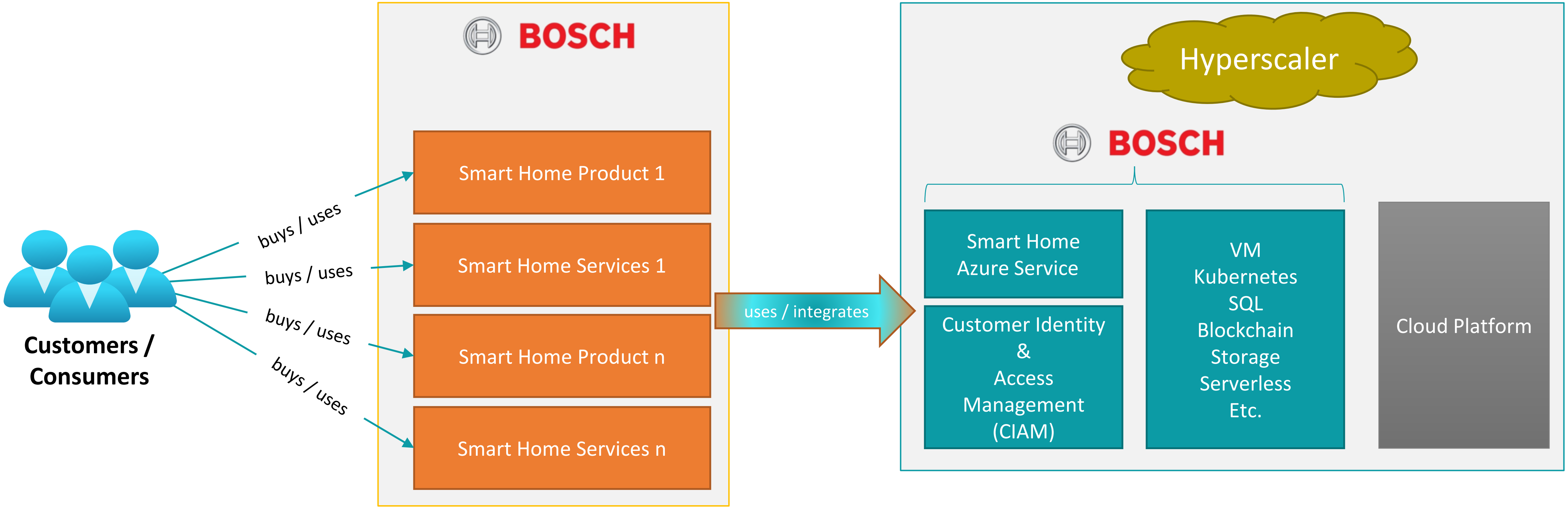
EU Cybersecurity Act

MEDINA

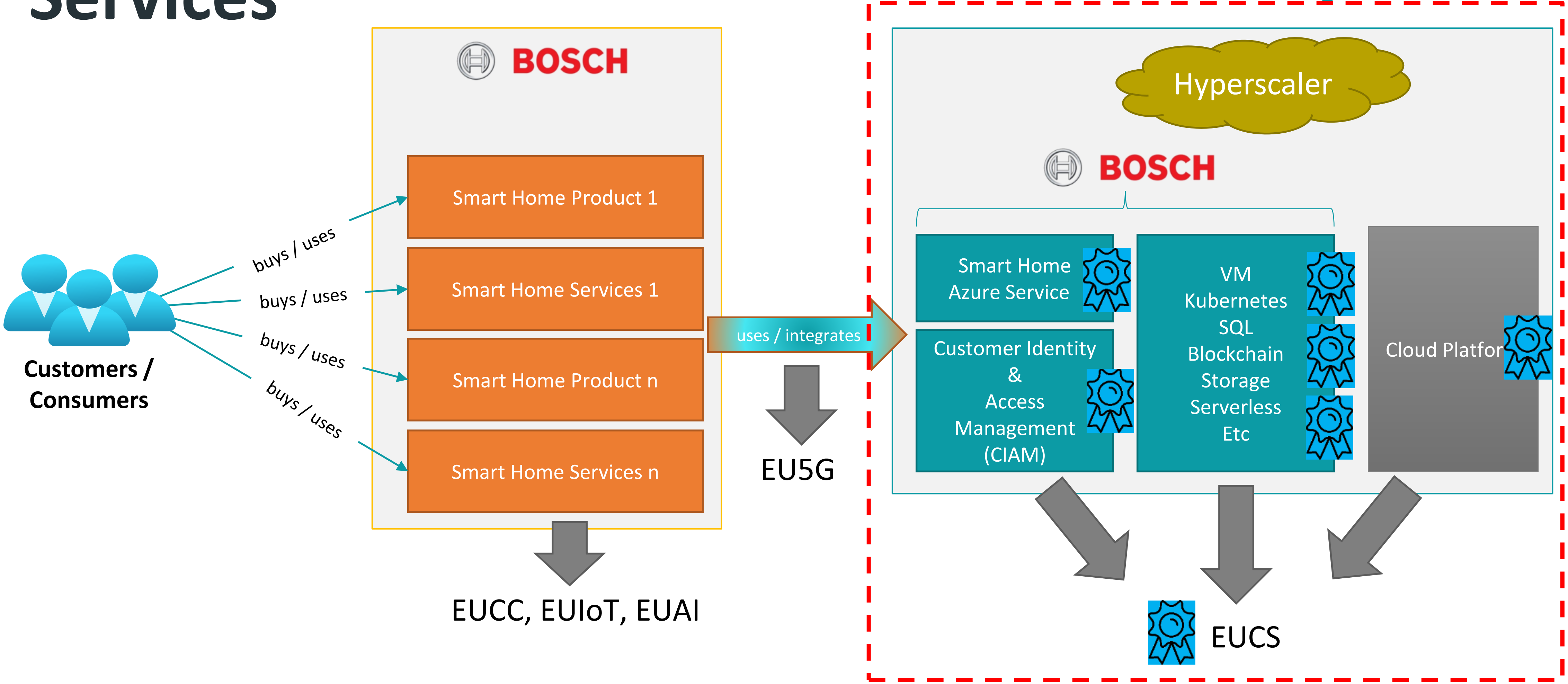
- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation EU-wide cybersecurity certification schemes in order to:
  - provide an EU-wide cybersecurity baseline (requirements, audit methods)
  - enable customers to make risk-based decisions about cybersecurity
  - ***enable continuous cybersecurity compliance***
- Two EUCSA-derived certification schemes are under preparation:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - ***EUCS - Cybersecurity Certification Scheme for Cloud Services***

enisa
THE EU
CYBERSECURITY
AGENCY

EUCS at a glance – Scope on Cloud Services



EUCS at a glance – Scope on Cloud Services



EUCS at a glance – Levels of Assurance

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment driven
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** risks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

‘high’ level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

EUCS at a glance – Continuous Monitoring

- Definition of “Continuous (Automated) Monitoring” in the EUCS **(draft Dec-2020)**:

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

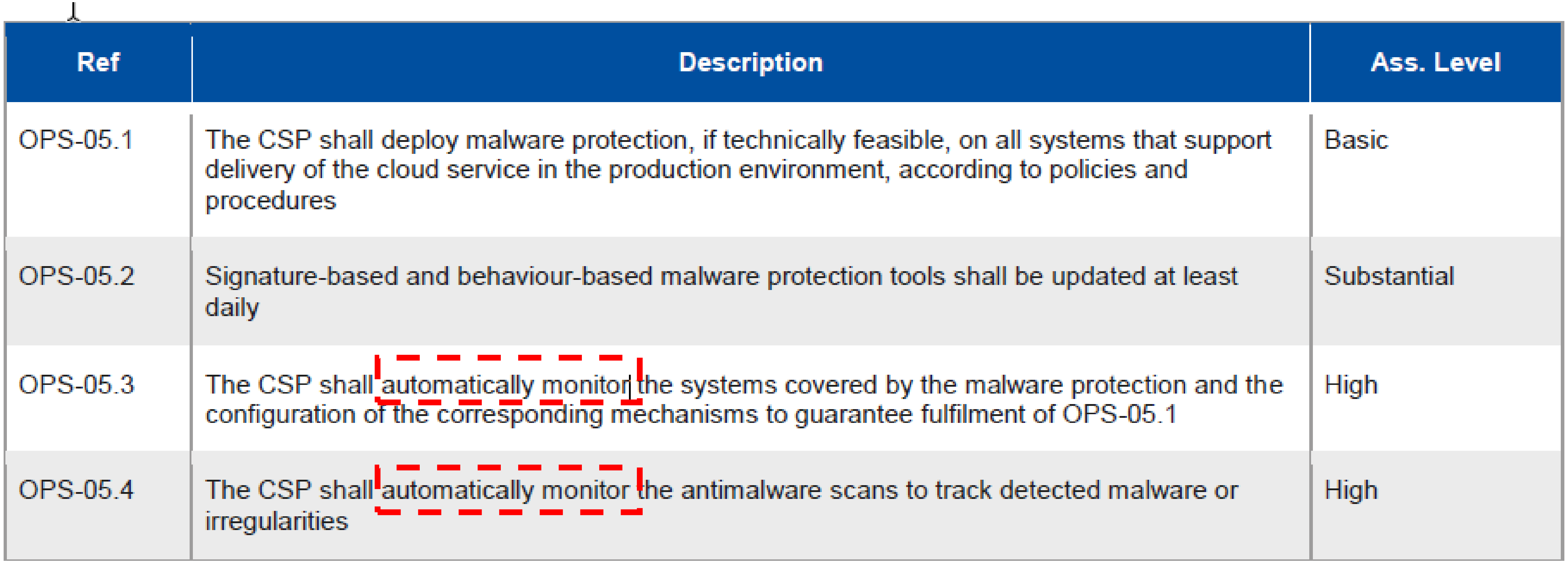
  1. *Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;*
  2. *Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;*
  3. *Report deviations to subject matter experts who 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.*

Only for HIGH Assurance!

EUCS at a glance – Continuous Monitoring

- Example (EUCS draft Dec-2020):



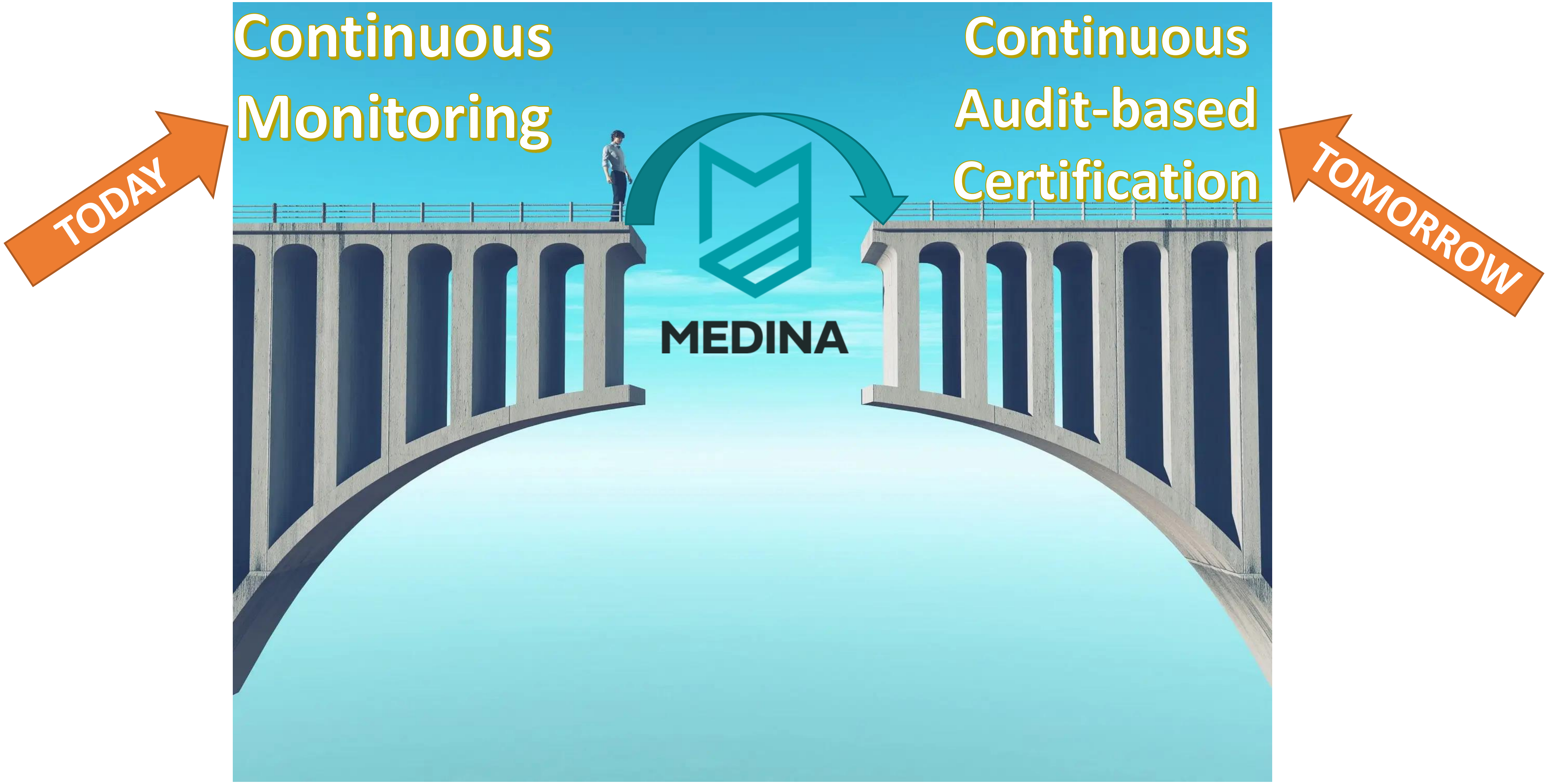
Ref	Description	Ass. Level
OPS-05.1	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures	Basic
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial
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	High
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	High

MEDINA

MEDINA – an Overview

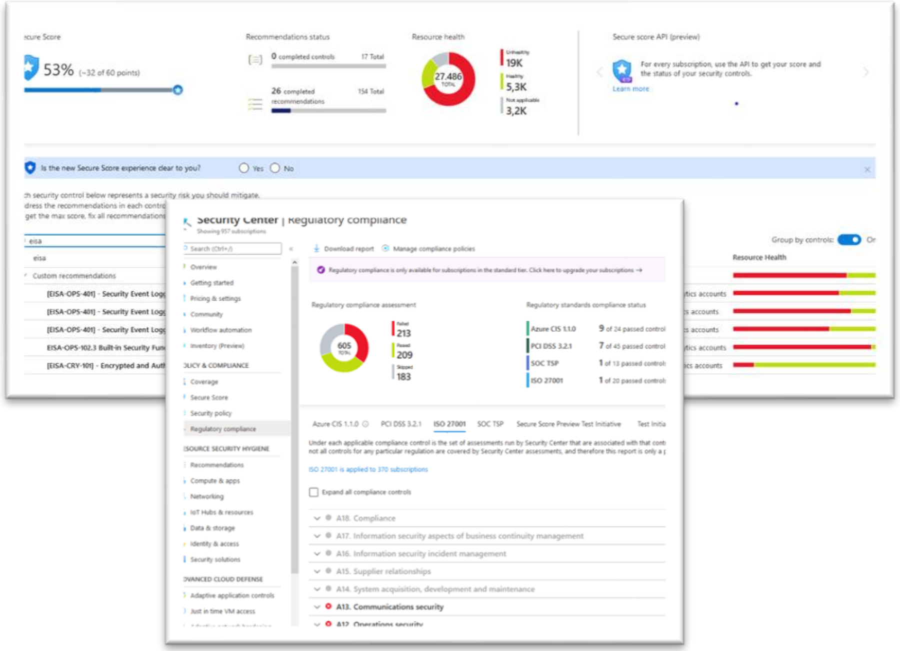
Paving the road towards EUCS

Bridging the Gap



From Continuous Monitoring to Continuous Certification

TODAY


ecure Score
53% (~32 of 60 points)
Recommendations status
0 completed controls 17 Total
26 completed recommendations 154 Total
Resource health
27.486 TOTAL
Unhealthy 19K
Healthy 5,3K
Not applicable 3,2K
Secure score API (preview)
Learn more
○ Yes ○ No
eisa
eisa
Custom recommendations
[EISA-OPS-401] - Security Event Log
[EISA-OPS-401] - Security Event Log
[EISA-OPS-401] - Security Event Log
EISA-OPS-102.3 Built-in Security Fun
[EISA-CRY-101] - Encrypted and Auth
Group by controls: On
Resource Health
tics accounts
s accounts
s accounts
tics accounts
cs accounts
Security Center | Regulatory compliance
Showing 957 subscriptions
Search (Ctrl+/)
Overview
Getting started
Pricing & settings
Community
Workflow automation
Inventory (Preview)
OLICY & COMPLIANCE
Coverage
Secure Score
Security policy
Regulatory compliance
ESOURCE SECURITY HYGIENE
Recommendations
Compute & apps
Networking
IoT Hubs & resources
Data & storage
Identity & access
Security solutions
DVANCED CLOUD DEFENSE
Adaptive application controls
Just in time VM access
Download report
Manage compliance policies
Regulatory compliance assessment
605 TOTAL
Failed 213
Passed 209
Skipped 183
Regulatory standards compliance status
Azure CIS 1.1.0 9 of 24 passed control
PCI DSS 3.2.1 7 of 45 passed control
SOC TSP 1 of 13 passed control
ISO 27001 1 of 20 passed control
Azure CIS 1.1.0
PCI DSS 3.2.1
ISO 27001
SOC TSP
Secure Score Preview Test Initiative
Test Initia
ISO 27001 is applied to 370 subscriptions
□ Expand all compliance controls
A18. Compliance
A17. Information security aspects of business continuity management
A16. Information security incident management
A15. Supplier relationships
A14. System acquisition, development and maintenance
A13. Communications security
A12. Operations security

For every subscription, use the API to get your score and the status of your security controls.

Is the new Secure Score experience clear to you?

ch security control below represents a security risk you should mitigate.
dress the recommendations in each contro
get the max score, fix all recommendations

Regulatory compliance is only available for subscriptions in the standard tier. Click here to upgrade your subscriptions →

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that cont
not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a p

DevOps

IT Security Governance

Internal Auditors

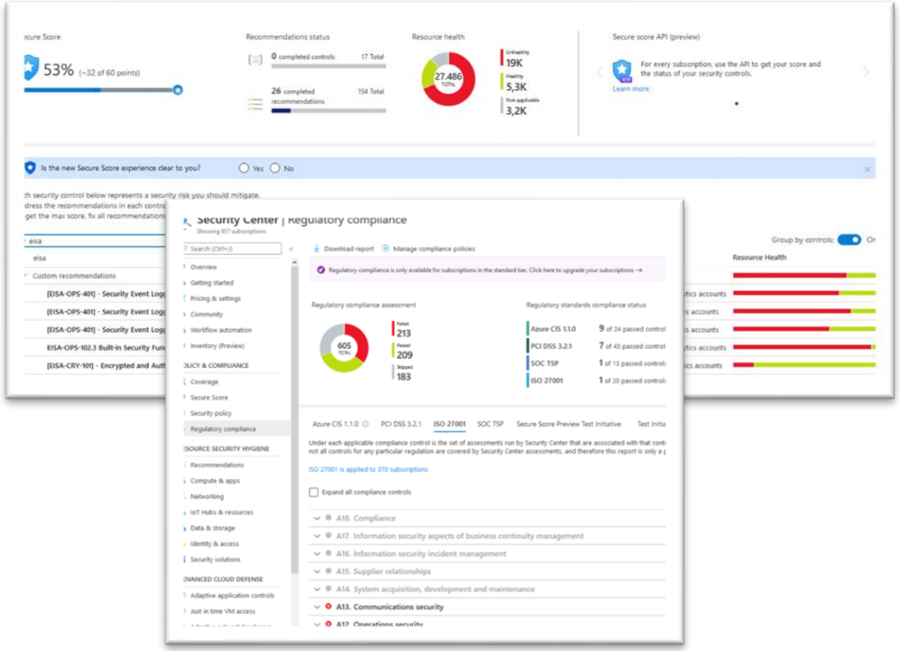
- Cloud Security Posture Management (CSPM) tools provide our internal stakeholders with “continuous” compliance data.
- Bosch-internal deployment (since mid-2019), monitors > 50,000 cloud resources for compliance with our internal ISO/IEC 27001-based security control framework.
- > 150 security KPIs being monitored.

From Continuous Monitoring to Continuous Certification

MEDINA

TODAY

TOMORROW



ecure Score

53% (~32 of 60 points)

Recommendations status

0 completed controls 17 Total

26 completed recommendations 154 Total

Resource health

27,486 TOTAL

Unhealthy 19K

Healthy 5,3K

Not applicable 3,2K

Secure score API (preview)

For every subscription, use the API to get your score and the status of your security controls.

Learn more

Is the new Secure Score experience clear to you? ○ Yes ○ No

ch security control below represents a security risk you should mitigate.
ddress the recommendations in each contro
get the max score, fix all recommendations

eisa

eisa

Custom recommendations

[EISA-OPS-401] - Security Event Logg

[EISA-OPS-401] - Security Event Logg

[EISA-OPS-401] - Security Event Logg

EISA-OPS-102.3 Built-in Security Fun

[EISA-CRY-101] - Encrypted and Auth

Group by controls: On

Resource Health

tics accounts

s accounts

s accounts

tics accounts

ics accounts

Security Center | Regulatory compliance

Showing 957 subscriptions

Search (Ctrl+/)

Download report | Manage compliance policies

Overview

Getting started

Pricing & settings

Community

Workflow automation

Inventory (Preview)

OLICY & COMPLIANCE

Coverage

Secure Score

Security policy

Regulatory compliance

ESOURCE SECURITY HYGIENE

Recommendations

Compute & apps

Networking

IoT Hubs & resources

Data & storage

Identity & access

Security solutions

DVANCED CLOUD DEFENSE

Adaptive application controls

Just in time VM access

Regulatory compliance is only available for subscriptions in the standard tier. Click here to upgrade your subscriptions →

Regulatory compliance assessment

605 TOTAL

Failed 213

Passed 209

Skipped 183

Regulatory standards compliance status

Azure CIS 1.1.0	9 of 24 passed control
PCI DSS 3.2.1	7 of 45 passed control
SOC TSP	1 of 13 passed control
ISO 27001	1 of 20 passed control

Azure CIS 1.1.0 | PCI DSS 3.2.1 | ISO 27001 | SOC TSP | Secure Score Preview Test Initiative | Test Initia

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that cont
not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a p

ISO 27001 is applied to 370 subscriptions

□ Expand all compliance controls

A18. Compliance

A17. Information security aspects of business continuity management

A16. Information security incident management

A15. Supplier relationships

A14. System acquisition, development and maintenance

A13. Communications security

A12. Operations security

BOSCH

External Auditor

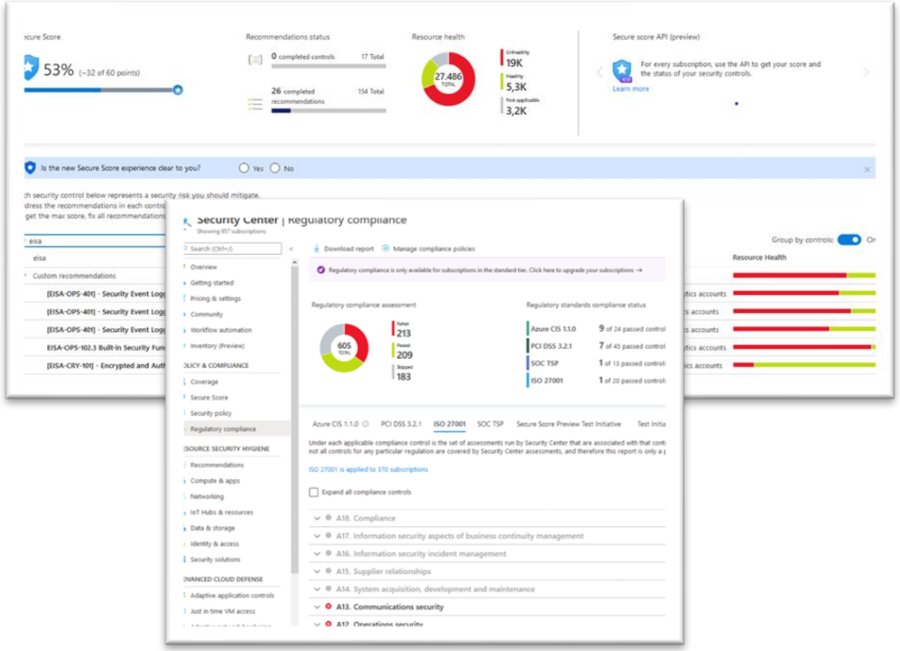
NIXU cybersecurity.

From Continuous Monitoring to Continuous Certification

MEDINA

TODAY

TOMORROW



For every subscription, use the API to get your score and the status of your security controls.

Is the new Secure Score experience clear to you? ○ Yes ○ No

...ch security control below represents a security risk you should mitigate.
...dress the recommendations in each contro...
...get the max score, fix all recommendations...

Regulatory compliance is only available for subscriptions in the standard tier. Click here to upgrade your subscriptions →

Azure CIS 1.1.0	9 of 24 passed control
PCI DSS 3.2.1	7 of 45 passed control
SOC TSP	1 of 13 passed controls
ISO 27001	1 of 20 passed controls

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that cont... not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a ...

ISO 27001 is applied to 370 subscriptions

□ Expand all compliance controls

- A18. Compliance
- A17. Information security aspects of business continuity management
- A16. Information security incident management
- A15. Supplier relationships
- A14. System acquisition, development and maintenance
- A13. Communications security
- A12. Operations security

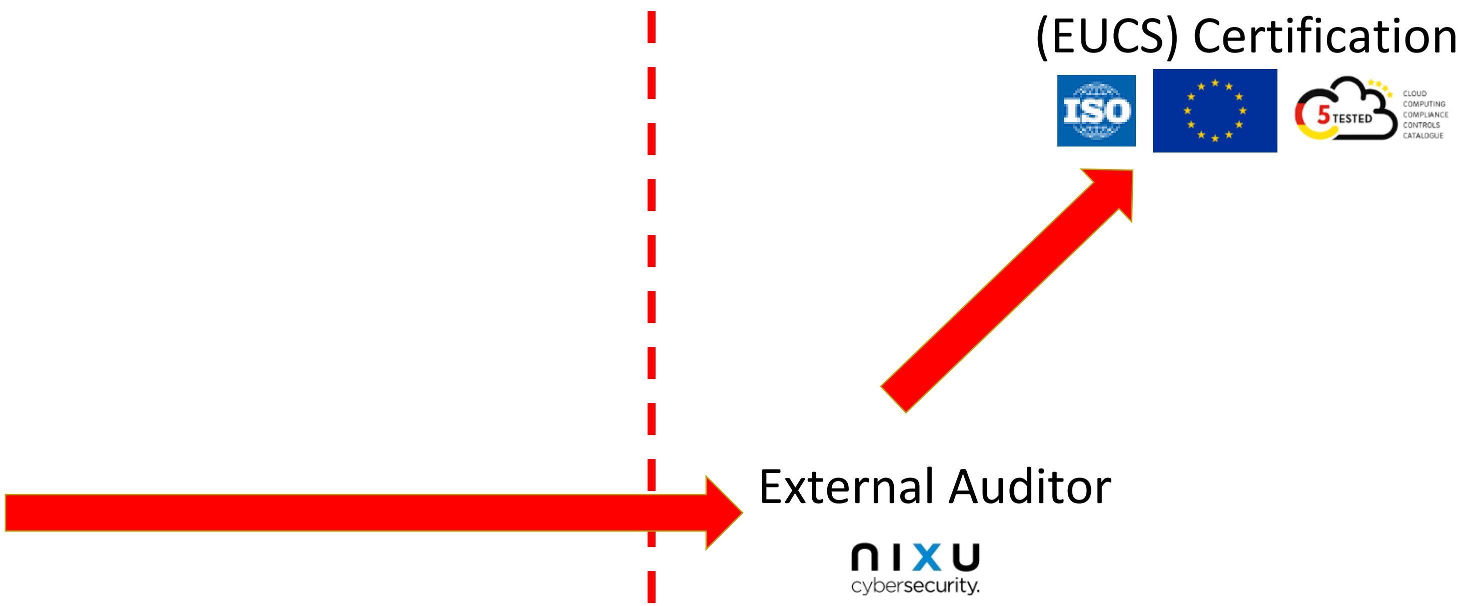
BOSCH

MEDINA

funded by

European Commission

Horizon 2020
European Union funding
for Research & Innovation



(EUCS) Certification

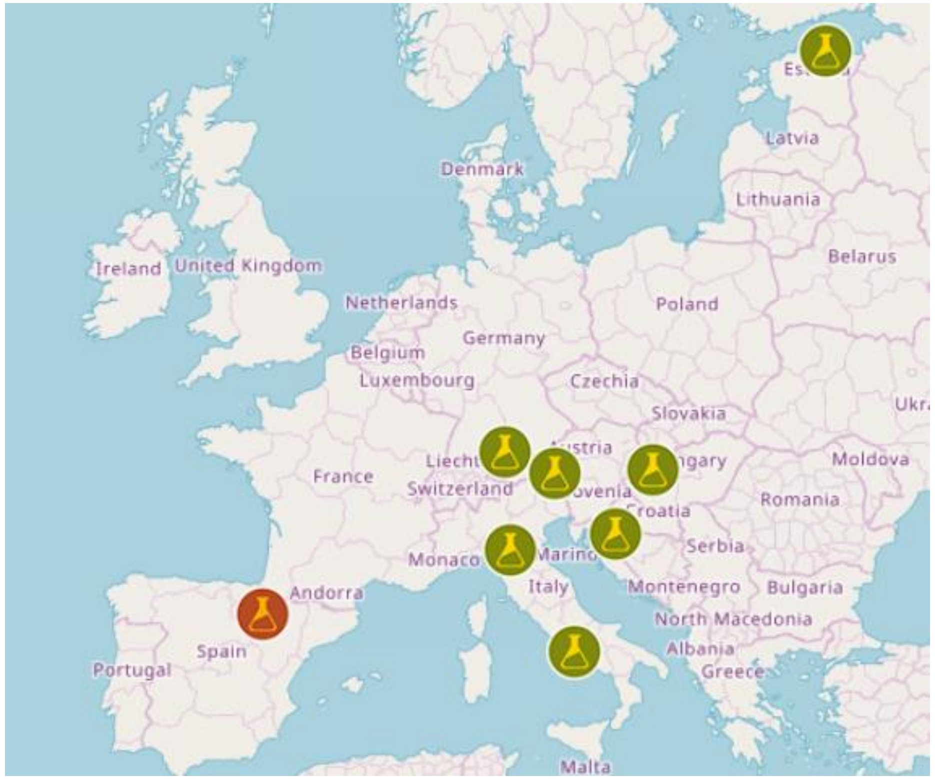
External Auditor

nixu cybersecurity.

MEDINA At a Glance

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€



tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft®

Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Challenges and Approaches

MEDINA

Existing Certifications	EUCS and MEDINA
Point in time certifications (e.g., once per-year)	Continuous certification based on automated monitoring
High costs and effort for certifying cloud services	AI-driven automation to support audit processes (incl. evidence management)
Lack of transparency in cloud security	Dynamic reporting provides different levels of details and transparency
High customization effort in commercial CSPM tools	Automated generation of compliance assessments based on natural language requirements

MEDINA

Initial Experiences with EUCS-Continuous

ENISA Experimentation Q1-Q3/2021

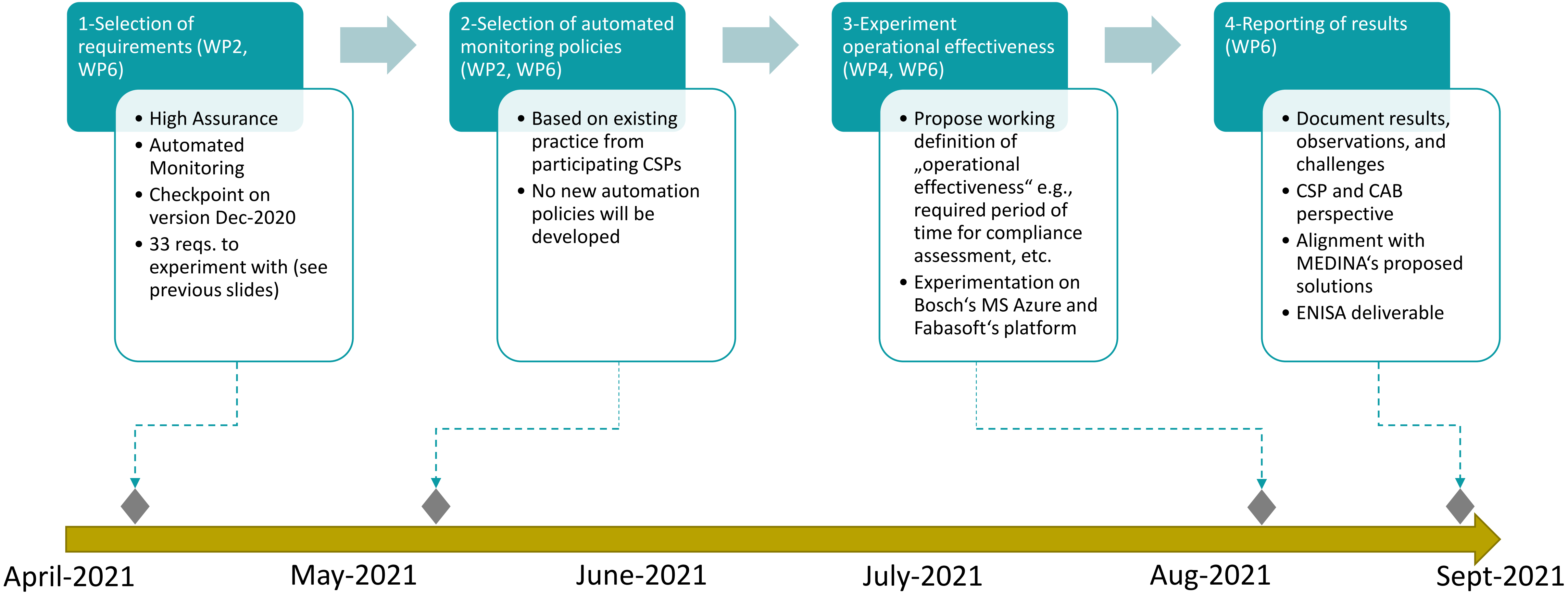
10/20/2023

Experimenting with EUCS

MEDINA

- In March 2021, ENISA released a "call for experimentation" related to different aspects of the candidate EUCS.
  - Main objective of these experiments was to empirically (pre-)validate some of the core requirements in EUCS
- In that context, the MEDINA consortium participated with the experimentation of *automated monitoring requirements extracted from the EUCS High Assurance baseline*.
  - Experiments ran by other teams focused on challenging topics e.g., composability of certificates.

Overall PoC Approach and Timeline



1-Selection of requirements (WP2, WP6)

- High Assurance
- Automated Monitoring
- Checkpoint on version Dec-2020
- 33 reqs. to experiment with (see previous slides)

2-Selection of automated monitoring policies (WP2, WP6)

- Based on existing practice from participating CSPs
- No new automation policies will be developed

3-Experiment operational effectiveness (WP4, WP6)

- Propose working definition of „operational effectiveness“ e.g., required period of time for compliance assessment, etc.
- Experimentation on Bosch‘s MS Azure and Fabasoft‘s platform

4-Reporting of results (WP6)

- Document results, observations, and challenges
- CSP and CAB perspective
- Alignment with MEDINA‘s proposed solutions
- ENISA deliverable

Obtained Results

- (Draft) Catalogue of metrics for EUCS requirements:
  - Facilitates automation of the EUCS requirement / removes subjectivity of EUCS requirement interpretation.
  - Structures basic information like ReqID, Metric Name, Metric Description, Scale.
  - Current draft provides 120+ metrics which cover all assessed 30+ relevant EUCS High requirements.
  - At the state of practice, we noticed an evident lack of standardized metric catalogues.

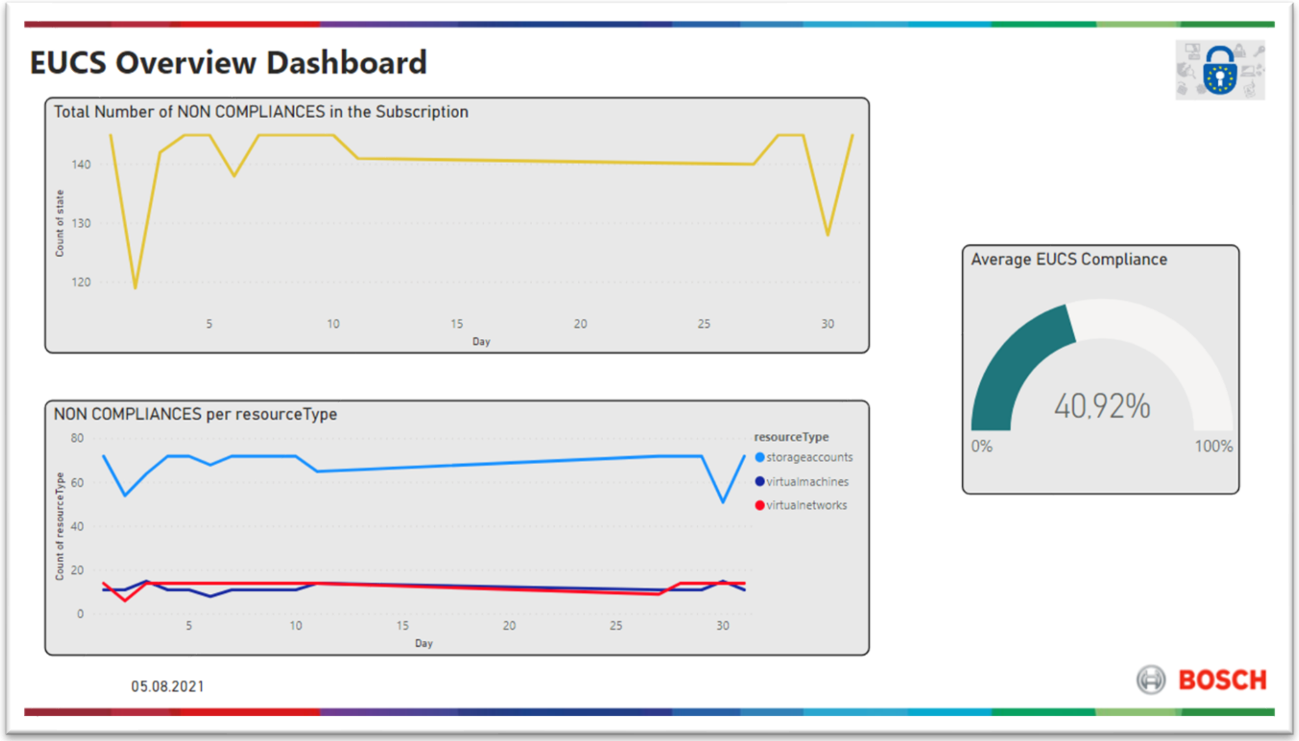
Obtained Results

- PoC for automated assessment policies:
  - Implemented in a well-known hyperscaler, with a deployed testbed from Bosch (VMs, storage, Web Server).
  - Leveraged out-of-the-box CSPM technology (Cloud Security Posture Management).
  - PoC covered less than 50% of relevant EUCS High Requirements, mostly due to time/resources restrictions.
  - Current toolset is technologically limited (not all cloud services support all relevant metrics, even in the same hyperscaler).

Obtained Results

- EUCS Dashboard (PoC):
  - Provides a better understanding of what “operational effectiveness” means for continuous in EUCS High.
  - Data from assessment policies was collected for a period of 30 days.
  - PoC limited to few resources/EUCS Requirements.
  - Homebrew development was required due to limitations in selected cloud-native solutions.

Obtained Results



EUCS Overview Dashboard

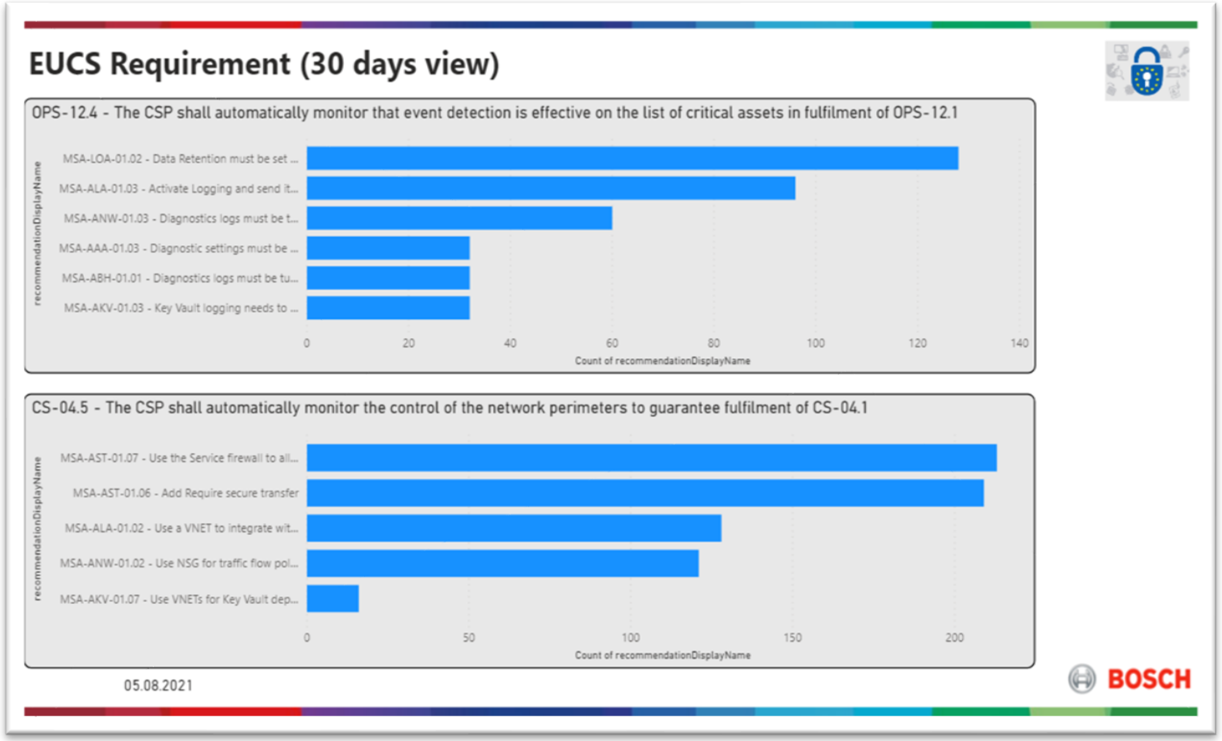
Total Number of NON COMPLIANCES in the Subscription

NON COMPLIANCES per resourceType

Average EUCS Compliance

05.08.2021

BOSCH



EUCS Requirement (30 days view)

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

recommendationDisplayName
MSA-LOA-01.02 - Data Retention must be set ...
MSA-ALA-01.03 - Activate Logging and send it...
MSA-ANW-01.03 - Diagnostics logs must be t...
MSA-AAA-01.03 - Diagnostic settings must be ...
MSA-ABH-01.01 - Diagnostics logs must be tu...
MSA-AKV-01.03 - Key Vault logging needs to ...
0
20
40
60
80
100
120
140
Count of recommendationDisplayName

CS-04.5 - The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1

recommendationDisplayName
MSA-AST-01.07 - Use the Service firewall to all...
MSA-AST-01.06 - Add Require secure transfer
MSA-ALA-01.02 - Use a VNET to integrate wit...
MSA-ANW-01.02 - Use NSG for traffic flow pol...
MSA-AKV-01.07 - Use VNETs for Key Vault dep...
0
50
100
150
200
Count of recommendationDisplayName

05.08.2021

BOSCH

Obtained Results

- Machine-readable format for EUCS:
  - Such format strongly benefits automation of requirements for EUCS High monitoring.
  - NIST OSCAL as a promising candidate in this area.
  - OSCAL natively offers support for requirements catalogues (e.g., NIST SP800-53), but also for assessments specification/reporting.
  - Performed PoC provides a sample representation of EUCS in OSCAL format, which was closely developed along with NIST’s.

The Auditor’s Perspective - Experimentation

- The PoC shows different levels of automation can be achieved in the implementation of experimented requirements
  - Auditor’s involvement is still required in most of the cases to ensure that the continuous monitoring provides trustworthy evidence
- The EUCS approach creates the foundations for shifting from point-in-time audits towards continuous audit services in the future
- Standardization of audit processes and good practices is still needed to leverage the full potential of automation
- About the auditor’s toolset:
  - Egg-chicken problem – who certifies the tools for certification?

Summary

What comes next?

The way forward

MEDINA

1. Provide a clear **implementation guidance** about EUCS requirements where some degree of automated monitoring is needed.
2. Provide clear **audit/assessment guidance** related to EUCS requirements needing some degree of automated monitoring.
3. Consider integrating a **catalogue of metrics** as part of the implementation guidance for EUCS.
4. Consider **focusing the EUCS requirements** needing some sort of automated monitoring only on capabilities offered by cloud platforms, and not by external systems.
5. **Guidance on selecting tools/technologies** for automated (continuous) monitoring.
6. Actively monitor the development of **NIST OSCAL**.

Summary

- MEDINA aims to facilitate adoption of EUCS, specifically for automated monitoring, while paving the road for continuous certification.
- Is EUCS' automation the silver bullet in cloud security certification?
- Can MEDINA be a game changer in the audit/certification practice?

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

MEDINA

Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com

Cyber insurance

Artsiom Yautsiukhin

Consiglio Nazionale delle Ricerche

Cyber Sure

MEDINA

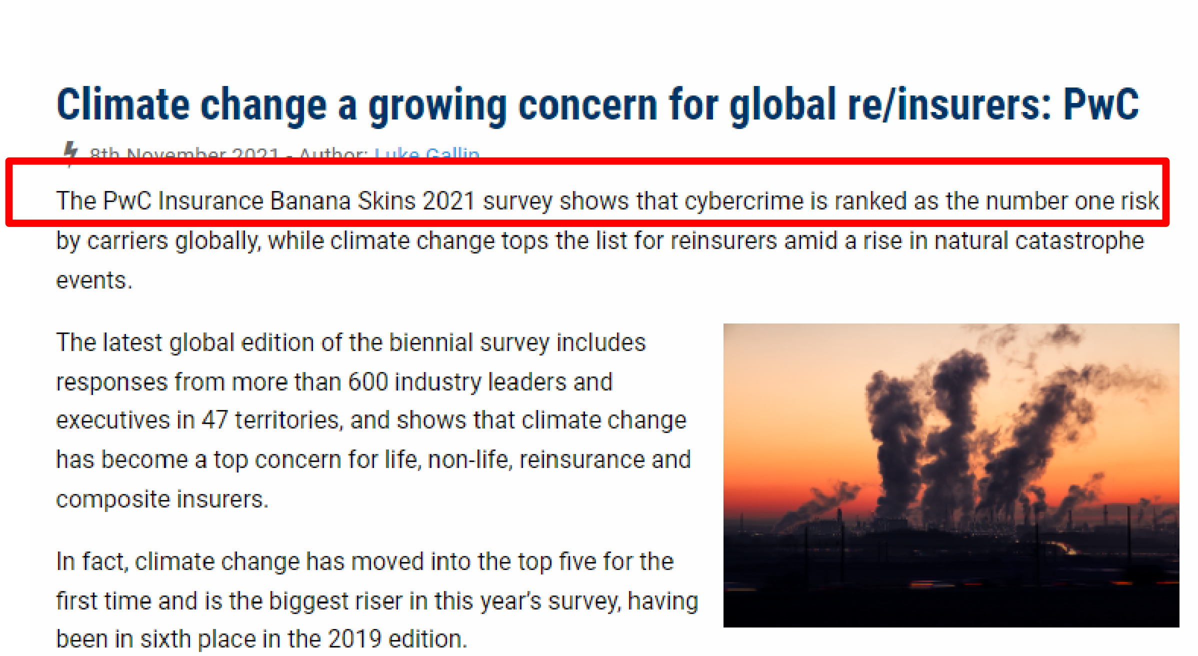
SPARTA

Outline

- Overview
  - Cyber security economics
  - Cyber insurance. Introduction
  - Cyber insurance. Peculiarities
- Formalisation
  - Formal models for cyber insurance.
  - Formal Analysis of cyber insurance models
- Projects
  - Some practical steps towards risk assessment and cyber insurance
- Conclusions

CYBER SECURITY ECONOMICS

Cyber security risk is on top



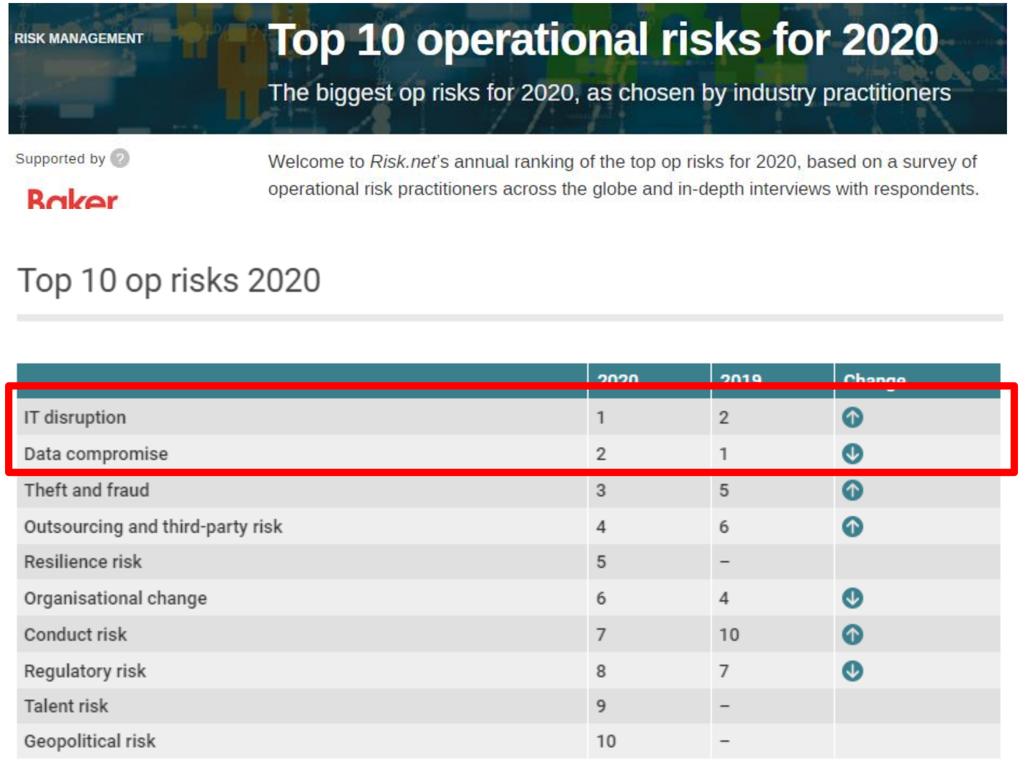
Climate change a growing concern for global re/insurers: PwC

8th November 2021 - Author: Luke Gallin

The PwC Insurance Banana Skins 2021 survey shows that cybercrime is ranked as the number one risk by carriers globally, while climate change tops the list for reinsurers amid a rise in natural catastrophe events.

The latest global edition of the biennial survey includes responses from more than 600 industry leaders and executives in 47 territories, and shows that climate change has become a top concern for life, non-life, reinsurance and composite insurers.

In fact, climate change has moved into the top five for the first time and is the biggest riser in this year's survey, having been in sixth place in the 2019 edition.



RISK MANAGEMENT

Top 10 operational risks for 2020

The biggest op risks for 2020, as chosen by industry practitioners

Supported by ?

Baker

Welcome to *Risk.net*'s annual ranking of the top op risks for 2020, based on a survey of operational risk practitioners across the globe and in-depth interviews with respondents.

Top 10 op risks 2020

	2020	2019	Change
IT disruption	1	2	↑
Data compromise	2	1	↓
Theft and fraud	3	5	↑
Outsourcing and third-party risk	4	6	↑
Resilience risk	5	–	
Organisational change	6	4	↓
Conduct risk	7	10	↑
Regulatory risk	8	7	↓
Talent risk	9	–	
Geopolitical risk	10	–	

Cyber security economics

- Why do we implement cyber security?
  - Because of high potential losses due to cyber attacks:
    - Colonial Pipeline Co. paid the hackers a $4.4 million ransom shortly after the hack (+100 Gb stolen data, rise in fuel prices, fuel shortage in several states, caused panic)
    - In 2021 REvil APT demanded 50 mln (ACER), (11 mln) JBS Food, (50 mln) Quanta/Apple, (70 mln) Kaseya
- Why do not we implement the best available security?
  - Because cyber security solutions are costly! And cyber security budget is limited.
- Then, how much security is enough?
  - We need security metrics and approaches, taking into account monetary aspect!
- Solution:
  - Economical methods to balance potential losses and benefits

Risk to measure security

- How to measure security?
  - Security outcomes are uncertain and negative
  - Metrics are required for high-level decision making
  - Indicators are required for non-technical managers (e.g., CIO)

- Most existing security metrics are not suitable
  - Most metrics are solution-specific
  - Cannot help to make a high level decision
  - Examples: time to update, amount of known virus signatures, percentage of trained personnel

- Solution from economics: **risk**

What is risk?

- **Risk** is the **possibility** of suffering harm or **loss** [NIST SP800-30]
  - **Threat** – cause of risk
  - **Vulnerability** – existing flow or weakness
  - **Impact** – possible loss

  - **Asset** – something valuable
  - **Incident** – threat occurrence

How to compute risk?

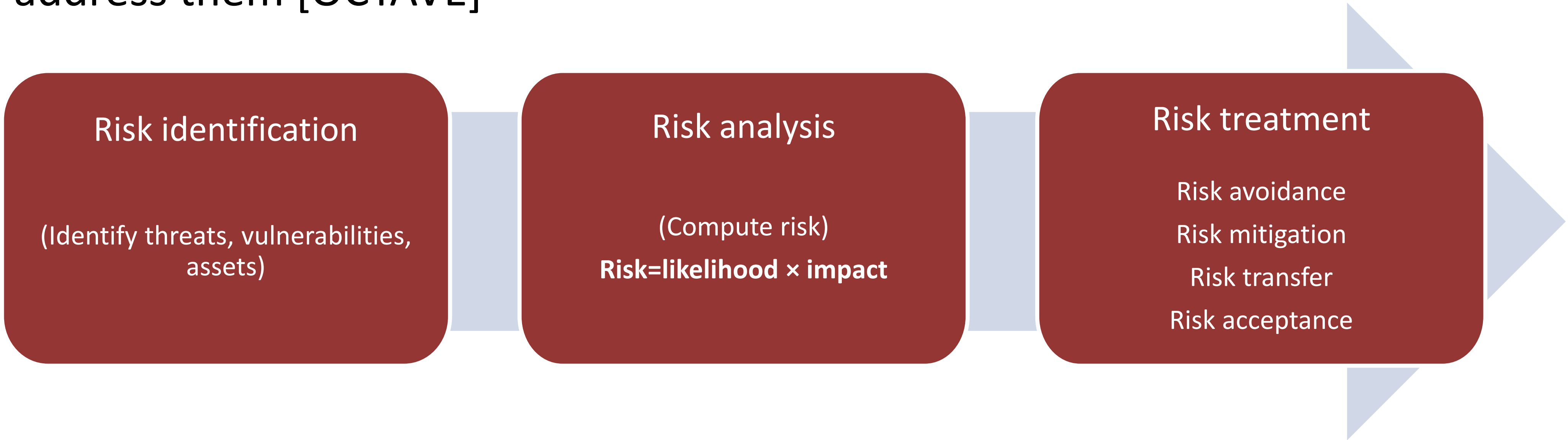
- Threat -> threat exposure
- Vulnerability -> survival probability
- Asset -> Impact

$$Risk = Threat\ Exposure \times Survival\ Probability \times Impact$$

$$Risk = Likelihood \times Impact$$

Risk management/assessment/analysis

- **Risk management** is a process of identifying risks and implementing plans to address them [OCTAVE]



Risk identification

(Identify threats, vulnerabilities, assets)

Risk analysis

(Compute risk)

Risk=likelihood × impact

Risk treatment

Risk avoidance

Risk mitigation

Risk transfer

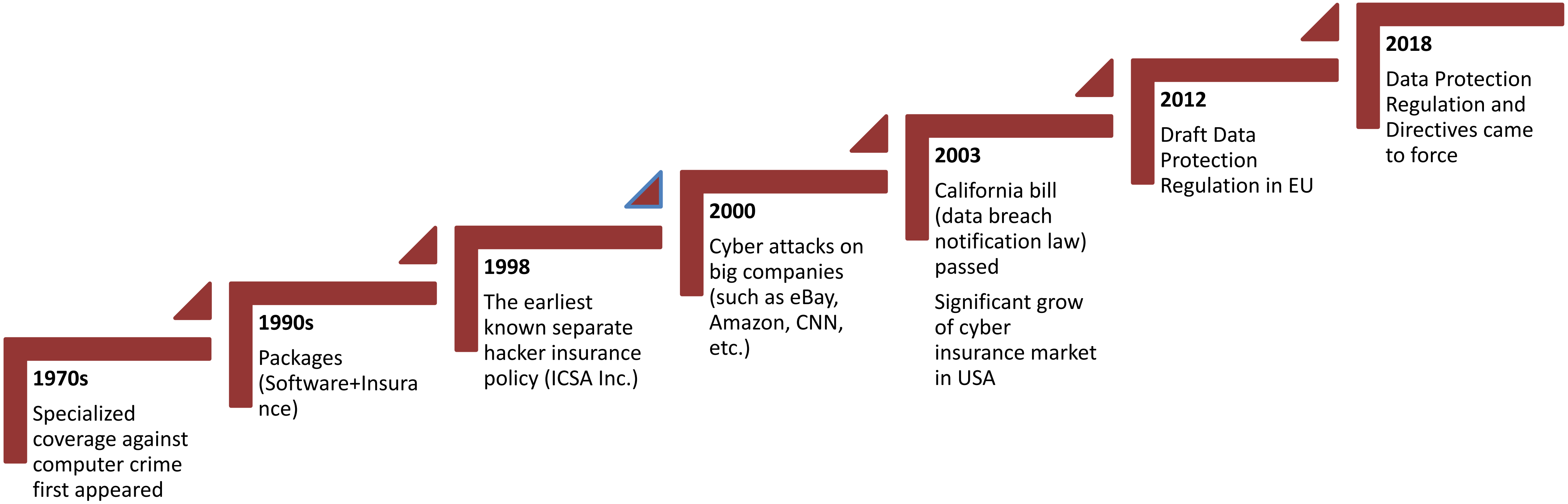
Risk acceptance

- Risk management methodologies: NIST 800-30, OCTAVE, Magerit, Mehari, Microsoft, etc.

Introduction

CYBER INSURANCE

A bit of history



1970s

Specialized coverage against computer crime first appeared

1990s

Packages (Software+Insura nce)

1998

The earliest known separate hacker insurance policy (ICSA Inc.)

2000

Cyber attacks on big companies (such as eBay, Amazon, CNN, etc.)

2003

California bill (data breach notification law) passed

Significant grow of cyber insurance market in USA

2012

Draft Data Protection Regulation in EU

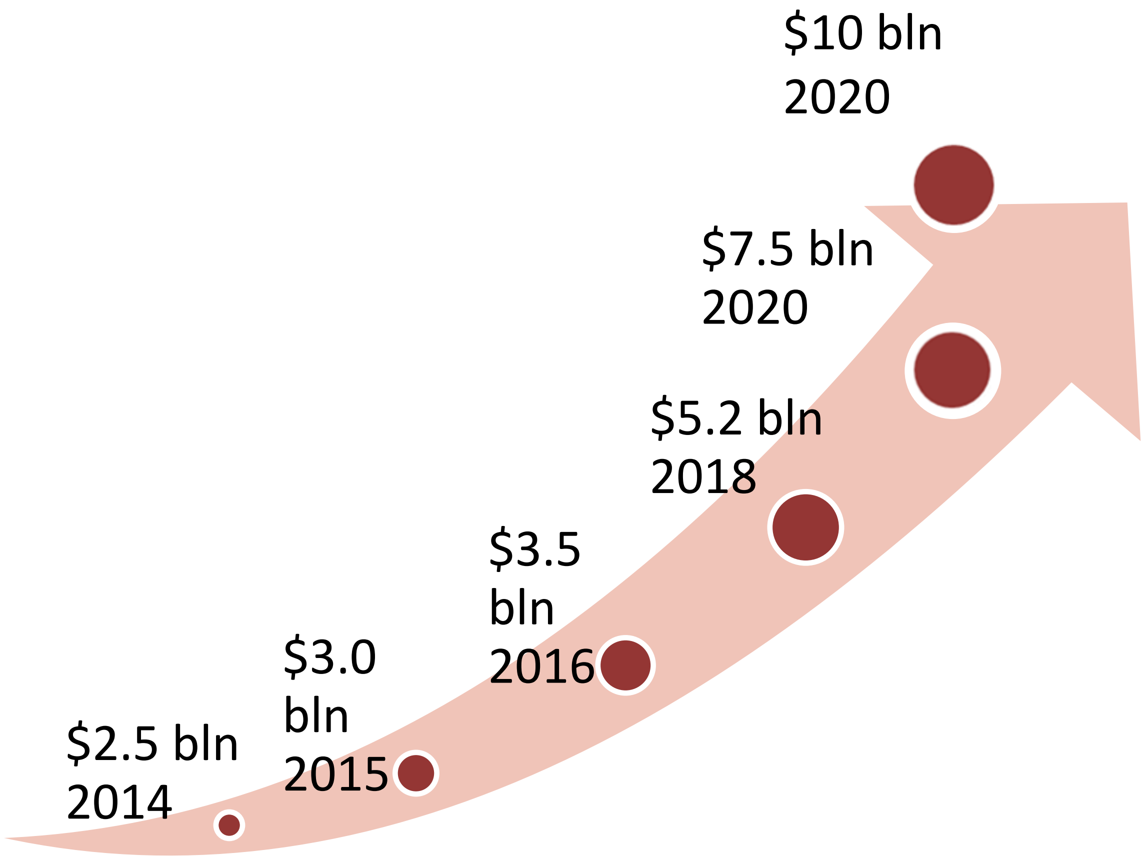
2018

Data Protection Regulation and Directives came to force

Insurance Companies

- Key Market Players
  - Allianz
  - American International Group, Inc.
  - Aon plc
  - AXA
  - Berkshire Hathway Inc.
  - Lloyd’s of London Ltd
  - Lockton Companies, Inc.
  - Munich Re
  - The Chubb Corporation
  - Zurich
  - And 50 more…

Numbers! Give us numbers!



$2.5 bln
2014

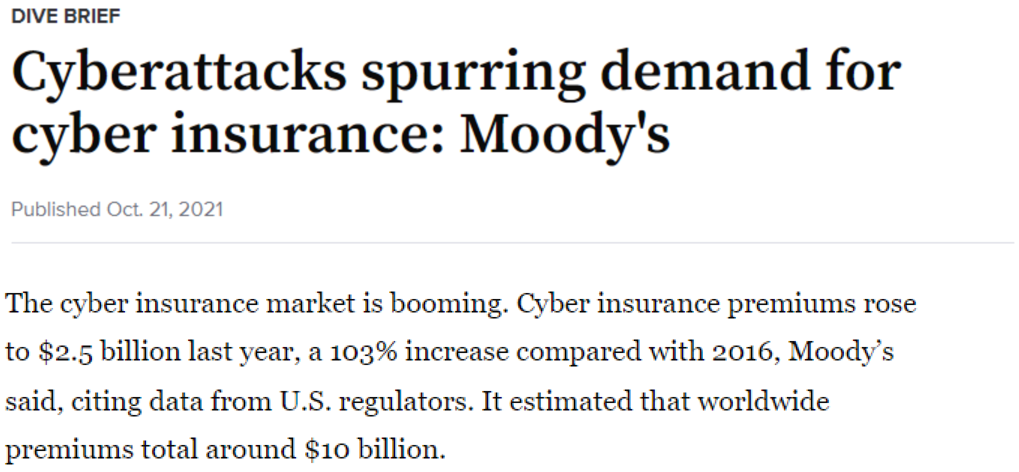
$3.0 bln
2015

$3.5 bln
2016

$5.2 bln
2018

$7.5 bln
2020

$10 bln
2020



DIVE BRIEF

Cyberattacks spurring demand for cyber insurance: Moody's

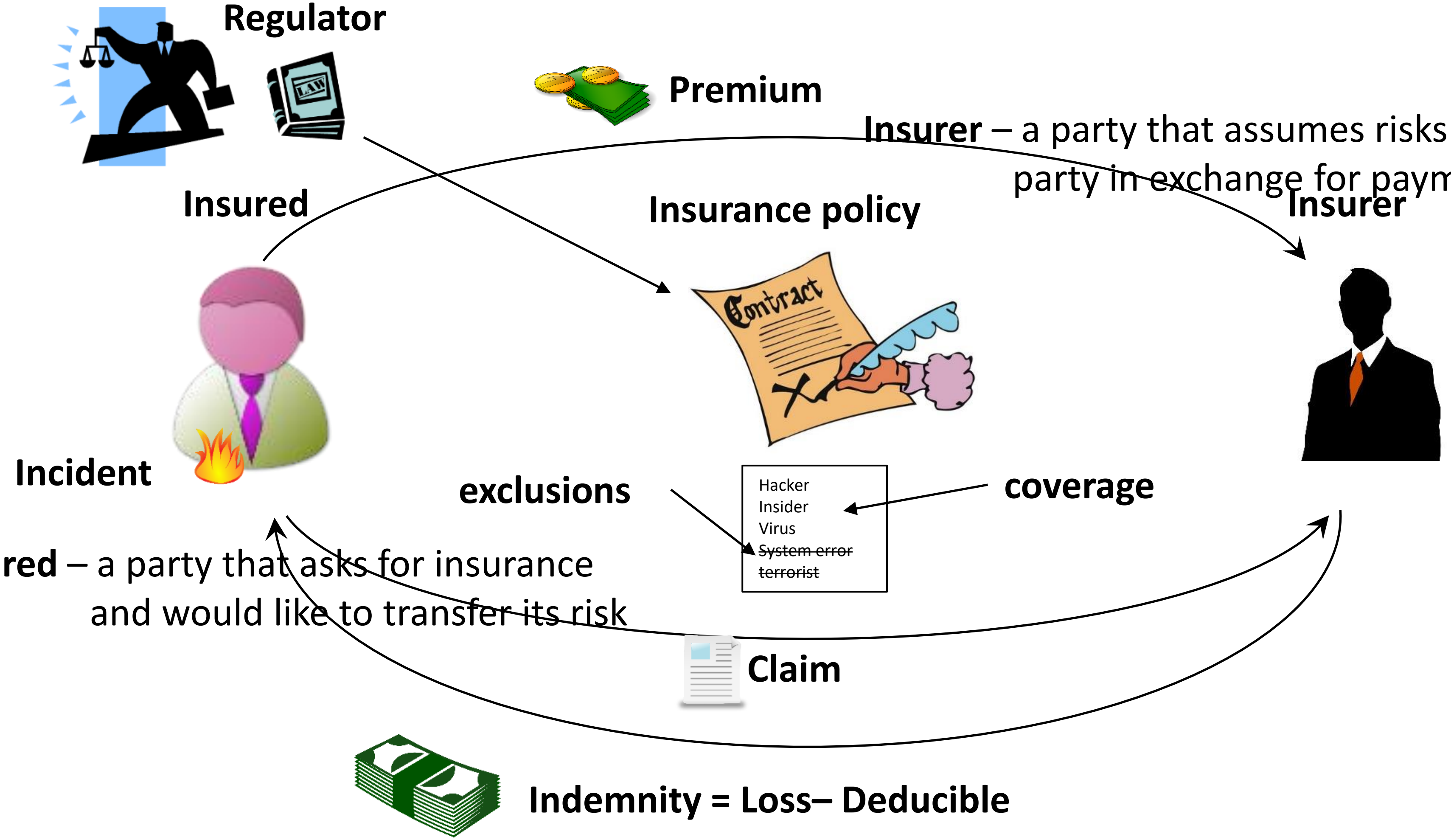
Published Oct. 21, 2021

The cyber insurance market is booming. Cyber insurance premiums rose to $2.5 billion last year, a 103% increase compared with 2016, Moody's said, citing data from U.S. regulators. It estimated that worldwide premiums total around $10 billion.

Why is cyber insurance important?

- Cyber insurance appeared because:
  - Vulnerability increased due to the expansion of information technology
  - Cyber threats cause large business risk
  - Risk mitigation does not eliminate risk completely
  - Risk managers’ approaches need to be integrated
- Expected benefits:
  - Smooth losses
  - Serve as an indicator of quality of protection
  - Incentive to invest in security
  - Rise societal welfare
  - Provoke appearance of advanced security standards

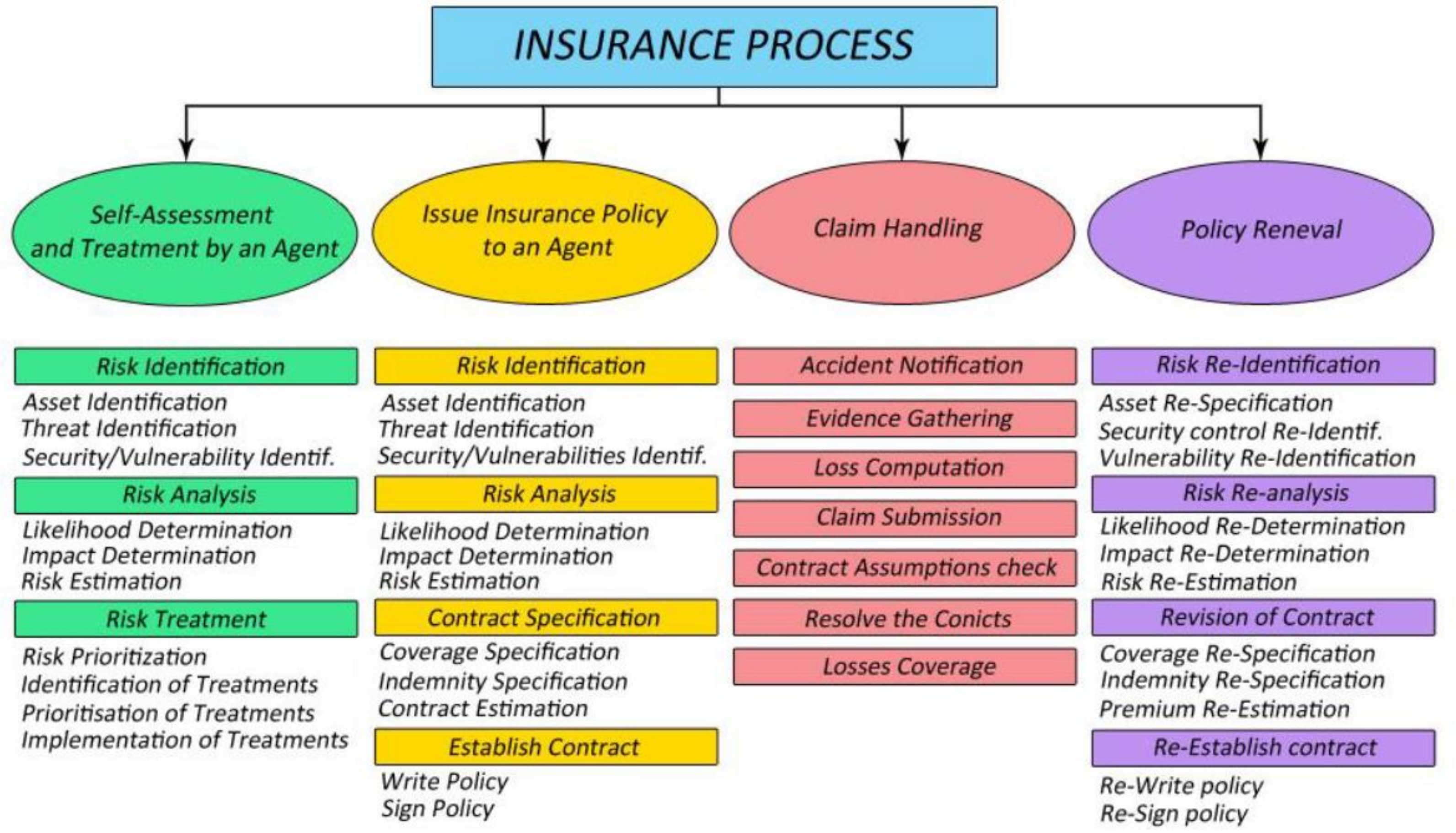
Terms



Insurer – a party that assumes risks of another party in exchange for payment

Insured – a party that asks for insurance and would like to transfer its risk

Insurance process



INSURANCE PROCESS

Self-Assessment and Treatment by an Agent

- Risk Identification
  - Asset Identification
  - Threat Identification
  - Security/Vulnerability Identif.
- Risk Analysis
  - Likelihood Determination
  - Impact Determination
  - Risk Estimation
- Risk Treatment
  - Risk Prioritization
  - Identification of Treatments
  - Prioritisation of Treatments
  - Implementation of Treatments

Issue Insurance Policy to an Agent

- Risk Identification
  - Asset Identification
  - Threat Identification
  - Security/Vulnerabilities Identif.
- Risk Analysis
  - Likelihood Determination
  - Impact Determination
  - Risk Estimation
- Contract Specification
  - Coverage Specification
  - Indemnity Specification
  - Contract Estimation
- Establish Contract
  - Write Policy
  - Sign Policy

Claim Handling

- Accident Notification
- Evidence Gathering
- Loss Computation
- Claim Submission
- Contract Assumptions check
- Resolve the Conicts
- Losses Coverage

Policy Reneval

- Risk Re-Identification
  - Asset Re-Specification
  - Security control Re-Identif.
  - Vulnerability Re-Identification
- Risk Re-analysis
  - Likelihood Re-Determination
  - Impact Re-Determination
  - Risk Re-Estimation
- Revision of Contract
  - Coverage Re-Specification
  - Indemnity Re-Specification
  - Premium Re-Estimation
- Re-Establish contract
  - Re-Write policy
  - Re-Sign policy

Peculiarities

CYBER INSURANCE

Cyber insurance issues I
Lack of experience

- Lack of statistical data
- Evolution of systems
- Hard to specify rate of occurrences
  - Evolution of attacks
  - Effectiveness of controls and standards
- Hard to specify losses
  - Tangible vs. intangible
  - Primary vs. secondary
- Insurers lack of experience and standards

Cyber insurance issues II
Practical issues

- Unclear coverage
- Exclusions and limited coverage
- Low indemnity limits
- Hard to verify predictions
- Contractual language is vague
- Overlapping with existing insurance coverages
- Unclear liability
- Unclear time for claims

Cyber insurance issues III
Risk correlation and information asymmetry

- **Interdependence of security** – security of one agent depends on security of another one
- **Correlation of risks** – one source, many victims (virus outbreak)
  - Lack of re-insurance
  - Geographical similarity
  - Monoculture
  - Attacks are easy to perform and replicate
- **Information asymmetry** – incomplete information possessed by one of the party (usually, Insurer)

Insurability of cyber risks

Mehr and Cammack

- Incidental loss
- Limited risk of huge losses
- Calculable loss
- Large number of similar exposure units
- Affordable premium
- Definite loss
- Large loss

Berliner

- Randomness of loss occurrence
- Maximum possible loss
- Average loss per incident
- Loss exposure
- Information Asymmetry
- Insurance premium
- Cover limits
- Public limits
- Legal restrictions

Formal models

CYBER INSURANCE

And what is about the research?

- Theoretical study of the behaviour of entities/system:
  - – Model the system
    - Model the entities (e.g., insured)
    - Model relations between entities (e.g., security interdependency)
    - Model conditions (e.g., CI market type, regulatory rules)
  - – Analyse the model

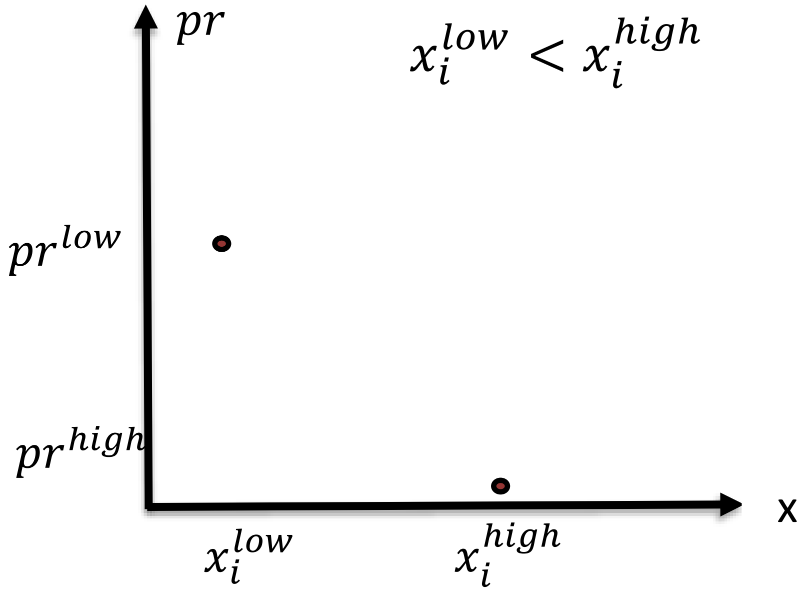
- Many economic/behavioural models are vague (not precise), but we still may analyse some tendencies.

Modelling probability

Discrete:

$$\mathrm{pr}(x_i) = \{\begin{matrix} pr, if\, x_i = x_i^{low} \\ 0, if\, x_i = x_i^{high} \end{matrix}$$

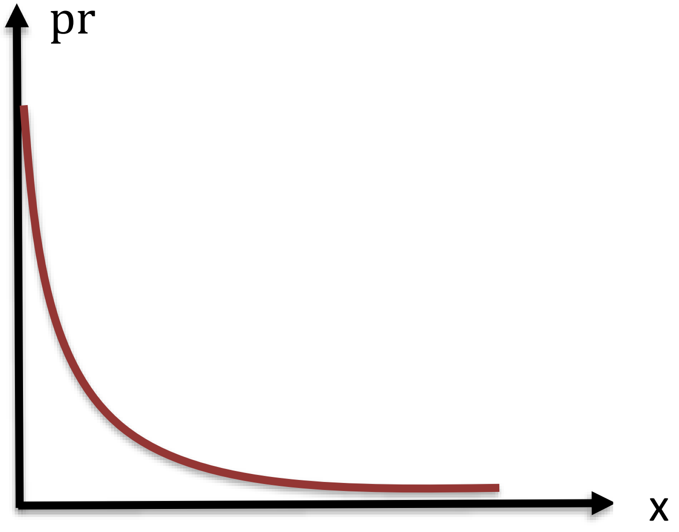
$$x_i^{low} < x_i^{high}$$



Continuous:

$\mathrm{pr}(x_i)$ and *x* - continuous

- $1 > pr(x_i) > 0$ and
- convex
  - $\mathrm{pr}'(x_i) < 0$
  - $\mathrm{pr}''(x_i) > 0$



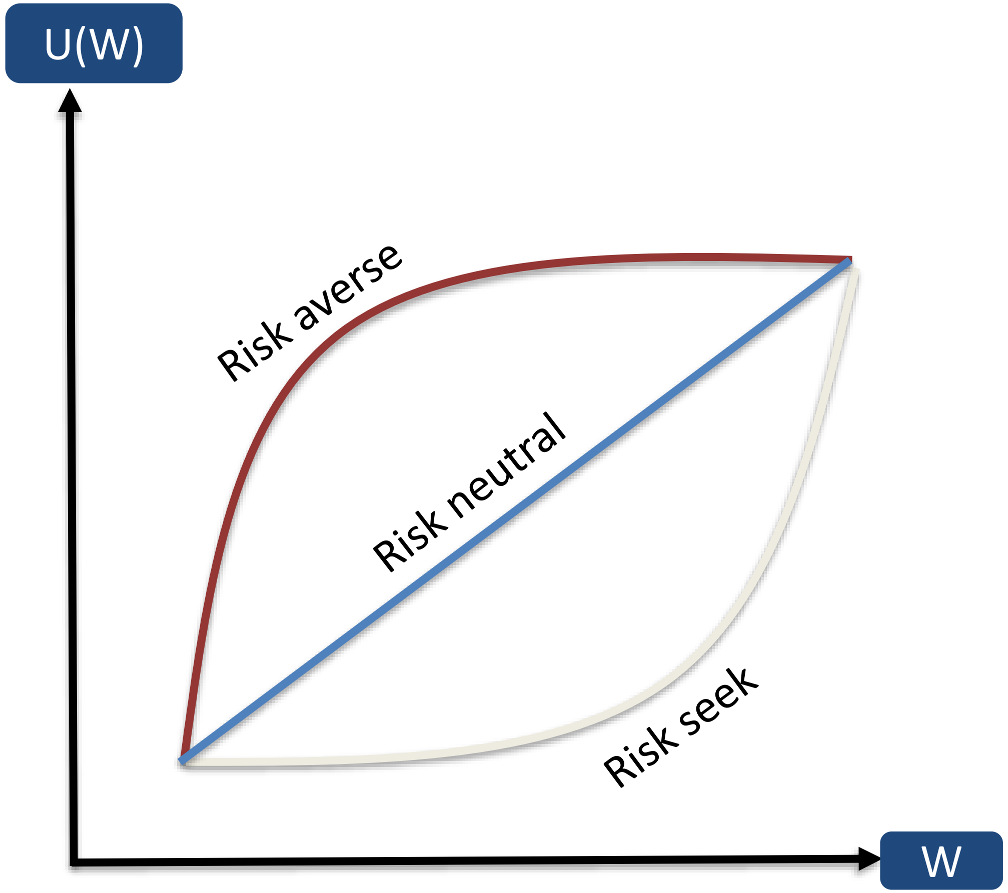
Wealth vs. Utility

- **Wealth** – the money an agent possesses
  - **W** – random wealth
  - W – definite wealth
  - W^0 – initial wealth
- **Utility function** – the satisfaction of an agent from possessing some amount of money
  - U(**W**) – utility of random wealth
  - U(W) – utility of definite wealth
- **Expected utility**
  - $E[U(\mathbf{W})]=\sum_{\forall i} pr_i \times U(W_i)$

Attitude to risk of agents

Agents could be:

- Risk neutral
  - Indifferent to risk
  - $U' = 0$, $U'' = 0$
- Risk averse
  - Avoids risk
  - $U' > 0, U'' < 0$
- Risk seeking
  - Loves to risk
  - $U' > 0, U'' > 0$



Typical examples of utility functions

- Identity function
  - $U(\boldsymbol{W})=\boldsymbol{W}$
- Constant absolute risk aversion (CARA): $-\frac{U''}{U'} = const$
  - $\mathrm{U}(\mathbf{W}) = E_1 - E_2 e^{-\sigma \boldsymbol{W}}$
- Constant relative risk aversion (CRRA): $-\frac{U''}{U'} W = const$
  - $\mathrm{U}(\mathbf{W}) = \begin{cases} \frac{W^{1-\sigma}-1}{1-\sigma} & for\ \sigma \neq 1 \\ \ln(\boldsymbol{W}) & for\ \sigma = 1 \end{cases}$

Attitude to risk of agents. Example

- Toss a coin
  - W^0 =200
  - Win: 100
  - W_{win} =200+100=300
  - Lose: -100
  - W_{loss} =200-100=100

- $E[U(\boldsymbol{W})] = pr_{win} \times (U_{win}) + pr_{loss} \times (U_{loss})$

□ ***Risk neutral***: $U_1(\boldsymbol{W}) = \boldsymbol{W}$

- ○ *Without gamble*: $E[U_1^N(W)] = \mathbf{200}$
- ○ *With gamble:* $E[U_1^G(W)] = 0.5\times300 + 0.5\times100 = \boldsymbol{200}$
- ○ $\boldsymbol{E[U_1^G(W)] = E[U_1^N(W)]}$

□ ***Risk averse***: $U_2(\boldsymbol{W}) = \ln(\boldsymbol{W}) * 10$

- ○ *Without gamble*: $E[U_2^N(W)] \approx \mathbf{53}$
- ○ *With gamble:* $E[U_2^G(W)] = 5\times\ln(300) + 5\times\ln(100) = \boldsymbol{51.5}$
- ○ $\boldsymbol{E[U_2^G(W)] < E[U_2^N(W)]}$

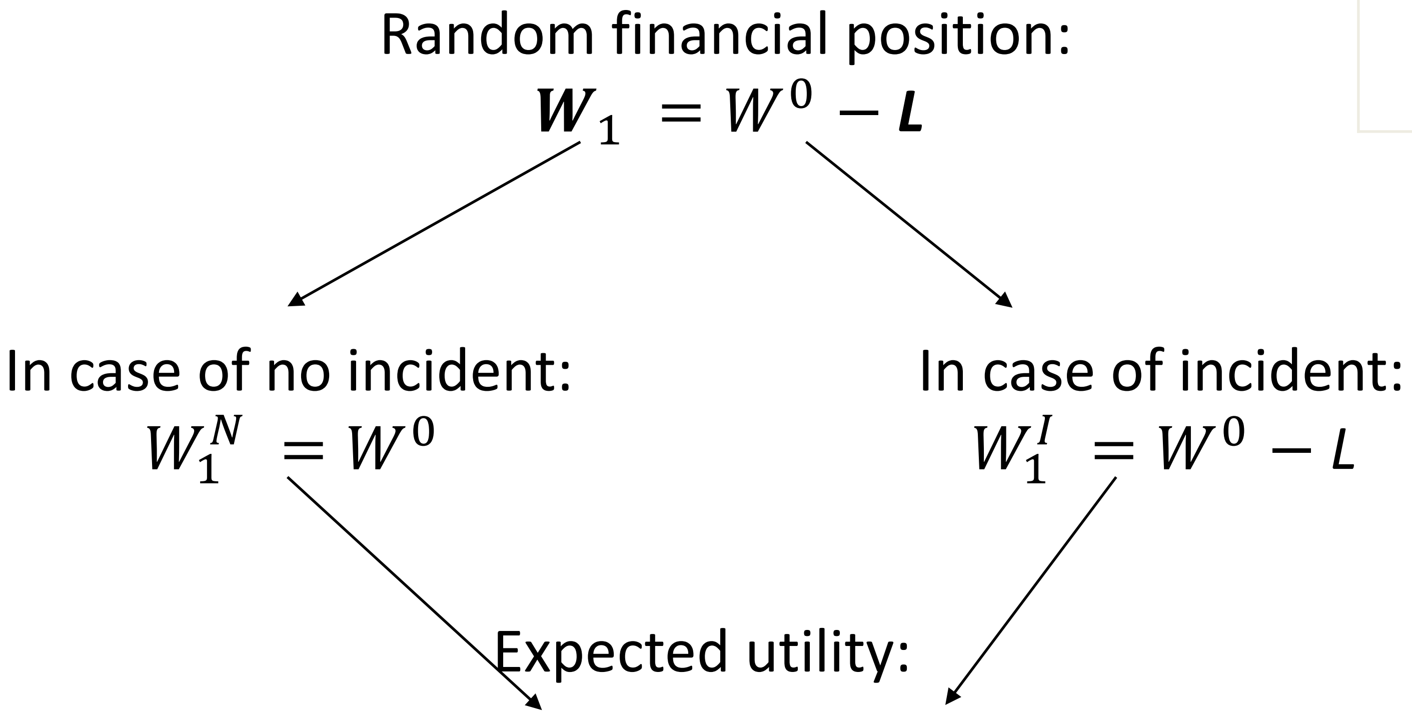
□ ***Risk seeker***: $U_3(\boldsymbol{W}) = W^2/1000$

- ○ *Without gamble*: $E[U_3^N(W)] = \mathbf{40}$
- ○ *With gamble:* $E[U_3^G(W)] = 0.5 \times (300^2/1000) + 0.5 \times (0/1000) = \boldsymbol{50}$
- ○ $\boldsymbol{E[U_3^G(W)] > E[U_3^N(W)]}$

Insured. No insurance.

L – loss ($\boldsymbol{L} \in [0, L]$)

pr – probability of incident



Random financial position:

$\boldsymbol{W}_1 = W^0 - \boldsymbol{L}$

In case of no incident:

$W_1^N = W^0$

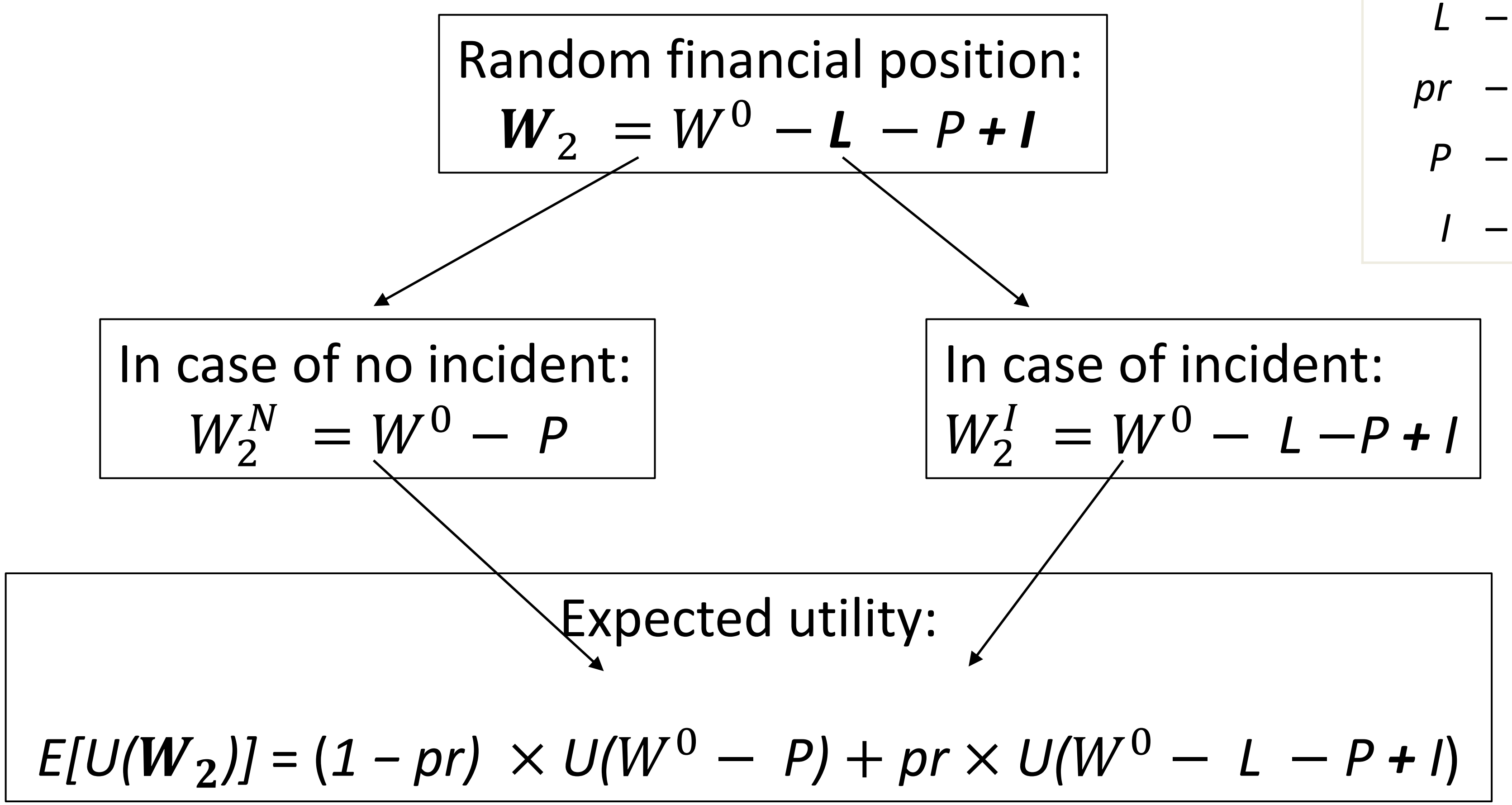
In case of incident:

$W_1^I = W^0 - L$

Expected utility:

$$E[U(\boldsymbol{W}_1)] = (1 - pr) \times U(W^0) + pr \times U(W^0 - L)$$

Insured. With insurance.



Random financial position:

$\boldsymbol{W}_2 = W^0 - \boldsymbol{L} - P + \boldsymbol{I}$

In case of no incident:

$W_2^N = W^0 - P$

In case of incident:

$W_2^I = W^0 - L - P + I$

Expected utility:

$E[U(\boldsymbol{W}_2)] = (1 - pr) \times U(W^0 - P) + pr \times U(W^0 - L - P + I)$

L – loss ($\boldsymbol{L} \in [0,L]$)

pr – probability of incident

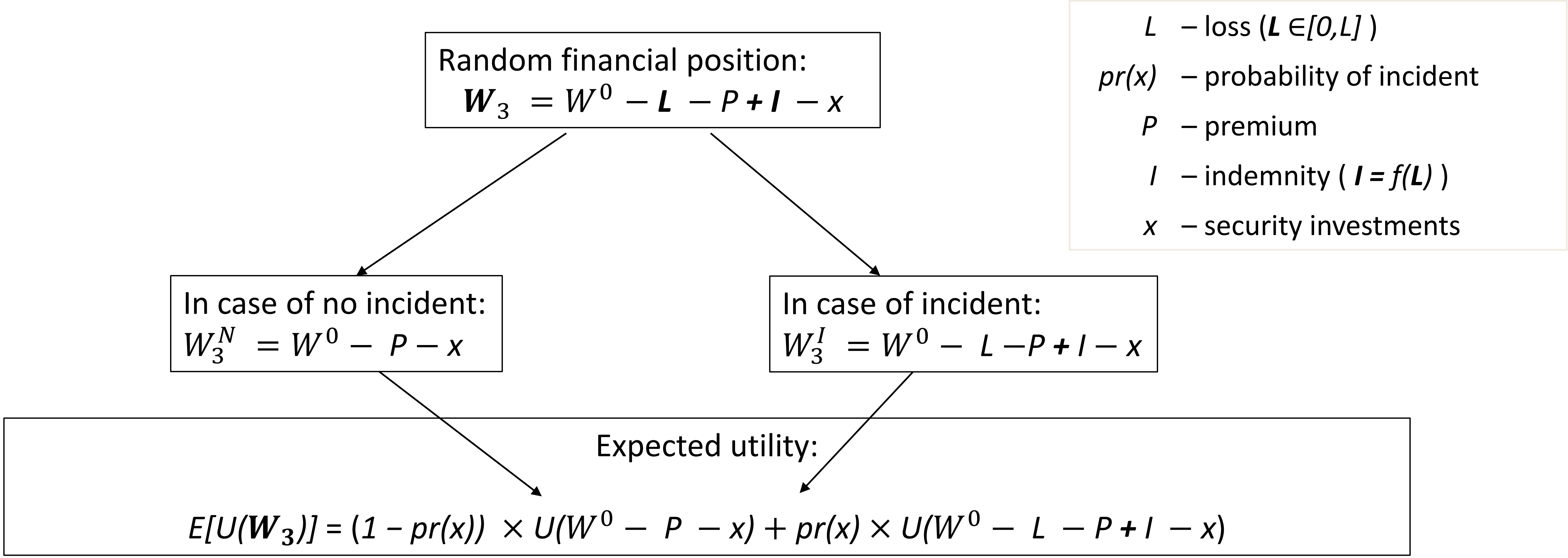
P – premium

I – indemnity ($\boldsymbol{I} = f(\boldsymbol{L})$)

Why does insurance work?

- Recall:
  - Without insurance: $E[U(\boldsymbol{W_1})] = (1 - pr) \times U(W^0) + pr \times U(W^0 - L)$
  - With insurance $E[U(\boldsymbol{W_2})] = (1 - pr) \times U(W^0 - P) + pr \times U(W^0 - L - P + I)$
- Consider
  - Full insurance: $\boldsymbol{I = L}$
  - Fair premium: $P = E[\boldsymbol{L}] = (1 - pr) \times 0 + pr \times L = pr \times L$
    - *Premium is equal to risk*
- *Then (using Jensen's inequality),*
  - Without insurance: $E[U(\boldsymbol{W_1})] \leq U(E[\boldsymbol{W_1}]) = U(W^0 - E[\boldsymbol{L}])$
  - With insurance $E[U(\boldsymbol{W_2})] = U(W^0 - P) = U(W^0 - E[\boldsymbol{L}])$
  - Result: $E[U(\boldsymbol{W_1})] \leq E[U(\boldsymbol{W_2})]$

Insured. Insurance + security



Random financial position:
$\boldsymbol{W}_3 = W^0 - \boldsymbol{L} - P + \boldsymbol{I} - x$

In case of no incident:
$W_3^N = W^0 - P - x$

In case of incident:
$W_3^I = W^0 - L - P + I - x$

Expected utility:

$$E[U(\boldsymbol{W}_3)] = (1 - pr(x)) \times U(W^0 - P - x) + pr(x) \times U(W^0 - L - P + I - x)$$

L – loss ($\boldsymbol{L} \in [0,L]$)

$pr(x)$ – probability of incident

P – premium

I – indemnity ($\boldsymbol{I} = f(\boldsymbol{L})$)

x – security investments

Insurer

- **Insurer** is usually assumed to be **risk neutral**
  - E[U(W)] = $W_s^0 + \sum_{\forall i}(P - E[I_i])]$
  - Unless re-insurance is considered
  - *Beware of correlations!*

- *Two types of insurance (Indemnity specification):*
  - ***Full** insurance: **I** = **L***
  - ***Partial** insurance **I** < **L** (or **I** = **L – D**)*
- Market types (Premium specification)
  - Competitive: fair premium P= $pr \times I$
  - Monopolistic: (usually) maximize utility $= \max_{P}$ E[U(W)]
  - Immature/oligopoly: premium includes $\boldsymbol{\lambda}$ (loading factor): $P = (1 + \lambda)pr \times I_i$

Voluntary and mandatory insurance

- Voluntary participation
  - insureds may skip buying insurance (I>=0)
- Mandatory participation
  - Insureds are bound to buy insurance ($I>=I_{min}\neq 0$)

An example of an analysis

- Consider
  - A risk averse insured
  - Competitive market $\mathrm{P}= pr(x) \times I$
  - Voluntary participation
- Analyse:
  - Would agents/insureds like to buy insurance (cyber insurance market exists)?
  - How much do agents/insureds would like to buy? i.e., find *I* .

An example of an analysis

- $E[U(\boldsymbol{W}_3)] = (1 - pr(x)) \times U(W^0 - pr(x) \times I - x) + pr(x) \times U(W^0 - L - pr(x) \times I + I - x)$

- Maximise utility = FOC(for I):
  - $-pr(x) \times (1 - pr(x)) \times U'(W^0 - pr(x) \times I - x) + pr(x) \times (1 - pr(x)) \times U'(W^0 - L - pr(x) \times I + I - x) = 0$
  - $-U'(W^0 - pr(x) \times I - x) + U'(W^0 - L - pr(x) \times I + I - x) = 0$
  - $U'(W^0 - pr(x) \times I - x) = U'(W^0 - L - pr(x) \times I + I - x)$
  - $W^0 - pr(x) \times I - x = W^0 - L - pr(x) \times I + I - x$
  - $0 = -L + I$
  - $I = L$

Do you want more fun?

- Under the same conditions:
  - Does availability of insurance affects investments in security? How?

1. Consider the case without insurance. Take FOC for x_N. Find x_N.
2. Consider the insurance case. Take FOC for x_I. Find x_I.
3. Compare x_N and x_I.

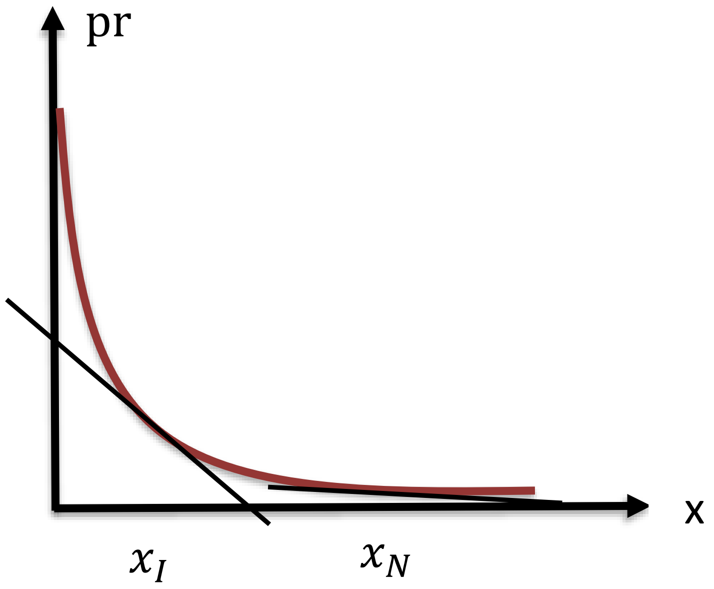
No insurance case:

- $E[U(\boldsymbol{W}_1)] = (1 - pr(x)) \times U(W^0 - x) + pr(x) \times U(W^0 - L - x)$
- $-\,pr'(x)U(W^0 - x) + (1 - pr(x))U'(W^0 - x) + pr'(x)U(W^0 - L - x) + pr(x)U'(W^0 - L - x) = 0$
- $pr'(x_N) = \frac{pr(x_N)U'(W^0 - L - x_N) + (1 - pr(x_N))U'(W^0 - x_N)}{U(W^0 - L - x_N) - U(W^0 - x_N)}$
- $Apply\ Taylor\ expansion$
- $pr'(x_N) = -\frac{pr(x_N)U'(W^0 - L - x_N) + (1 - pr(x_N))U'(W^0 - x_N)}{U'(W^0 - L - x_N)L} > -\frac{1}{L}$

Insurance case

- $E[U(\boldsymbol{W}_3)] = (1 - pr(x)) \times U(W^0 - pr(x) \times L - x) + pr(x) \times U(W^0 - \ L \ - pr(x) \times L + L - x)$
- $E[U(\boldsymbol{W}_3)] = (1 - pr(x)) \times U(W^0 - pr(x) \times I - x) + pr(x) \times U(W^0 \ - pr(x) \times L - x)$
- $E[U(\boldsymbol{W}_3)] = U(W^0 - pr(x) \times L - x)$

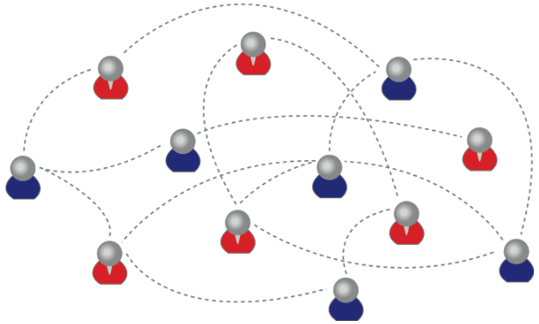
- *FOC:*
  - $(-pr'(x_I)-1)\ U(W^0 - pr(x_I) \times L - x_I)=0$
  - $pr'(x_I)= -\frac{1}{L} < pr'(x_N)$



- $x_N > x_I$ Right?
  - *But only if the Taylor expansion is applicable! For $L \to 0$.*
  - *Otherwise, both situations are possible*

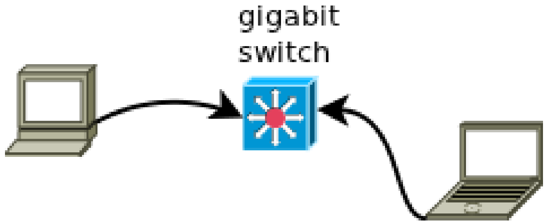
Interdependent security

- Cyber security is interdependent:
  - **Positive externality**: security level of one agent **increases** because of increase of security level of another one
    - Example: virus which uses infected machine for further infection
    - Free riding problem
  - **Negative externality**: security level of one agent **decreases** because of increase of security level of another one
    - Example: an attacker selecting the weakest target.
- Formal model: $pr = pr(x_i, X_{-i})$
  - X_{-i} - *is a set of probabilities of all other agents but agent i*



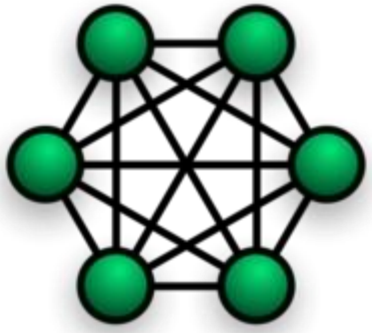
Interdependency and network topology I

- General model:
  - $\pi(x_i)$ - probability of direct attack
  - q_{ij} - probability of contagion from j to i
  - $pr(x_i, X_{-i}) = 1 - (1 - \mathbf{direct}) \times (1 - \boldsymbol{indirect}) = 1 - (1 - \pi(x_i)) \times \prod_{j \neq i}(1 - q_{ij}\pi(x_j))$
- Independent nodes:
  - q_{ij}=0
  - $pr(x_i) = \pi(x_i)$
- Two nodes
  - $q_{ij} = q$
  - $pr(x_i, x_j) = 1 - (1 - \pi(x_i)) \times (1 - q\pi(x_j))$



Interdependency and network topology II

- Complete graph (all nodes are interconnected)
  - $q_{ij} = q$ (usually)
  - $pr(x_i, X_{-i}) = 1 - \left(1 - \pi(x_i)\right) \times \prod_{j \neq i}(1 - q\pi\left(x_j\right))$



- Random graph (Erdos-Renyi graph)
  - q_{ij} *(usually,* $q_{ij} = q$*) is determined probabilistically between 2 nodes.*

- Weakest security link
  - $pr(x_i, X_{-i}) = \min(\pi(x_i), \pi(X_{-i}))$

Social planner/Regulator

- Goal
  - concerned about public good (e.g., high security for the society)
  - $SW = \sum_{\forall i} E[U_i(W_i)]$
- Affects the market through law
  - Mandatory insurance
  - Fines and rebates
  - Bonuses and penalties
  - Mandatory investment level
  - Taxes
  - Liability of contagion

Information asymmetry. Moral hazard

- **Description**: once insurance is bought, an insured behaves in a way to increase its risk
- **Effect**: insured does not know the risk level of insured **after signing the contract**
- **Modelling**: premium does not depend on probability of an incident/ insureds are free to change it after signing the contract (P<pr(x)I)
- **Solutions**: deductibles and security checks by insurer

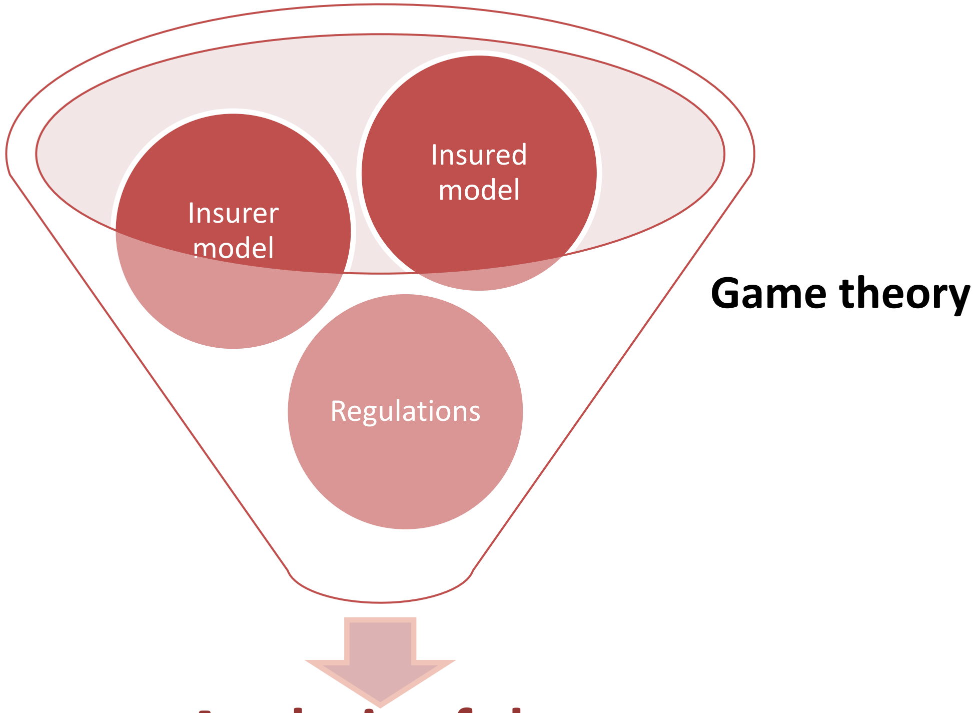
Information asymmetry. Adverse selection

- **Description**: insureds with high risk tend to buy insurance more than the ones with low risk
- **Effect**: insurer does not know the risk level of insured **before signing the contract**
- **Modelling**: insureds are assumed to be of one of two classes: high and low risk, but premium does not depend on the probability of incident ($P \neq P(x_I)$).
- **Solutions**: separate contracts ((P_{low}, I_{low}) and (P_{high}, I_{high})) and partial insurance

Analysis

CYBER INSURANCE

So what?



Analysis of the scenario

Typical questions to answer

- Do insurer and insured find the best strategy
  - There is an equilibrium
- Does cyber insurance market exist?
  - Agents prefer to buy insurance (to not buying it)
- Does Insurance incentivise agents to invest in self-protection
  - Investment level (x) increases in case of buying insurance.
- Reach social optimum
  - Greedy agents invest in security in a non-cooperative scenario as if they were cooperating

Balance it! Game theory.

- Game theory
  - Helps to make a decision for every actor
  - Points out the best decision (strategy)
  - Defines balance
- Set a game:
  - Insurer. Goal maximize its utility :
    - Set contract(s) (P, I)
  - Insured. Goal: maximize its utility:
    - Set x
    - Select a contract (P, I)

Some findings so far

Positive externalities caused by interdependence of security reduce the **incentive** for the **insured** to invest in **self-protection** if **insurance** option is **available**.

Insureds would prefer to **invest** in **self-protection** only if the **fines** and **rebates** regulatory mechanism is applied and **no information asymmetry** exists.

It is **unclear** where **insurance** can be served as a **tool** for approaching **optimal level** of **investments**. Some studies **contradict** on this point.

Effect of **heterogeneity** of nodes and validity of the **discrete** model of **insureds** needs a more focused **study**.

Research gaps

- Dynamic cyber-insurance
- Deal with information asymmetry
- Methods to define security level and effect of security controls
- Increase information sharing capabilities
- New approaches to damage estimation
- Cyber insurance for unique systems
- New theoretical approaches and practical studies of interdependency of security
- Evaluation of real impact because of correlated risks
- Diversification
- New liability models for improving overall security

More practical approach

CURRENT RESEARCH (AT CNR)

How to determine premium?

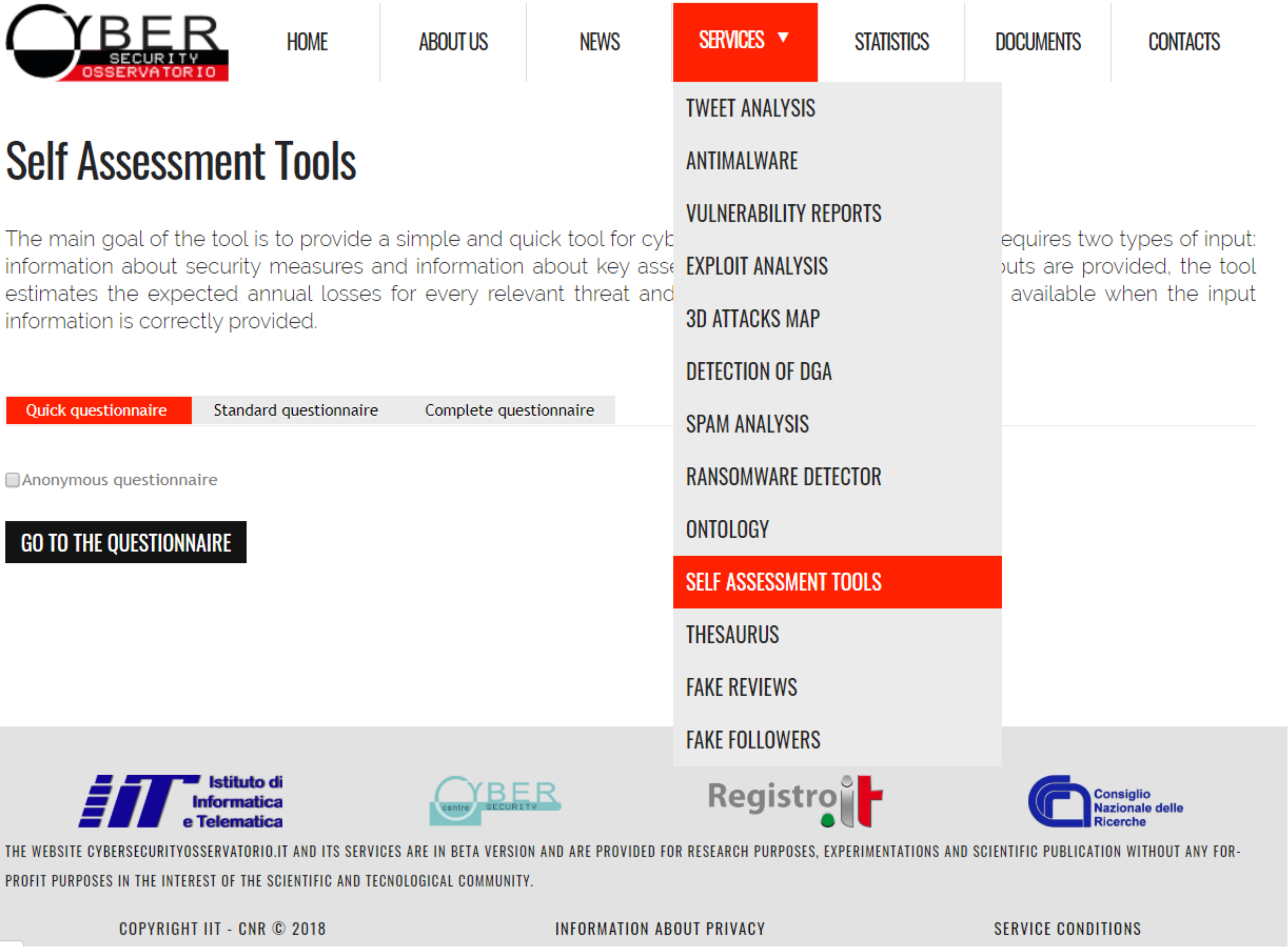
- Using generic information (revenue, number of employees)
  - Not possible to split good and bad security practices
  - Outdated approach
  - High price
- Use risk for determining premium
  - Security discrimination (low premium for less risky)
  - Modern approach
  - Incentivise to invest in self-protection

Cyber Security Risk Assessment at CNR

- We provide **an approach cyber risks assessment** (to be used for cyber insurance premium computation), based on:
  - Basic set of threats for a computer system
  - A set of requirements based on cyber security standards on cyber security
  - A list of major assets
- Our approach:
  - Simple
  - Fast
  - Less knowledge dependent

Self-Assessment Tool for Risk Analsys

- Goal
  - The main goal of our tool is to provide a **simple** and **fast** way for self-assessment of cyber risks.
- On-line:
  - https://www.cybersecurityosservatorio.it
  - Login
  - Go to Services->Self Assessment tools



Self Assessment Tools

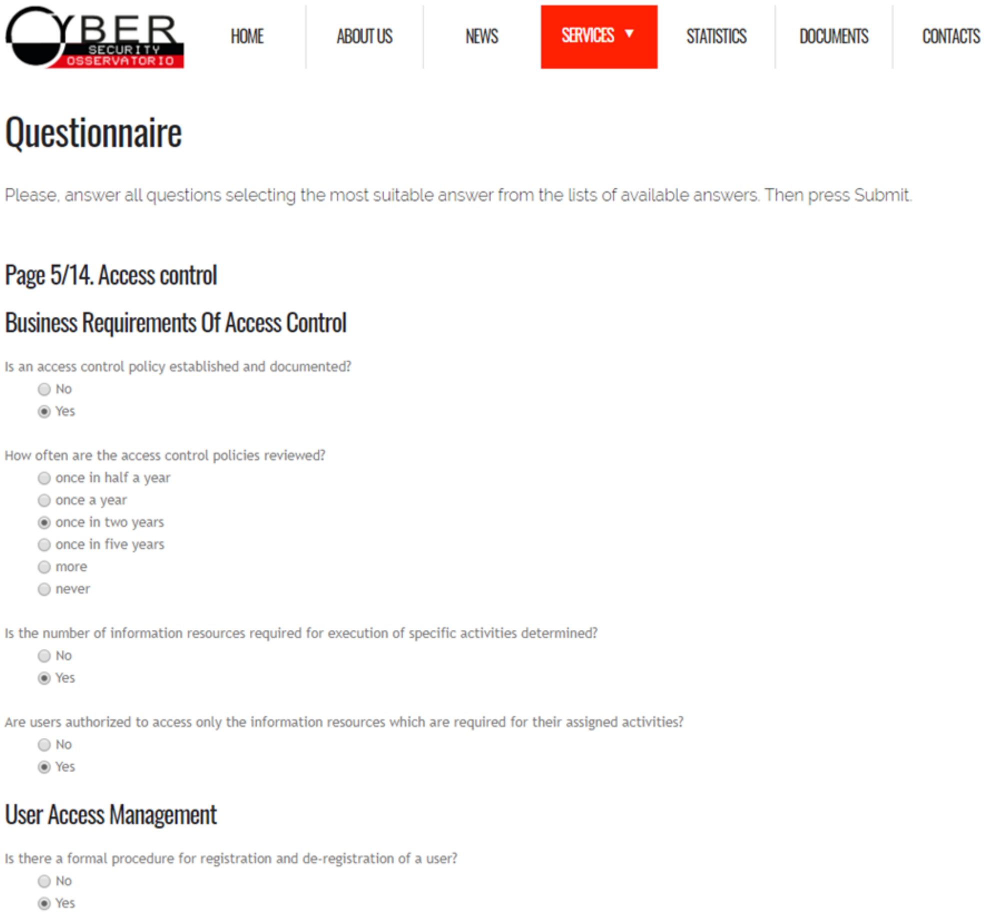
The main goal of the tool is to provide a simple and quick tool for cyb equires two types of input: information about security measures and information about key asse outs are provided, the tool estimates the expected annual losses for every relevant threat and available when the input information is correctly provided.

□ Anonymous questionnaire

THE WEBSITE CYBERSECURITYOSSERVATORIO.IT AND ITS SERVICES ARE IN BETA VERSION AND ARE PROVIDED FOR RESEARCH PURPOSES, EXPERIMENTATIONS AND SCIENTIFIC PUBLICATION WITHOUT ANY FOR-PROFIT PURPOSES IN THE INTEREST OF THE SCIENTIFIC AND TECNOLOGICAL COMMUNITY.

COPYRIGHT IIT - CNR © 2018

Tool input



Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

Page 5/14. Access control

Business Requirements Of Access Control

Is an access control policy established and documented?

○ No
● Yes

How often are the access control policies reviewed?

○ once in half a year
○ once a year
● once in two years
○ once in five years
○ more
○ never

Is the number of information resources required for execution of specific activities determined?

○ No
● Yes

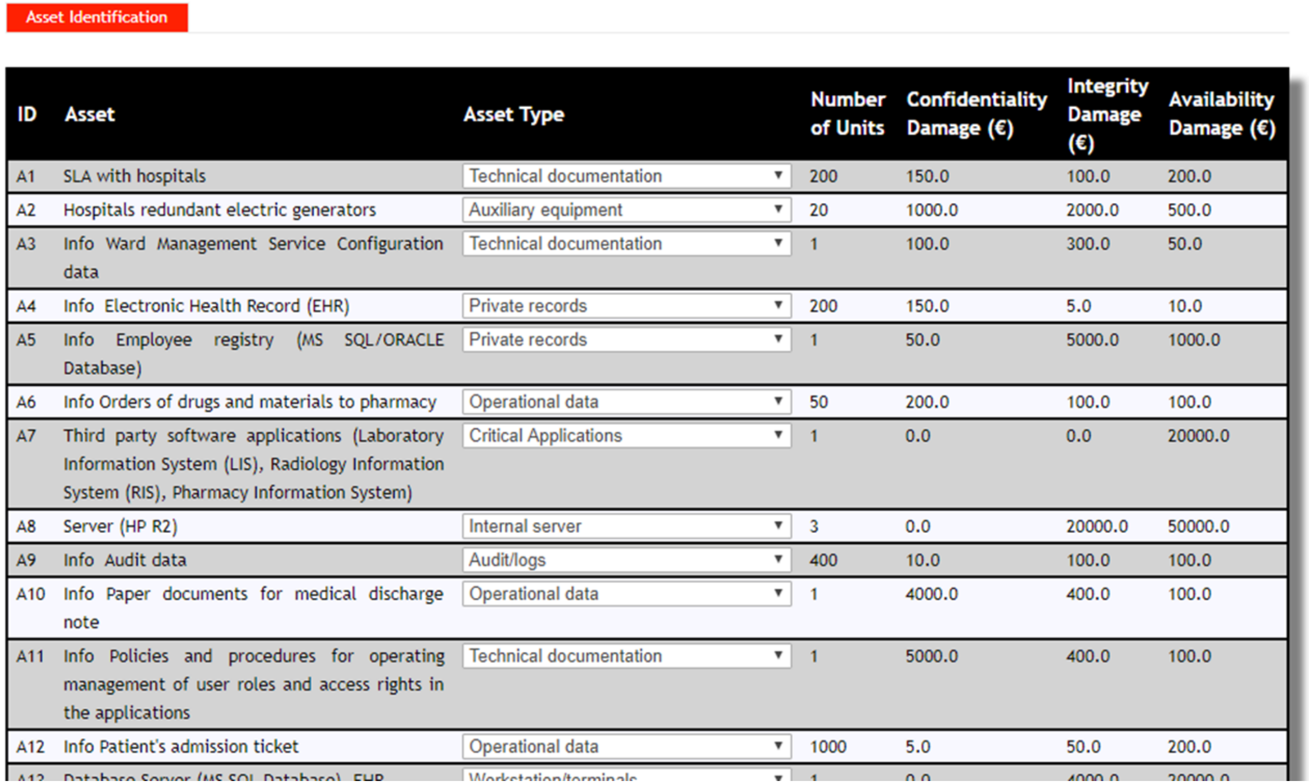
Are users authorized to access only the information resources which are required for their assigned activities?

○ No
● Yes

User Access Management

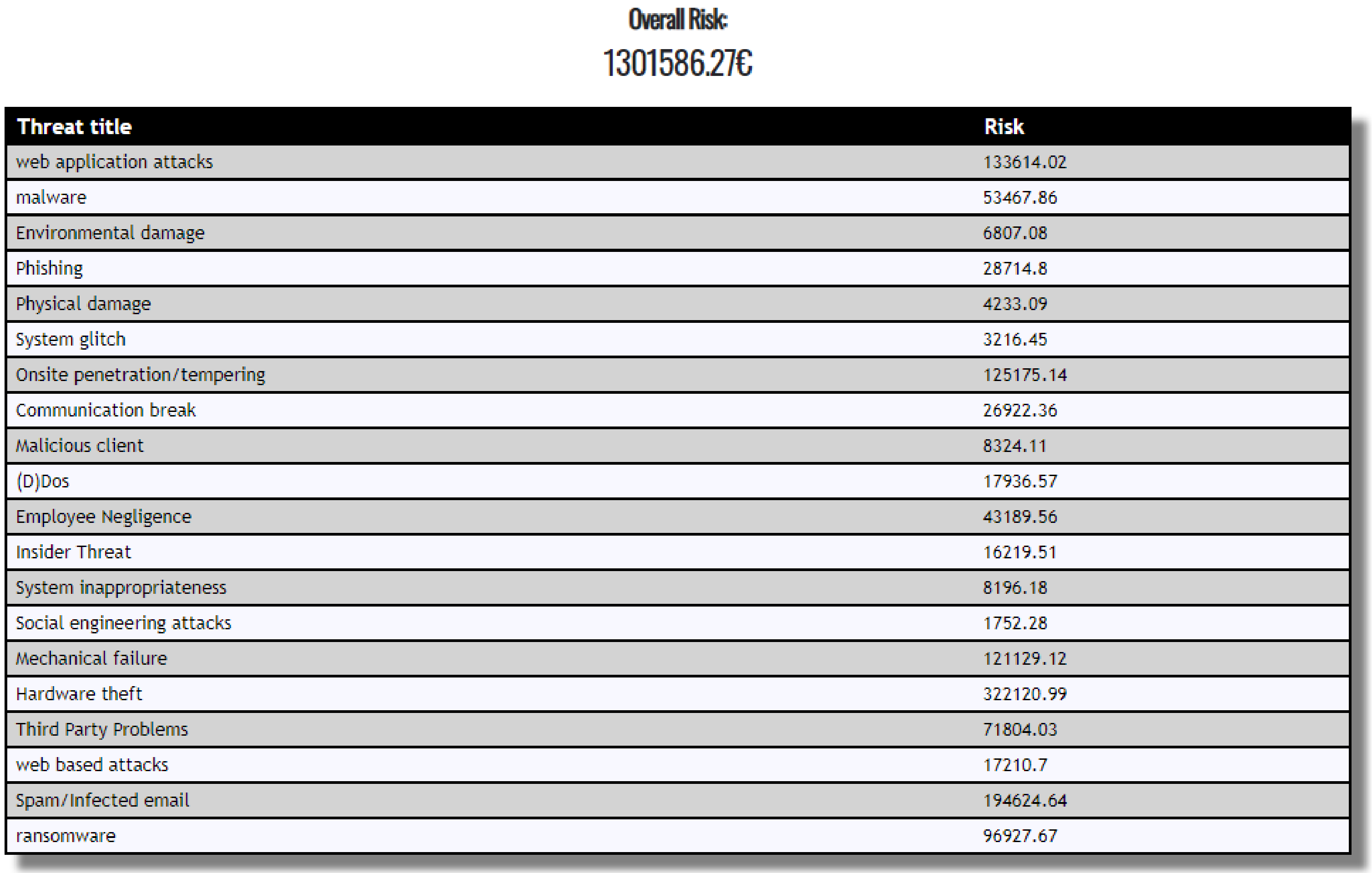
Is there a formal procedure for registration and de-registration of a user?

○ No
● Yes



ID	Asset	Asset Type	Number of Units	Confidentiality Damage (€)	Integrity Damage (€)	Availability Damage (€)
A1	SLA with hospitals	Technical documentation ▼	200	150.0	100.0	200.0
A2	Hospitals redundant electric generators	Auxiliary equipment ▼	20	1000.0	2000.0	500.0
A3	Info Ward Management Service Configuration data	Technical documentation ▼	1	100.0	300.0	50.0
A4	Info Electronic Health Record (EHR)	Private records ▼	200	150.0	5.0	10.0
A5	Info Employee registry (MS SQL/ORACLE Database)	Private records ▼	1	50.0	5000.0	1000.0
A6	Info Orders of drugs and materials to pharmacy	Operational data ▼	50	200.0	100.0	100.0
A7	Third party software applications (Laboratory Information System (LIS), Radiology Information System (RIS), Pharmacy Information System)	Critical Applications ▼	1	0.0	0.0	20000.0
A8	Server (HP R2)	Internal server ▼	3	0.0	20000.0	50000.0
A9	Info Audit data	Audit/logs ▼	400	10.0	100.0	100.0
A10	Info Paper documents for medical discharge note	Operational data ▼	1	4000.0	400.0	100.0
A11	Info Policies and procedures for operating management of user roles and access rights in the applications	Technical documentation ▼	1	5000.0	400.0	100.0
A12	Info Patient's admission ticket	Operational data ▼	1000	5.0	50.0	200.0
A13	Database Server (MS SQL Database) EHR	Workstation/terminals ▼	1	0.0	4000.0	20000.0

Results



Overall Risk:

1301586.27€

Threat title	Risk
web application attacks	133614.02
malware	53467.86
Environmental damage	6807.08
Phishing	28714.8
Physical damage	4233.09
System glitch	3216.45
Onsite penetration/tempering	125175.14
Communication break	26922.36
Malicious client	8324.11
(D)Dos	17936.57
Employee Negligence	43189.56
Insider Threat	16219.51
System inappropriateness	8196.18
Social engineering attacks	1752.28
Mechanical failure	121129.12
Hardware theft	322120.99
Third Party Problems	71804.03
web based attacks	17210.7
Spam/Infected email	194624.64
ransomware	96927.67

CyberSure

- Goal: develop an on-line tool for risk-based and monitoring-supported cyber insurance management

- Compute risk of an insured
  - SATRA tool based on ISO 27002
- Set up premium based on the risk assessment results (HDI tool)
- Monitor fulfilment of the declared security features (CUMULUS)
- Re-assess risk and modify premium if monitoring detects failures (SATRA and HDI)

Risk assessment elements

Controls: ISO 27002

Policies

Organisation

HR evaluation

Physical and environmental protection

Access control

System protection

Cryptography

Communication security

Incident management

Asset management

Partner protection

Compliance

System acquisition, development and maintenance

Business continuity

Asset types

Private records

Business process

Operational data

Audit logs

Web service

Critical application

Web application

…

Threats

Malware/ransomware

web-based attacks

web-application attacks

(D)Dos

Communication break

Social engineering attacks

Insider Threat

Physical damage

Hardware theft

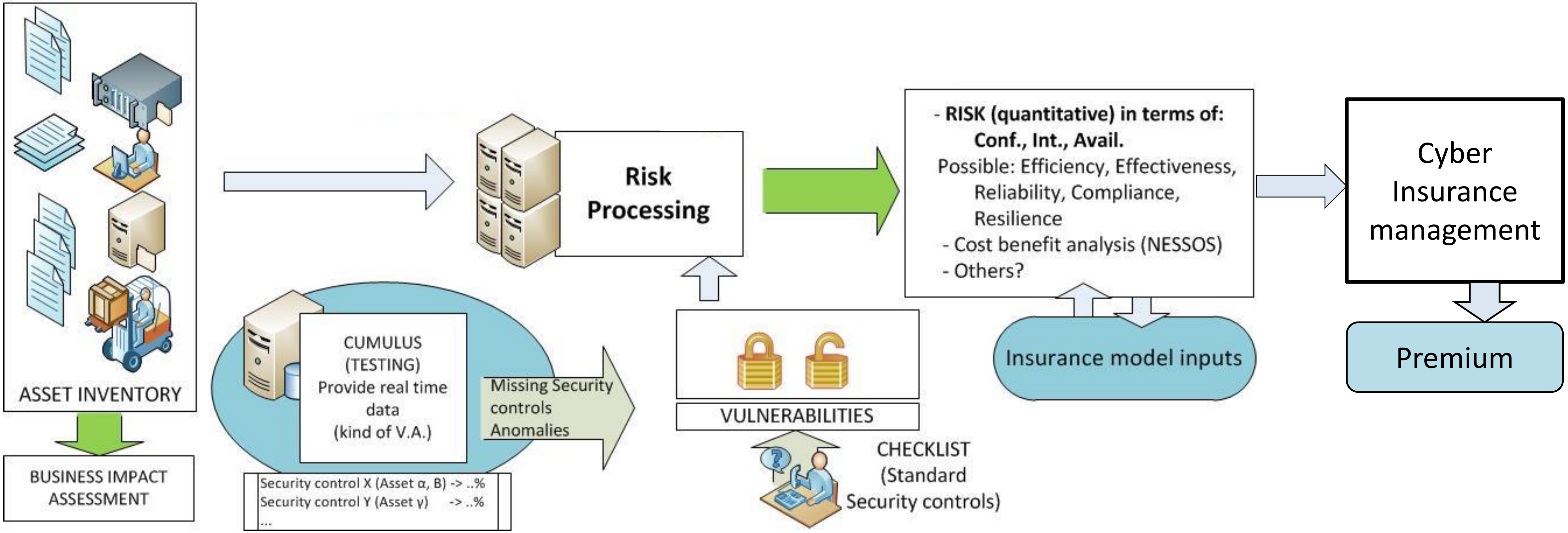
Environmental damage

Employee Negligence

System glitch

…

H2020 EU project on Cyber Insurance - CyberSure


ASSET INVENTORY
BUSINESS IMPACT ASSESSMENT
CUMULUS (TESTING) Provide real time data (kind of V.A.)
Missing Security controls Anomalies
Security control X (Asset α, B) -> ..%
Security control Y (Asset γ) -> ..%
...
Risk Processing
VULNERABILITIES
CHECKLIST (Standard Security controls)
- RISK (quantitative) in terms of: Conf., Int., Avail.
Possible: Efficiency, Effectiveness, Reliability, Compliance, Resilience
- Cost benefit analysis (NESSOS)
- Others?
Insurance model inputs
Cyber Insurance management
Premium

Medina

MEDINA

- Goal: develop a modular framework, which will allow cloud providers to manage certification of their cloud supply chain continuously.
- Risk assessment is used
  - to evaluate non-conformities with the selected certification scheme
  - ensure that the selected requirements are useful for cloud provider
- Risk assessment for cloud products
- Based on upcoming EUCS (for cloud services)

Risk assessment elements

Controls EUCS

Organisation Of Information Security
Information Security Policies
Risk Management
Human Resources
Asset Management
Physical Security
Operational Security
Identity, Authentication, And Access Control Management
Cryptography And Key Management
Communication Security
Portability And Interoperability
Change And Configuration Management
Development Of Information Systems
Procurement Management
Incident Management
Business Continuity
Compliance
User Documentation
Dealing With Investigation Requests From Government Agencies
Product Safety And Security (Pss)

Asset types

CI CD
Virtual Machines and Containers
Database Services
Images
IoT
Networking
Client trust
…

Threats

Account hijacking (client/CSP)
web-application threat
Meta- interfaces (client/CSP)
Web-based attack
CI/CD attacks
Poor IAM(client/ CSP)
Exploit Poor configuration (client/CSP)
DoS (client/CSP)
Insider hacker
Compromised Communication
System glitch
Malicious client
Unlawful client
Malicious client employee
CSP's employee Negligence and mistakes
Third party problems
Hardware theft/loss (DC)
Environment threat (DC)
Physical threat (DC)

SPARTA

SPARTA

- CAPE - Continuous assessment in polymorphous environments

- Risk assessment is used to evaluate a software product according the quality of its SDLC.

- Risk assessment for software products
  - Software specific assets (process, user/internal data, context etc.)
- Based on Common Criteria ISO / IEC 15408

Risk assessment elements

Controls (Common Criteria)

Security audit

Communication Repudiation

User Data

Identification and authentication

Security management

Failure/Recovery protection

Exported system data

Resource utilisation

System access

Trusted path/channels

Vulnerability Assessment

Problem, objectives and requirements

Development

Guidance Documents

Life-Cycle support

Tests

Asset types

User data

- Stored
- Transferred
- Exported

Process

- Transferred
- Exported

Context

Threats (STRIDE)

Spoofing

Tampering

Repudiation

Information Disclosure

DoS

Elevation of Privileges

Projects

- http://www.cybersure.eu/
- https://medina-project.eu/
- https://www.sparta.eu/

Cyber Sure

MEDINA

SPARTA

Conclusion

- Cyber insurance is a rapidly developing market.
- It is young, immature and faces many challenges, both practical and theoretical.
- Cyber insurance is not only an economical means to treat residual risk, but it is also could be an instrument to rise cyber protection investments
- Interdependency of security, correlated risks and information asymmetry are ones of the main obstacles for cyber insurance to be an incentive for self-protection.
- Cyber insurance has a lot of room for research.
- Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando and Artsiom Yautsiukhin. Cyber-Insurance Survey. Computer Science Review, Volume 24, May 2017, pp 35-61, 2017.

Questions?

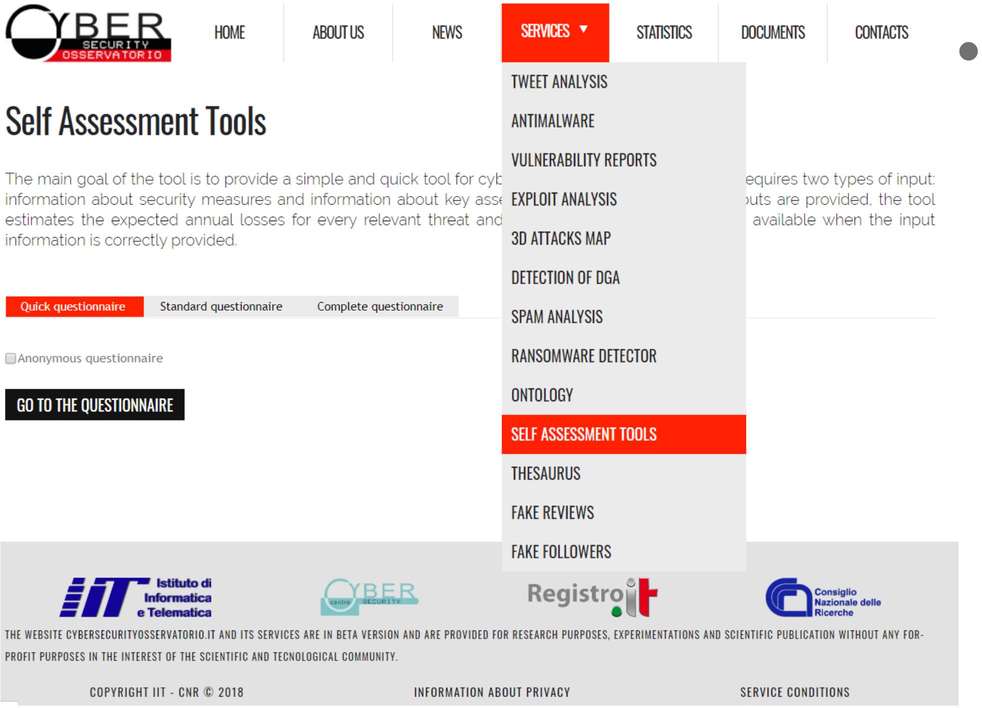
This work is partially supported and uses the material developed in the scope of the following EU projects:

MEDINA SPARTA Cyber Sure

Lo strumento di analysi e riduzione dei rischi

Artsiom Yautsiukhin (IIT-CNR)

Lo scopo



Self Assessment Tools

The main goal of the tool is to provide a simple and quick tool for cyb equires two types of input:
information about security measures and information about key asse uts are provided, the tool
estimates the expected annual losses for every relevant threat and available when the input
information is correctly provided.

Quick questionnaire | Standard questionnaire | Complete questionnaire

□ Anonymous questionnaire

GO TO THE QUESTIONNAIRE

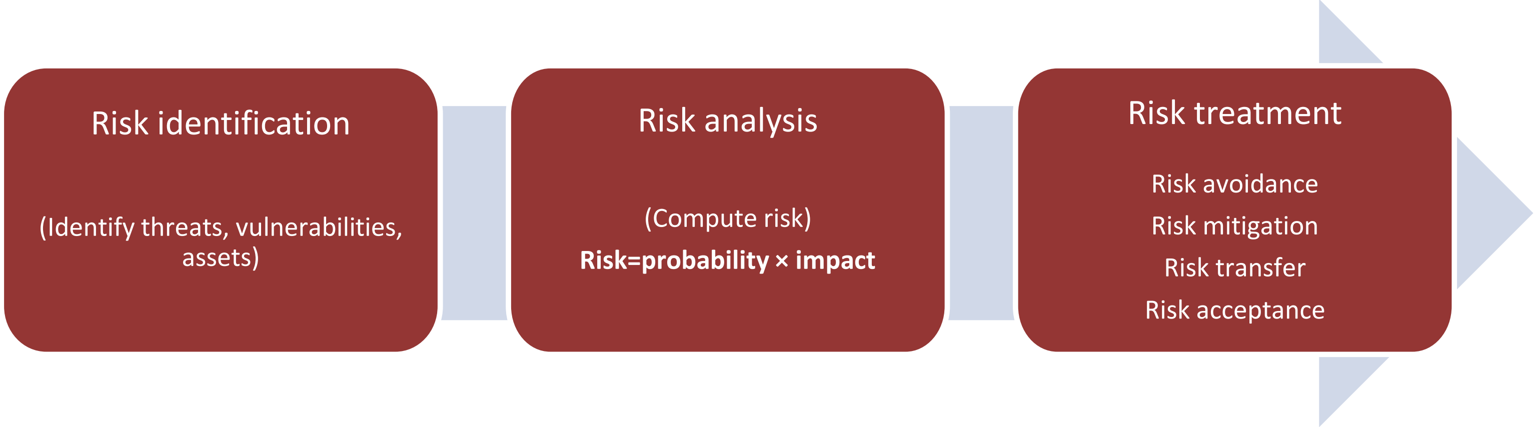
THE WEBSITE CYBERSECURITYOSSERVATORIO.IT AND ITS SERVICES ARE IN BETA VERSION AND ARE PROVIDED FOR RESEARCH PURPOSES, EXPERIMENTATIONS AND SCIENTIFIC PUBLICATION WITHOUT ANY FOR-PROFIT PURPOSES IN THE INTEREST OF THE SCIENTIFIC AND TECNOLOGICAL COMMUNITY.

COPYRIGHT IIT - CNR © 2018 | INFORMATION ABOUT PRIVACY | SERVICE CONDITIONS

- Lo scopo principale del nostro strumento è di offrire un modo **semplice** e **veloce** per effettuare un **self-assessment** dei cyber rischi e **ottimizzare gli investimenti** in sicurezza cyber.

Risk assessment and risk treatment

- Il **risk assessment** è un processo di identificazione e valutazione dei rischi.
- Il **risk treatment** è un processo per modificare dei rischi.



Risk identification

(Identify threats, vulnerabilities, assets)

Risk analysis

(Compute risk)

Risk=probability × impact

Risk treatment

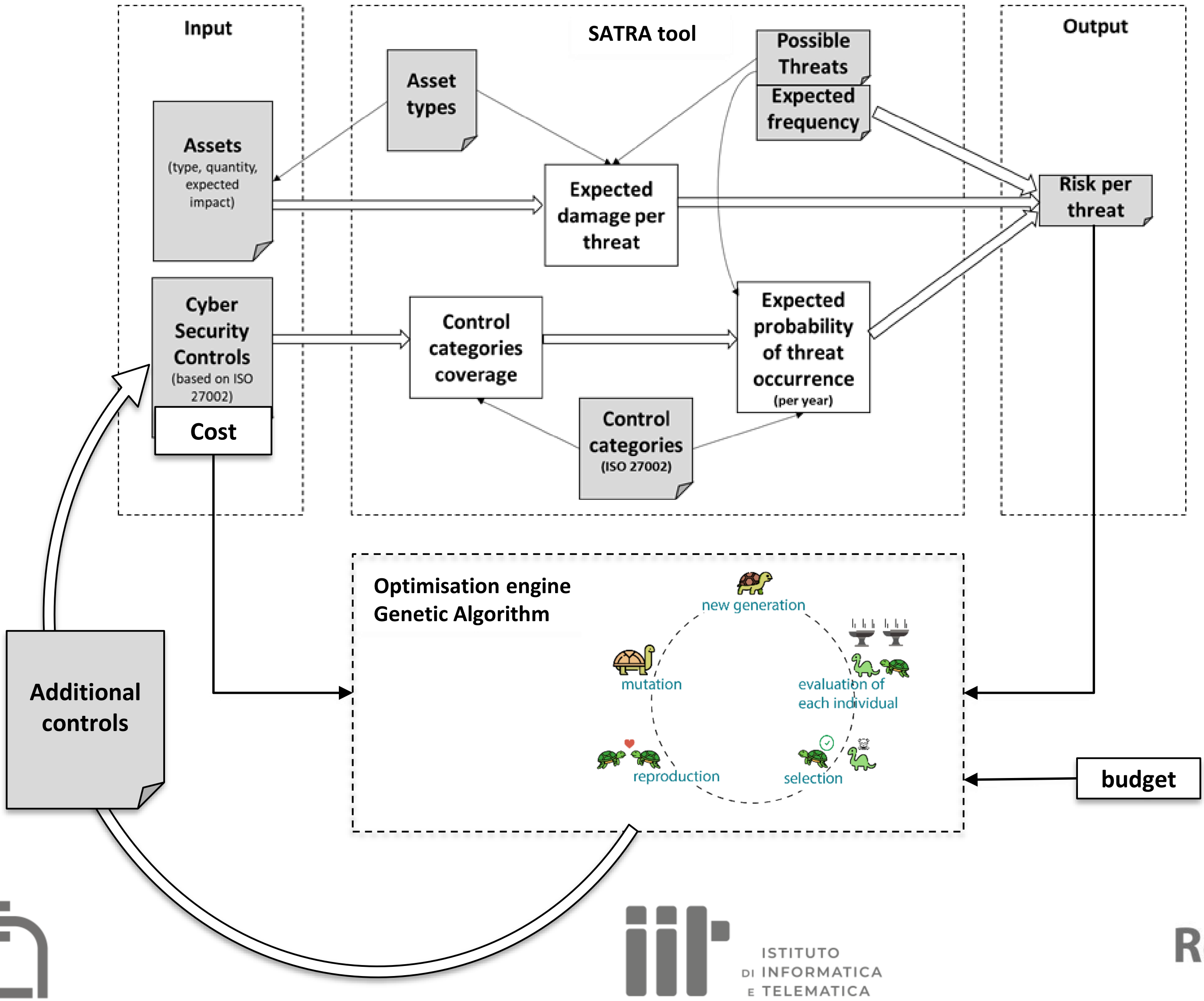
Risk avoidance

Risk mitigation

Risk transfer

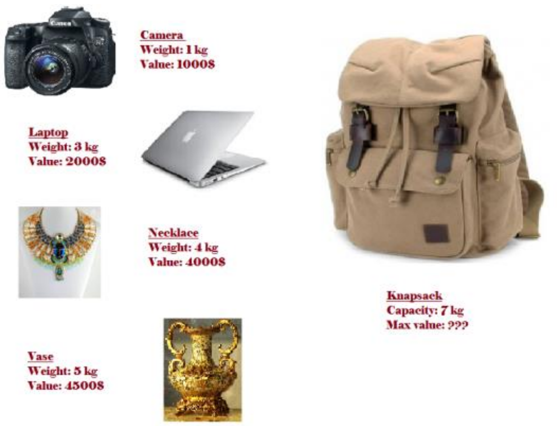
Risk acceptance

Modello base

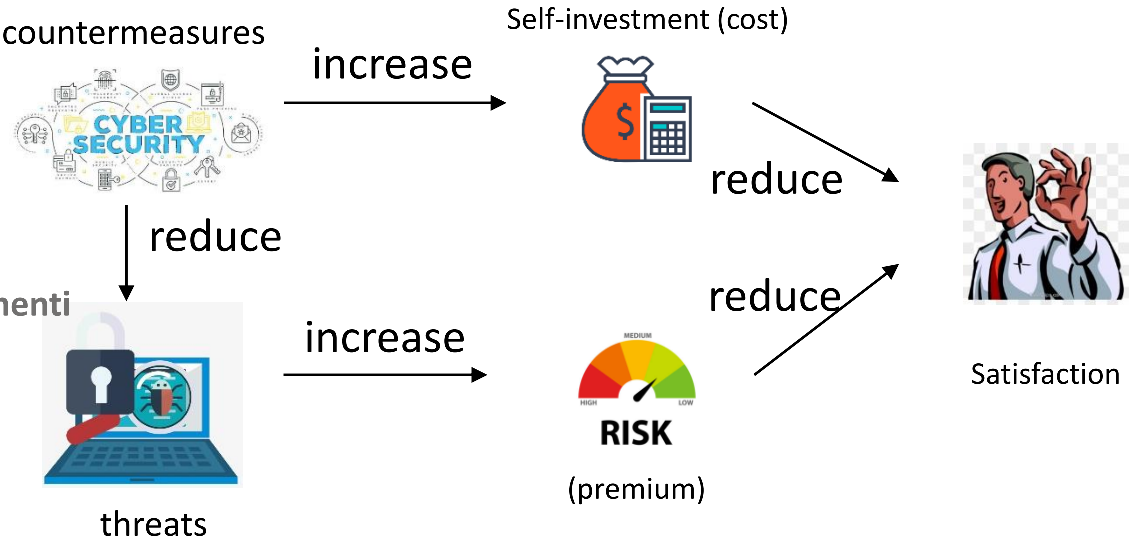

Input
SATRA tool
Output
Asset types
Possible Threats
Expected frequency
Assets (type, quantity, expected impact)
Expected damage per threat
Risk per threat
Cyber Security Controls (based on ISO 27002)
Cost
Control categories coverage
Expected probability of threat occurrence (per year)
Control categories (ISO 27002)
Optimisation engine Genetic Algorithm
new generation
evaluation of each individual
selection
reproduction
mutation
budget
Additional controls

Il problema matematico

- **Knapsack problem.**
  - Avere uno zaino di **capacità** limitata e un oggetti di varie **valore** e **peso**:
    - Aggiungere elementi per massimizzare il **valore** complessivo
    - Rispettare il limite di **capacità** (peso).



- **Il nostra problema**
  - La capacità e opzionale, trovare:
    - per massimizzare
      - **valore** complessivo + **investimenti**
    - Selezionare I **controlli** di sicurezza



countermeasures

increase

Self-investment (cost)

reduce

reduce

reduce

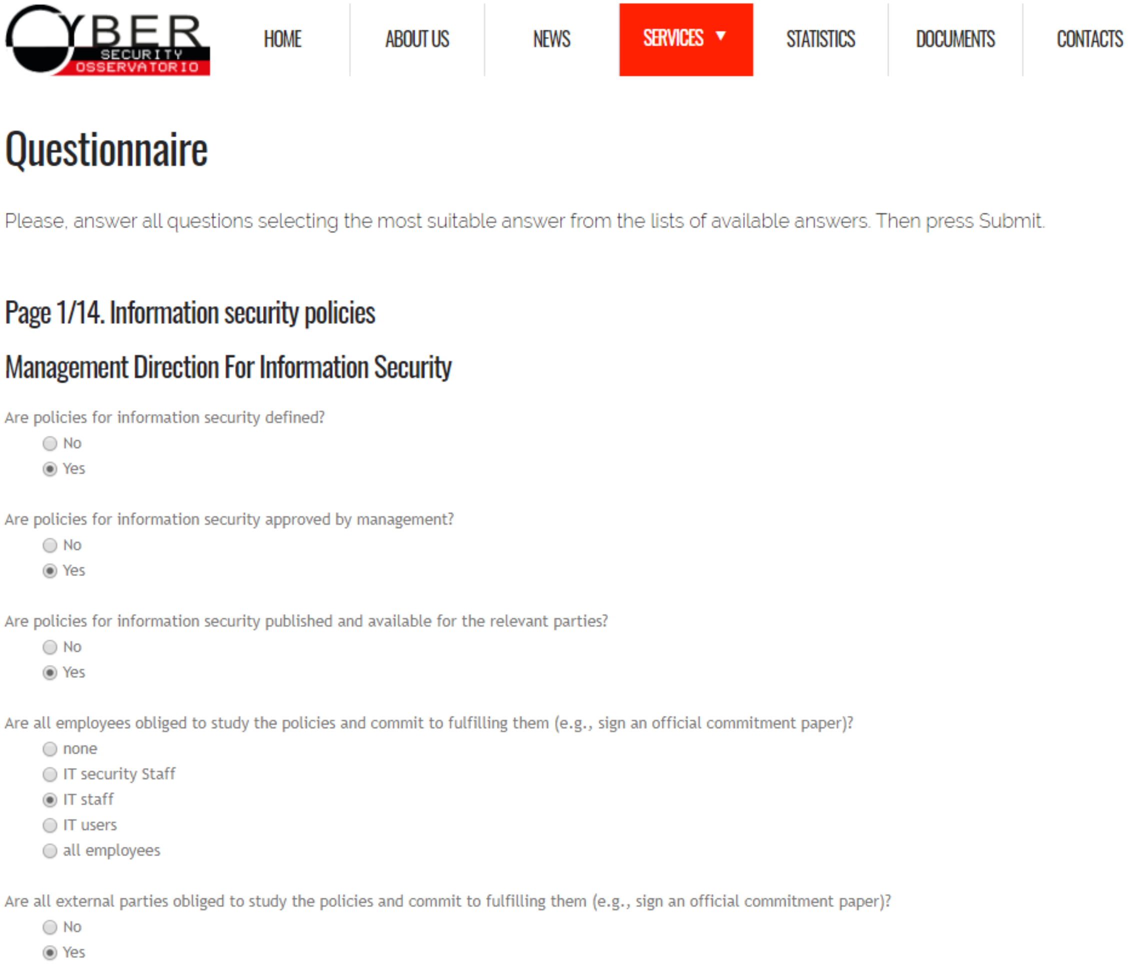
increase

threats

(premium)

Satisfaction

Controlli di sicurezza



Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

Page 1/14. Information security policies

Management Direction For Information Security

Are policies for information security defined?
○ No
● Yes

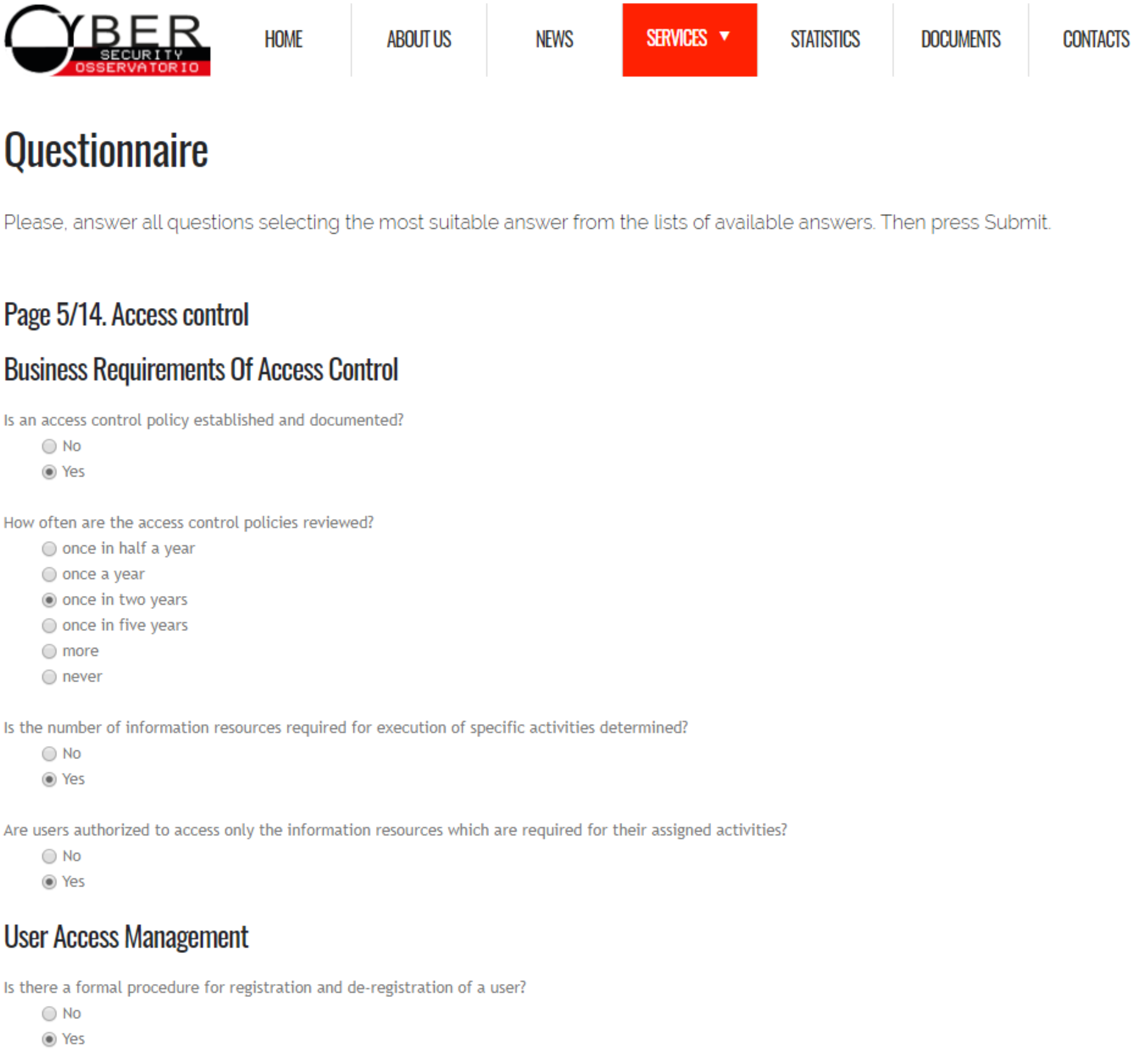
Are policies for information security approved by management?
○ No
● Yes

Are policies for information security published and available for the relevant parties?
○ No
● Yes

Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?
○ none
○ IT security Staff
● IT staff
○ IT users
○ all employees

Are all external parties obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?
○ No
● Yes

Controlli di sicurezza



Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

Page 5/14. Access control

Business Requirements Of Access Control

Is an access control policy established and documented?

○ No
● Yes

How often are the access control policies reviewed?

○ once in half a year
○ once a year
● once in two years
○ once in five years
○ more
○ never

Is the number of information resources required for execution of specific activities determined?

○ No
● Yes

Are users authorized to access only the information resources which are required for their assigned activities?

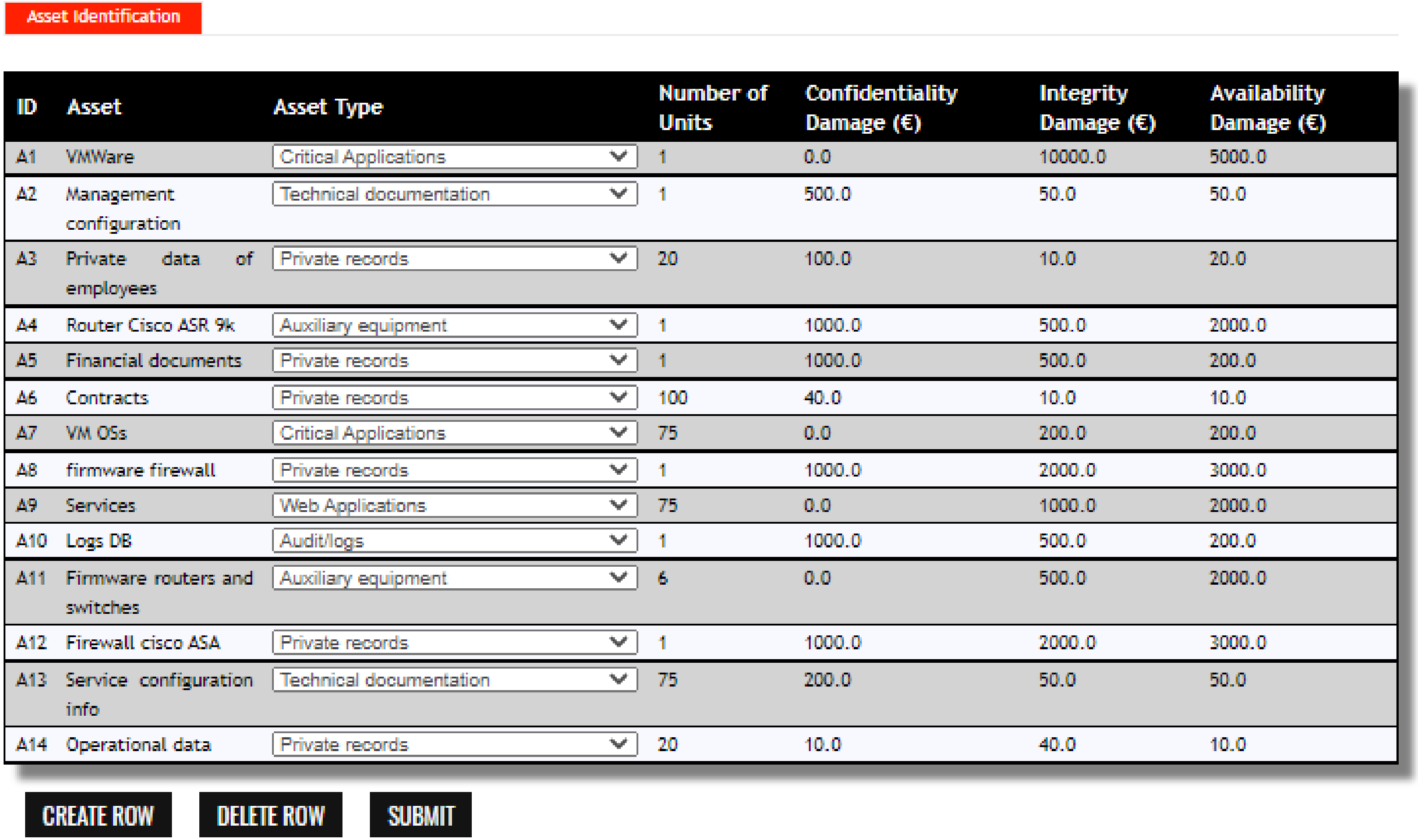
○ No
● Yes

User Access Management

Is there a formal procedure for registration and de-registration of a user?

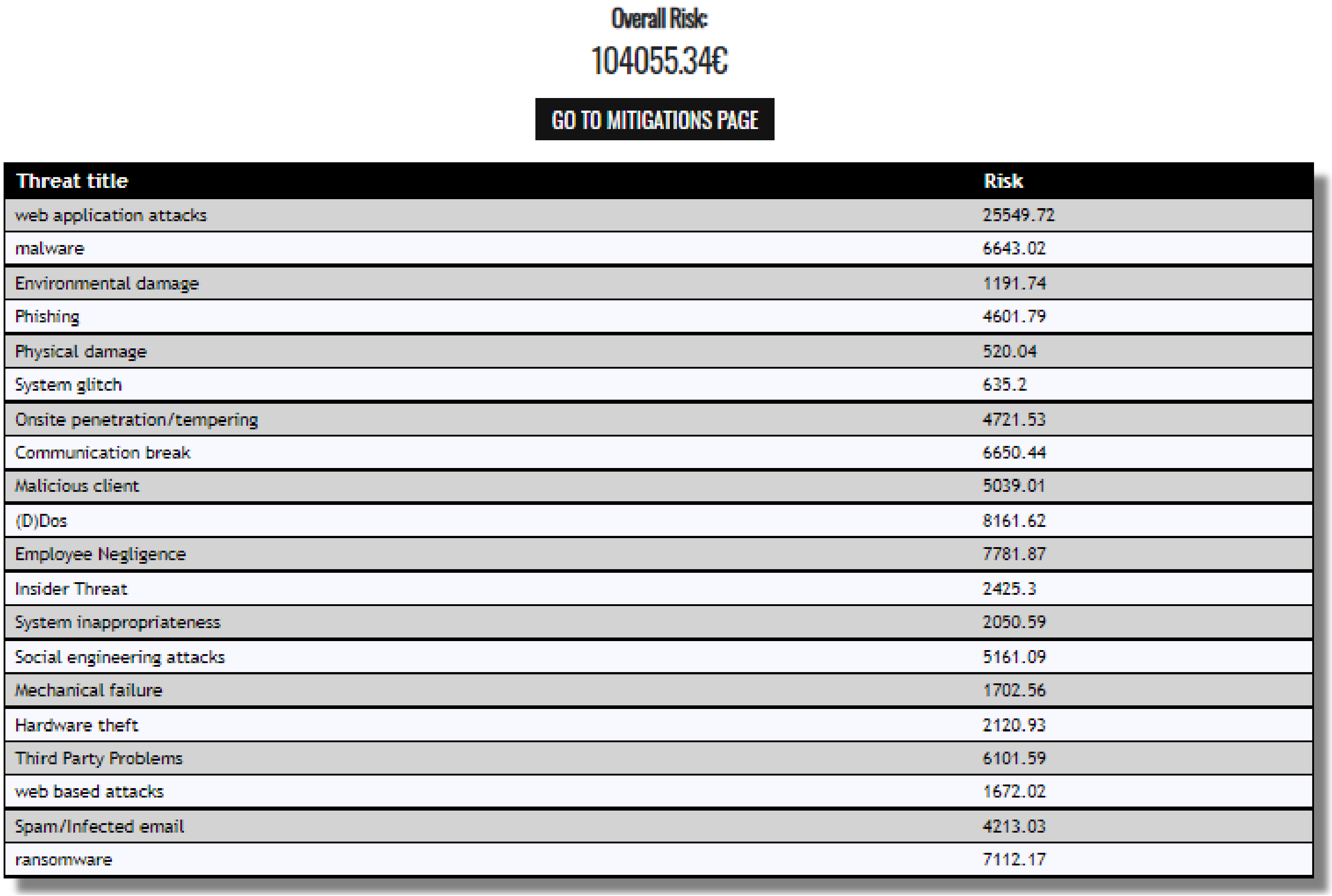
○ No
● Yes

Assets



ID	Asset	Asset Type	Number of Units	Confidentiality Damage (€)	Integrity Damage (€)	Availability Damage (€)
A1	VMWare	Critical Applications	1	0.0	10000.0	5000.0
A2	Management configuration	Technical documentation	1	500.0	50.0	50.0
A3	Private data of employees	Private records	20	100.0	10.0	20.0
A4	Router Cisco ASR 9k	Auxiliary equipment	1	1000.0	500.0	2000.0
A5	Financial documents	Private records	1	1000.0	500.0	200.0
A6	Contracts	Private records	100	40.0	10.0	10.0
A7	VM OSs	Critical Applications	75	0.0	200.0	200.0
A8	firmware firewall	Private records	1	1000.0	2000.0	3000.0
A9	Services	Web Applications	75	0.0	1000.0	2000.0
A10	Logs DB	Audit/logs	1	1000.0	500.0	200.0
A11	Firmware routers and switches	Auxiliary equipment	6	0.0	500.0	2000.0
A12	Firewall cisco ASA	Private records	1	1000.0	2000.0	3000.0
A13	Service configuration info	Technical documentation	75	200.0	50.0	50.0
A14	Operational data	Private records	20	10.0	40.0	10.0

Resulti. Rischi

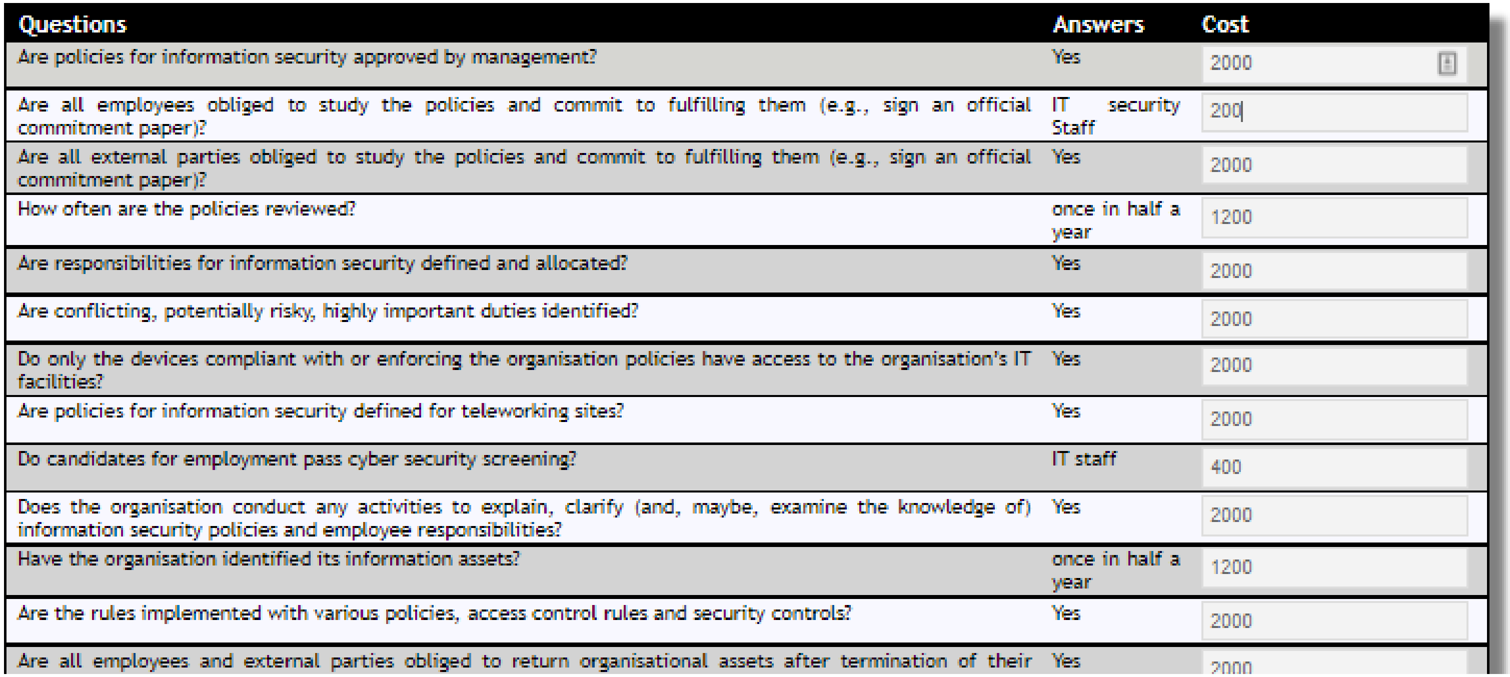


Overall Risk:

104055.34€

Threat title	Risk
web application attacks	25549.72
malware	6643.02
Environmental damage	1191.74
Phishing	4601.79
Physical damage	520.04
System glitch	635.2
Onsite penetration/tempering	4721.53
Communication break	6650.44
Malicious client	5039.01
(D)Dos	8161.62
Employee Negligence	7781.87
Insider Threat	2425.3
System inappropriateness	2050.59
Social engineering attacks	5161.09
Mechanical failure	1702.56
Hardware theft	2120.93
Third Party Problems	6101.59
web based attacks	1672.02
Spam/Infected email	4213.03
ransomware	7112.17

Control costs (optional)

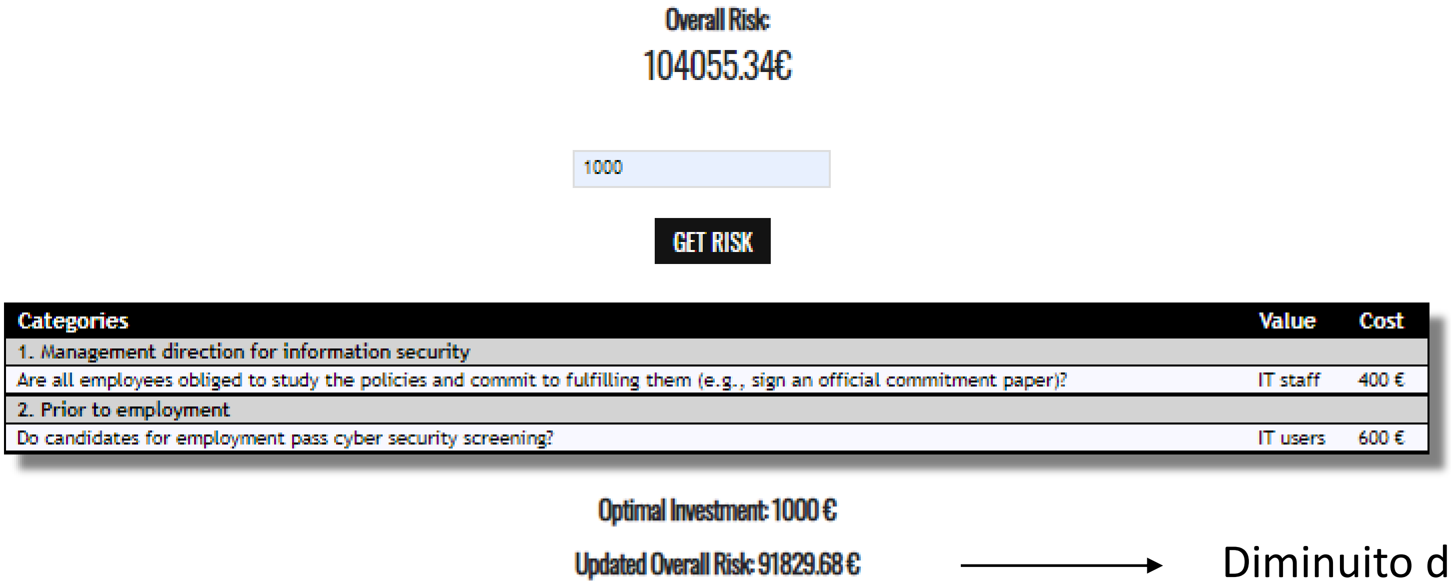


Questions	Answers	Cost
Are policies for information security approved by management?	Yes	2000
Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	IT security Staff	200
Are all external parties obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	Yes	2000
How often are the policies reviewed?	once in half a year	1200
Are responsibilities for information security defined and allocated?	Yes	2000
Are conflicting, potentially risky, highly important duties identified?	Yes	2000
Do only the devices compliant with or enforcing the organisation policies have access to the organisation's IT facilities?	Yes	2000
Are policies for information security defined for teleworking sites?	Yes	2000
Do candidates for employment pass cyber security screening?	IT staff	400
Does the organisation conduct any activities to explain, clarify (and, maybe, examine the knowledge of) information security policies and employee responsibilities?	Yes	2000
Have the organisation identified its information assets?	once in half a year	1200
Are the rules implemented with various policies, access control rules and security controls?	Yes	2000
Are all employees and external parties obliged to return organisational assets after termination of their	Yes	2000

- Sono le domande per identificare i controlli di sicurezza applicate

- Si puo modificare is costi

Resulto di ottimizazione. Con budget



Overall Risk:

104055.34€

1000

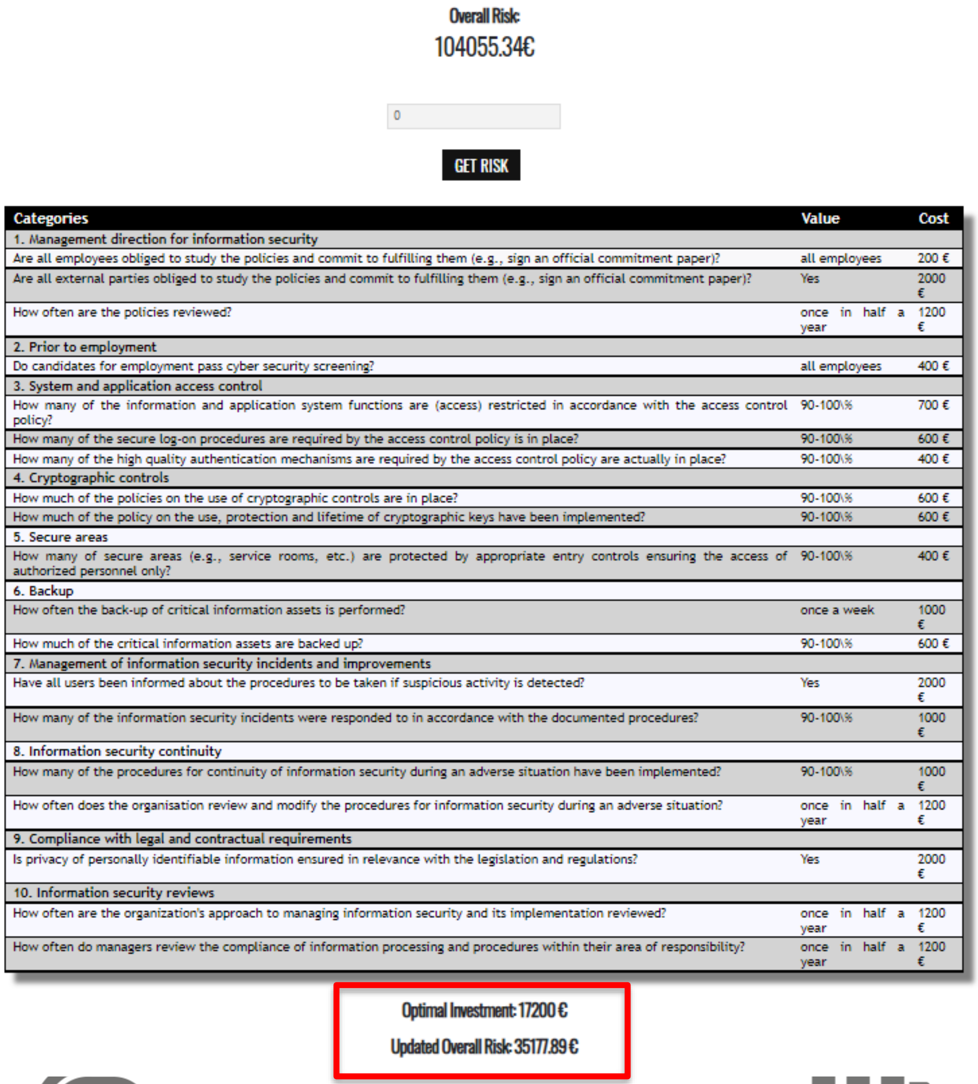
Categories	Value	Cost
1. Management direction for information security		
Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	IT staff	400 €
2. Prior to employment		
Do candidates for employment pass cyber security screening?	IT users	600 €

Optimal Investment: 1000 €

Updated Overall Risk: 91829.68 €

Diminuito dal 104055.34€ con il budget di 1000€

Resulto di ottimizazione. Senza budget



Overall Risk:

104055.34€

Categories	Value	Cost
1. Management direction for information security		
Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	all employees	200 €
Are all external parties obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?	Yes	2000 €
How often are the policies reviewed?	once in half a year	1200 €
2. Prior to employment		
Do candidates for employment pass cyber security screening?	all employees	400 €
3. System and application access control		
How many of the information and application system functions are (access) restricted in accordance with the access control policy?	90-100\%	700 €
How many of the secure log-on procedures are required by the access control policy is in place?	90-100\%	600 €
How many of the high quality authentication mechanisms are required by the access control policy are actually in place?	90-100\%	400 €
4. Cryptographic controls		
How much of the policies on the use of cryptographic controls are in place?	90-100\%	600 €
How much of the policy on the use, protection and lifetime of cryptographic keys have been implemented?	90-100\%	600 €
5. Secure areas		
How many of secure areas (e.g., service rooms, etc.) are protected by appropriate entry controls ensuring the access of authorized personnel only?	90-100\%	400 €
6. Backup		
How often the back-up of critical information assets is performed?	once a week	1000 €
How much of the critical information assets are backed up?	90-100\%	600 €
7. Management of information security incidents and improvements		
Have all users been informed about the procedures to be taken if suspicious activity is detected?	Yes	2000 €
How many of the information security incidents were responded to in accordance with the documented procedures?	90-100\%	1000 €
8. Information security continuity		
How many of the procedures for continuity of information security during an adverse situation have been implemented?	90-100\%	1000 €
How often does the organisation review and modify the procedures for information security during an adverse situation?	once in half a year	1200 €
9. Compliance with legal and contractual requirements		
Is privacy of personally identifiable information ensured in relevance with the legislation and regulations?	Yes	2000 €
10. Information security reviews		
How often are the organization's approach to managing information security and its implementation reviewed?	once in half a year	1200 €
How often do managers review the compliance of information processing and procedures within their area of responsibility?	once in half a year	1200 €

Optimal Investment: 17200 €

Updated Overall Risk: 35177.89 €

Con un investimento di 17,200 euro
Riduciamo il rischi fino a 35,177 euro

In totale: 52,377 < 91,829 < 104,055

Thanks

- This work is partially supported by EU projects:

MEDINA https://medina-project.eu/

SPARTA https://www.sparta.eu/

zit

IKT
horizontalna
mreža

DRIVING
DIGITAL
SLOVENIA.

ikthm.gzs.si
ai4si.gzs.si
smartsociety.gzs.si
www.gzs.si/zit
dihslovenia.si

Varnost v dobavnih verigah

mag. Aleš Černivec (ales.cernivec@xlab.si)

Ljubljana, 21.09.2021

Gospodarska zbornica Slovenije
zit Združenje za informatiko in telekomunikacije
REPUBLIKA SLOVENIJA MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
EVROPSKA UNIJA EVROPSKI SKLAD ZA REGIONALNI RAZVOJ NALOŽBA V VAŠO PRIHODNOST
SRIP Pametna mesta in skupnosti
DIGITALNO INOVACIJSKO STIČIŠČE SLOVENIJE

"Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj".

Agenda

- Kratka predstavitev XLAB
- Varnost v dobavnih verigah
- Rešitve
- Raziskave in razvoj

XLAB Products & Research

islonline

Enterprise
Remote
Desktop

XLAB Steampunk

Integrations into
Red Hat Ansible
Automation

Gaea+

3D GIS &
Vizualization

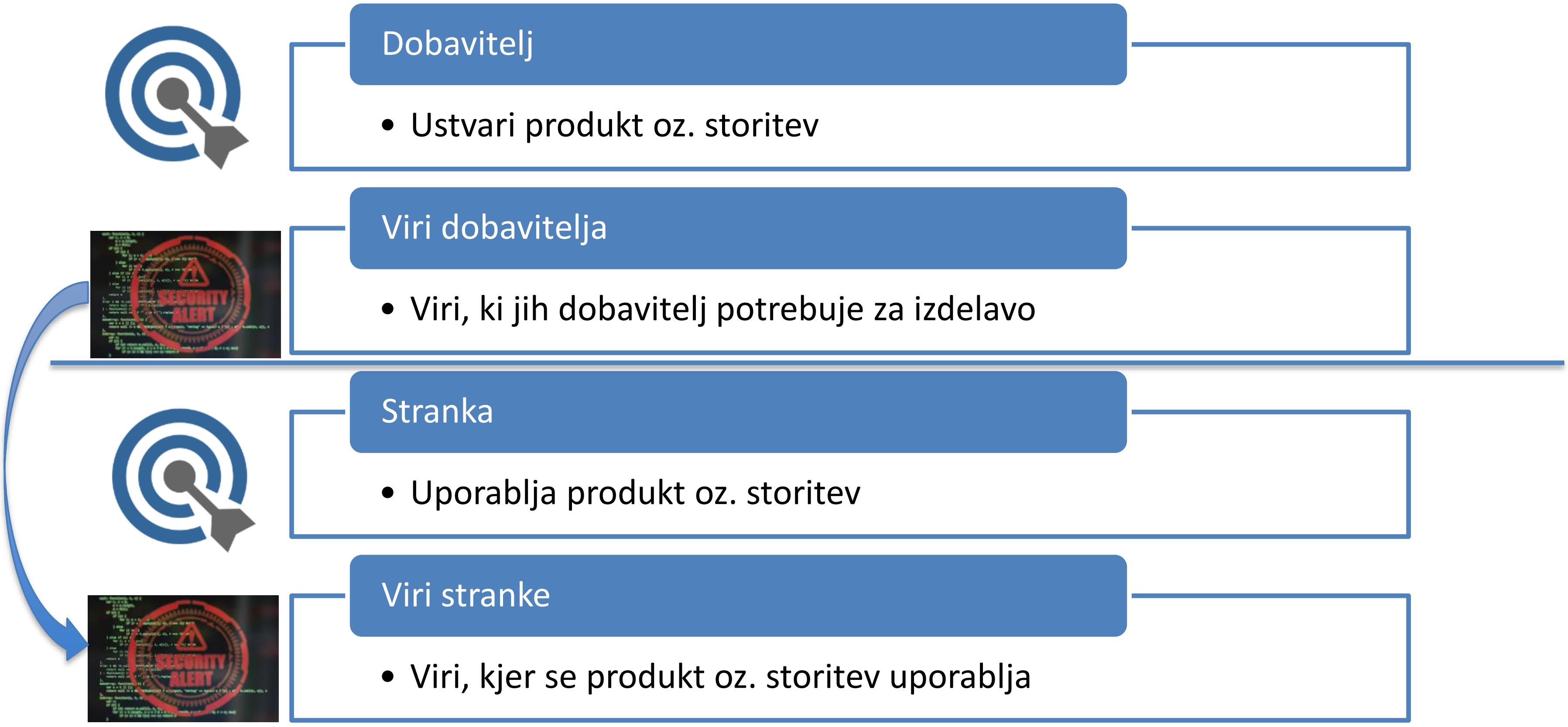
XLAB MEDICAL

3D Medical
Imaging

Research department

Among largest Slovenian private research groups.
50+ EU research projects.

Kaj je napad na dobavno verigo?



Dobavitelj

- Ustvari produkt oz. storitev

Viri dobavitelja

- Viri, ki jih dobavitelj potrebuje za izdelavo

Stranka

- Uporablja produkt oz. storitev

Viri stranke

- Viri, kjer se produkt oz. storitev uporablja

Vir: ENISA [1]

Taksonomija

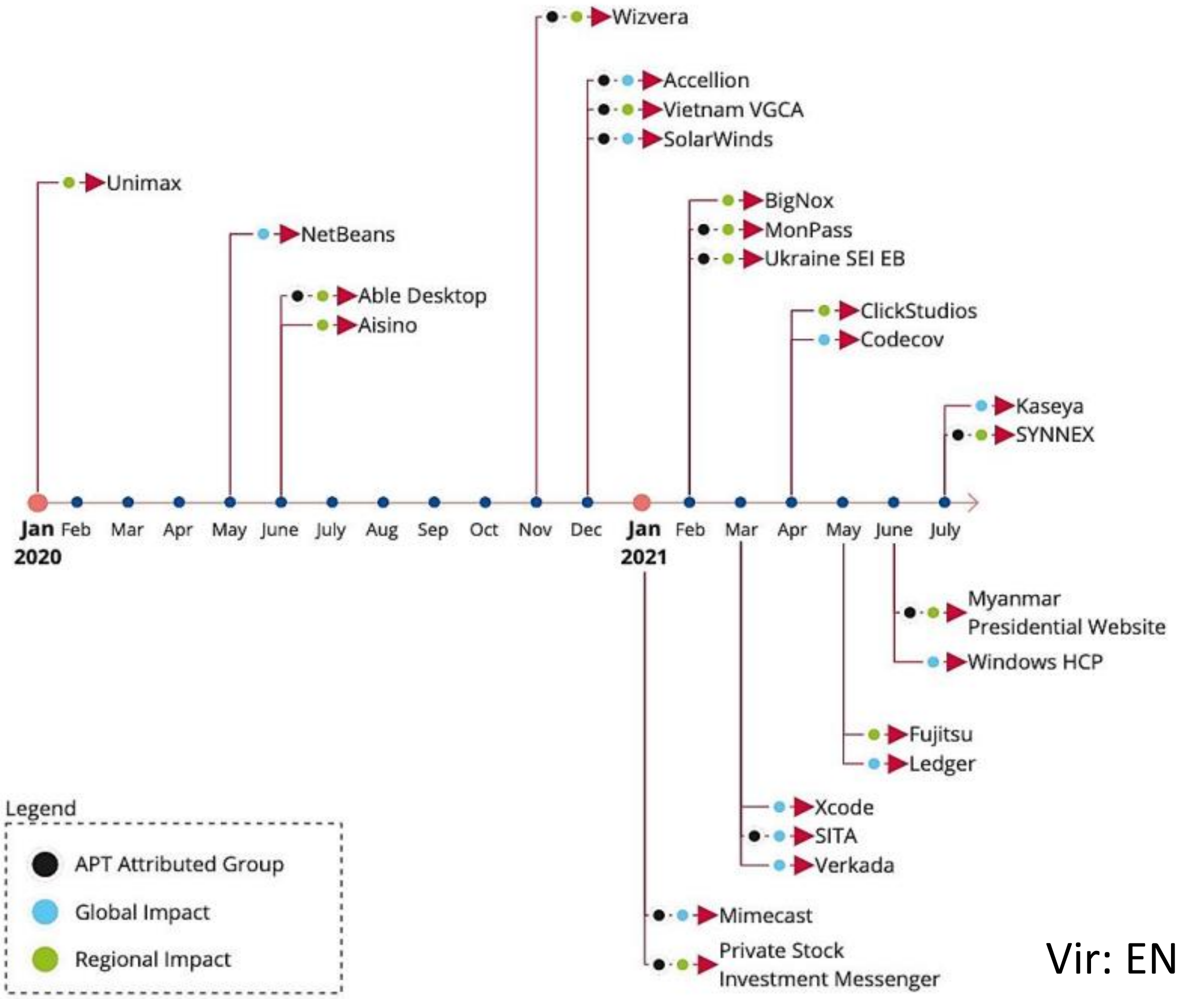
Dobavitelj

Tip napada	Vir napada
Zlonamerna koda	Programska oprema
Socialno inženirstvo	Programske knjižnice
Izkoriščanje ranljivosti programske opreme	Nastavitve
OSINT	Podatki
	Zaposleni

Stranka

Tip napada	Tarča napada
Zaupanje	(osebni) podatki
Ribarjenje	Intelektualna lastnina
Okužba z zlonamerno kodo	Programska oprema
	Procesi

Primeri napadov



Vir: ENISA [1]

Varnost v dobavnih verigah

- Dobavne verige so lahko velike, raznolike in kompleksne
- Pregled nad varnostjo dobaviteljev je težaven
- Zlonamerna koda je največkrat uporabljena tehnika napada (62% delež napadov; vir: ENISA, julij 2021), socialno inženirstvo, „brute-force“ napadi, zloraba ranljivosti v programski opremi

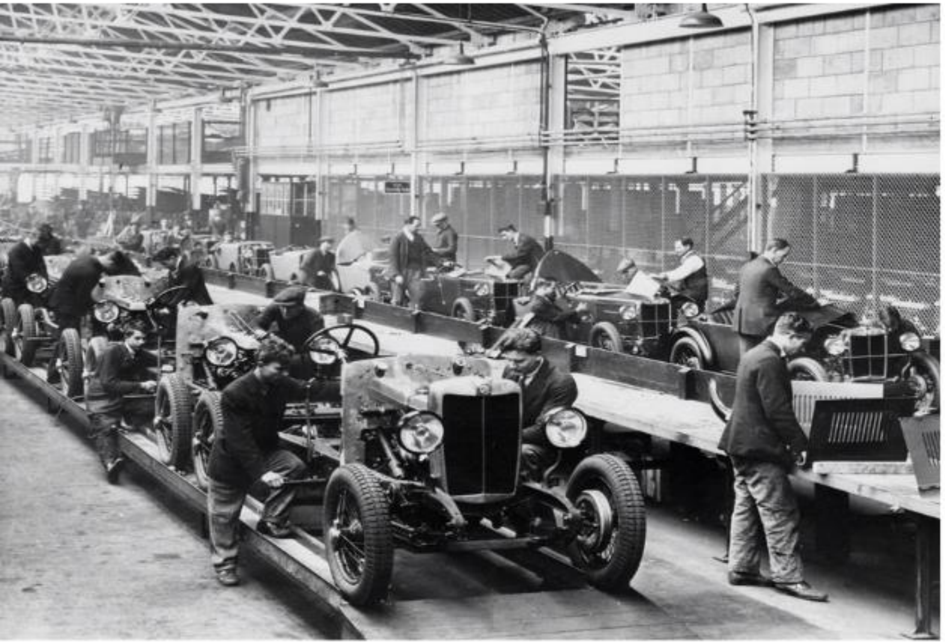
Kako nasloviti težave?

- Podpora certifikaciji (zagotavljanje skladnosti s standardi, npr. ISO/IEC 27001, SOC1/SOC2, PCI-DSS, CSA STAR, HIPPA, EUCS)
- (Tehnična) rešitev za izmenjavo podatkov glede izpolnjevanja varnostnih zahtev med deležniki

- XLAB naslavlja te težave v okviru
  - internih procesov
  - rešitve in produkti
  - raziskav in razvoja

Rešitve

What about the fear of losing jobs to Automation ?



" Gartner says **by 2025**, **>90%** of enterprises will have an automation architect, **<20%** today. "

Produkti

XLAB Steampunk

- Steampunk in razvoj Ansible Collections [4]
  - Podpora digitalni transformaciji poslovnih procesov
  - Avtomatizacija procesov z uporabo Ansible (npr. cloud automation)
  - Razvoj preverjenih standardiziranih zbirk - Enterprise Ansible Collections

Raziskave in razvoj

Raziskave in razvoj

MEDINA (H2020) - 1. 11. 2020 - 31. 10. 2023

– https://medina-project.eu/
– https://www.xlab.si/research/medina/
– Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

MEDINA

FISHY (H2020) - 01. 09. 2020 - 31. 08. 2023

– https://fishy-project.eu/
– https://www.xlab.si/research/fishy/
– A framework for (cyber) resilient supply chain systems

FiSHY

MEDINA

Standardizacija in izkazovanje skladnosti

tecnalia Inspiring Business

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft

Fraunhofer FOKUS

nixu cybersecurity.

Hewlett Packard Enterprise

XLAB

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

MEDINA

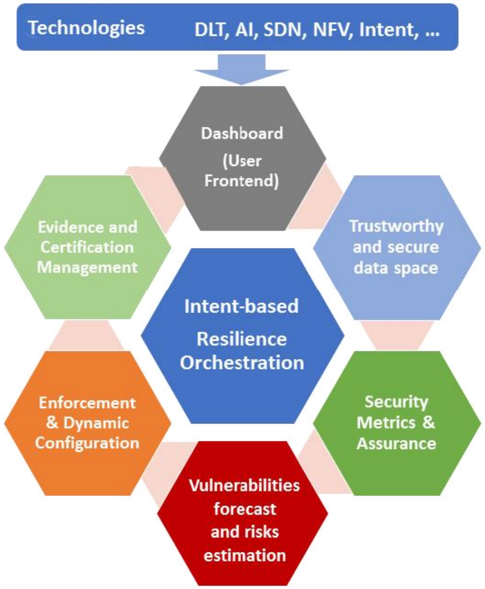
MEDINA - Aktivni nadzor varnosti

Podpora certifikaciji s “samodejnimi in rednimi” presojami [2]

- Detekcija ranljivosti z vgrajenimi skenerji
- Definicija poljubnih testov za:
  - nadzor nad pravilnim delovanjem in dosegljivostjo storitev
  - podporo spremljanja sprememb sistemov (oz. mreže)
- Možnost integracije z obstoječimi sistemi SIEM
- Preslikava stanja (dogodkov) v stanje skladnosti z zahtevami oz. kontrolami standarda

FISHY

Ogrodje za zagotavljanje kibernetske odpornosti v dobavnih verigah [3] (angl. A coordinated framework for cyber resilient supply chain systems)



Technologies DLT, AI, SDN, NFV, Intent, …

Dashboard (User Frontend)

Trustworthy and secure data space

Security Metrics & Assurance

Vulnerabilities forecast and risks estimation

Enforcement & Dynamic Configuration

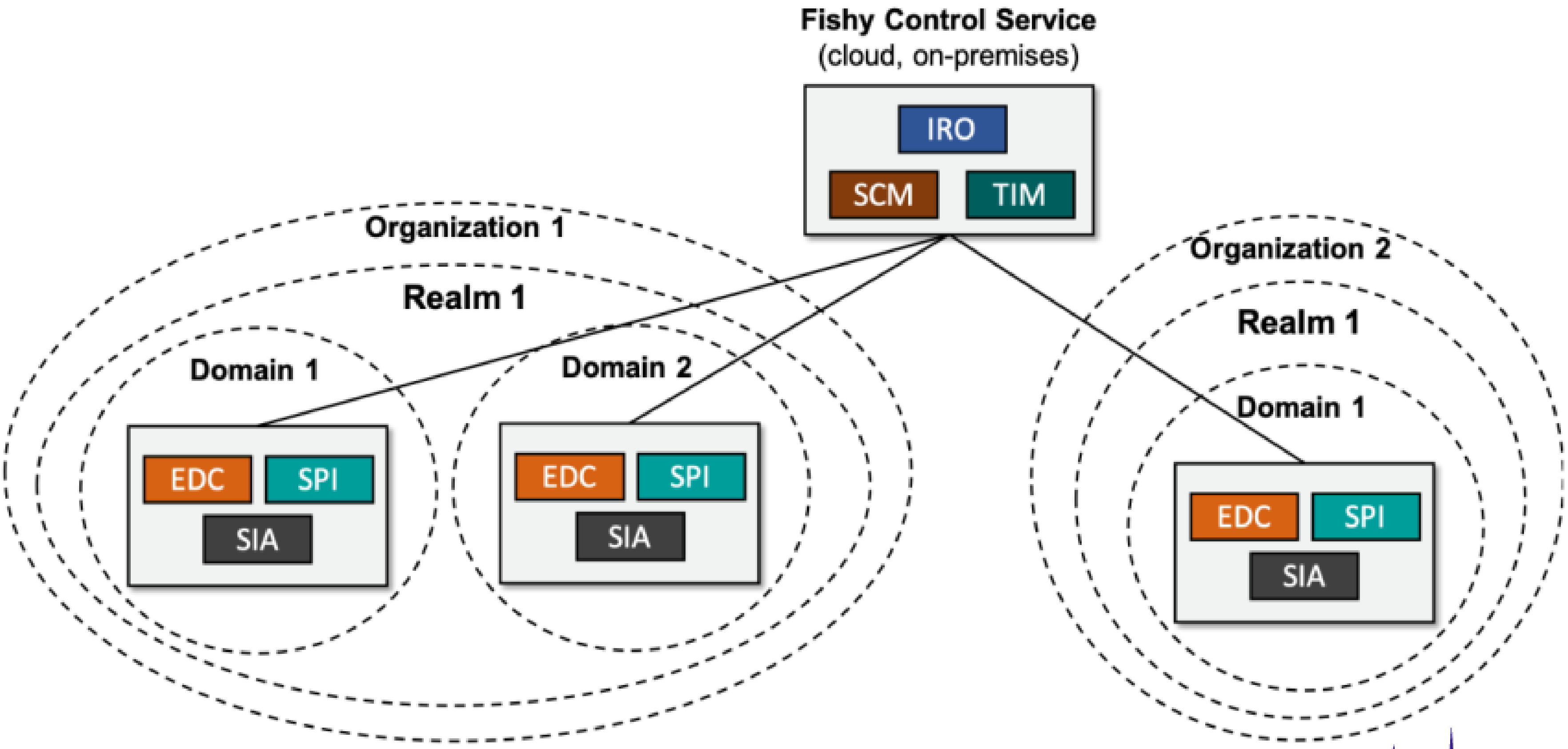
Evidence and Certification Management

Intent-based Resilience Orchestration

Atos
Synelixis
XLAB
Politecnico di Torino
Telefónica
Universitat Politècnica de Catalunya BarcelonaTech
Technische Universität Braunschweig
optimum
Sonae Arauco Taking wood further
Altran Part of Capgemini
Sphynx Technology Solutions
Universidade do Minho

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 952644.

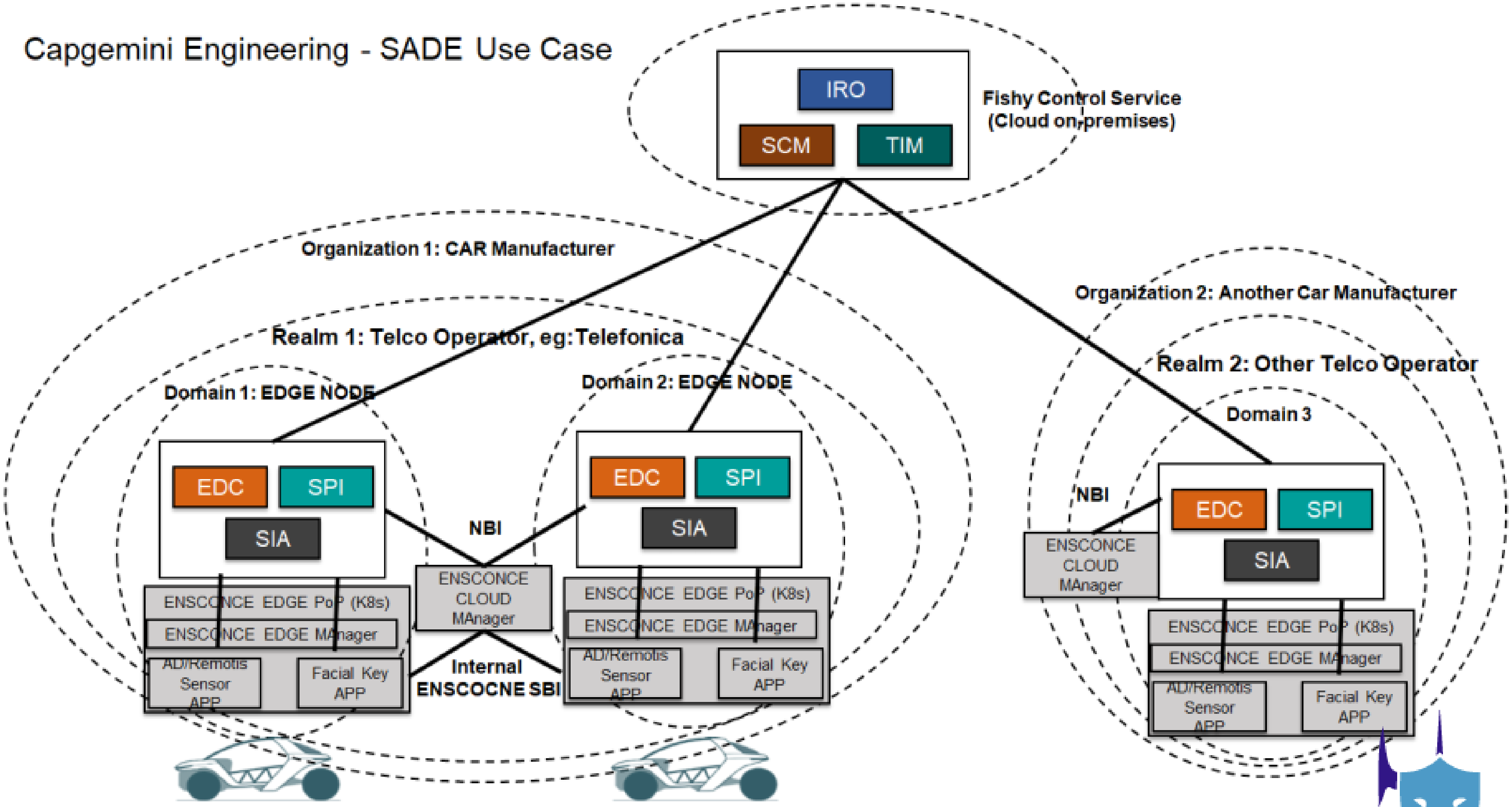
FISHY



Organization: company, consortium, law enforcement, etc.
Realm: environment from cybersecurity perspective, with same policies, rules, etc.
Domain: group of assets with certain relationship (same network, infrastructure, location, etc.)

FISHY – primer uporabe

Capgemini Engineering - SADE Use Case



Povzetek

- Varnost v dobavnih verigah – osnovni pojmi
- Kako nasloviti težave varnosti
- Rešitve

- Hvala!

Viri

1) Threat Landscape for Supply Chain Attacks - https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
2) MEDINA project https://medina-project.eu/
3) FISHY project https://fishy-project.eu/
4) Smarter Automation with Enterprise Ansible Collections https://steampunk.si/

APPENDIX B: Material for the preparation of the training videos

This Appendix contains the slides of the presentations which have been used in the preparation of the MEDINA Training videos depicted in Table 2.

- **Overview of the MEDINA Framework** (Bosch)
- **MEDINA Integrated UI** (Bosch)
- **EUCS Automation with MEDINA - An IoT Cloud Use Case** (Bosch)
- **Company Compliance Dashboard. A continuous audit of SaaS solutions Use Case** (Fabasoft)
- **Are you ready for European Cloud Service Security Certification?** (NIXU)
- **MEDINA Training: MEDINA Architecture** (TECNALIA)
- **MEDINA Training: Installation of the MEDINA Framework** (HPE)
- **MEDINA Training: Catalogue of Controls and Metrics** (TECNALIA)
- **MEDINA Training: Customization of Requirements** (CNR, HPE)
- **MEDINA Training: Risk Assessment** (CNR)
- **MEDINA Training: Clouditor components** (FhG)
- **MEDINA Training: Assessment and Management of Organizational Evidence** (AMOE) (Fabasoft)
- **MEDINA Training: Codyze** (FhG)
- **MEDINA Training: Wazuh and VAT Evidence Collection** (XLAB)
- **MEDINA Training: Integrity Validation of Evidence** (TECNALIA)
- **MEDINA Training: Continuous Life-Cycle Management of Cloud Security Certifications** (XLAB, FhG, CNR)
- **MEDINA Training: Credentials and Proofs of certificates** (TECNALIA)

MEDINA

Overview of the MEDINA Framework

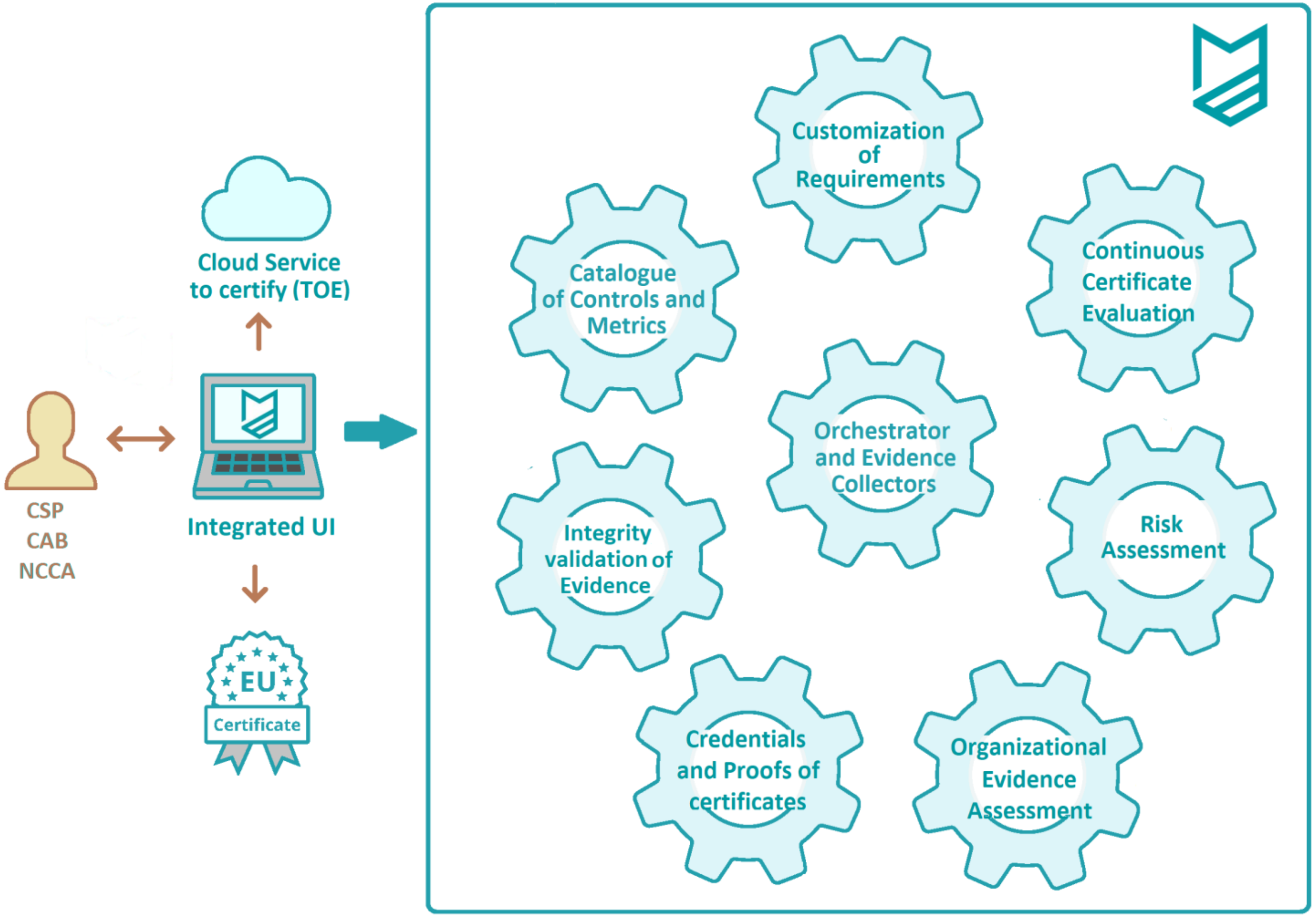
Jesus Luna Garcia, Bosch

October 2023

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

Chapters

- EUCS Background
- H2020 MEDINA
- Framework At a Glance
- Further information

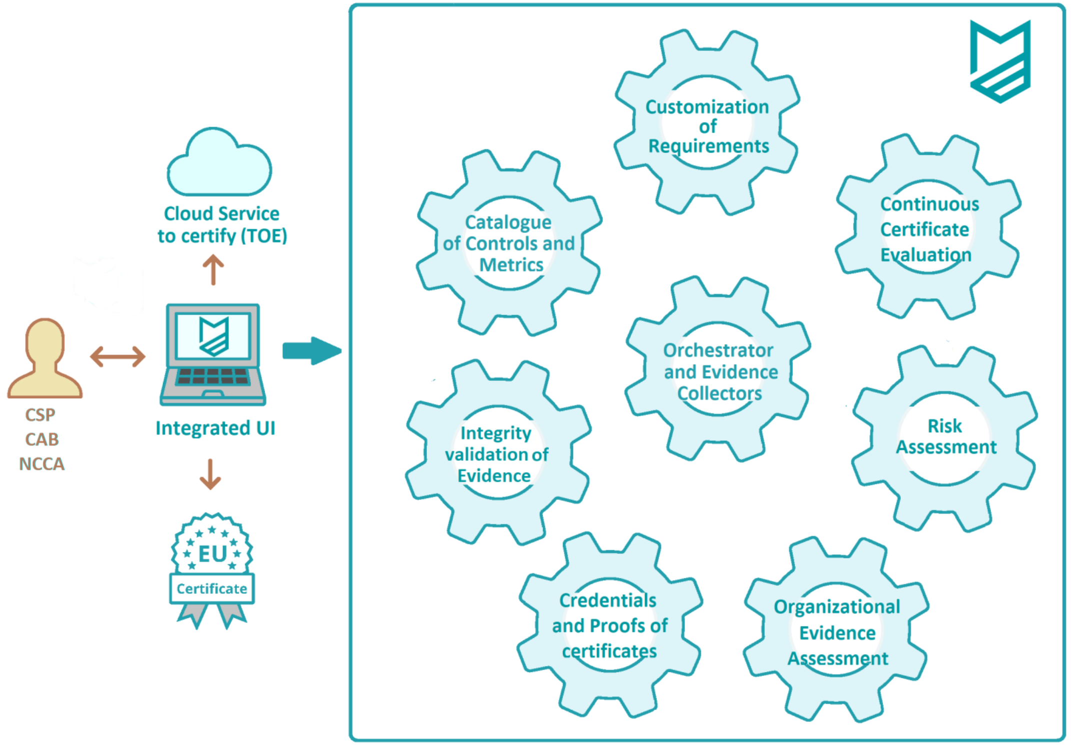


CSP
CAB
NCCA
Cloud Service to certify (TOE)
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Overview of the MEDINA Framework

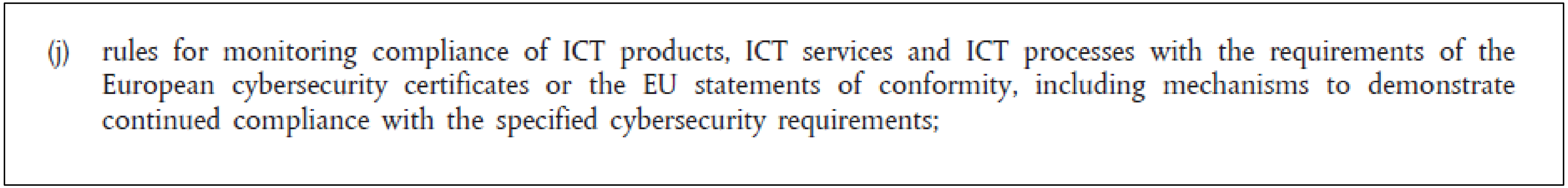
- ➤ EUCS Background

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

What is an EU-cybersecurity certification?

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation of cybersecurity certification schemes which include the notions of:
  - Levels of assurance (***Basic, Substantial, High***)
  - ***Continuous cybersecurity compliance (Art. 54(j))***



(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

- Three EUCSA-derived certification schemes are under preparation by ENISA:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - **EUCS - Cybersecurity Certification Scheme for Cloud Services**
  - EU5G - Cybersecurity Certification Scheme for 5G

A Few Words About EUCS

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment reviewed by a third-party
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

‘high’ level

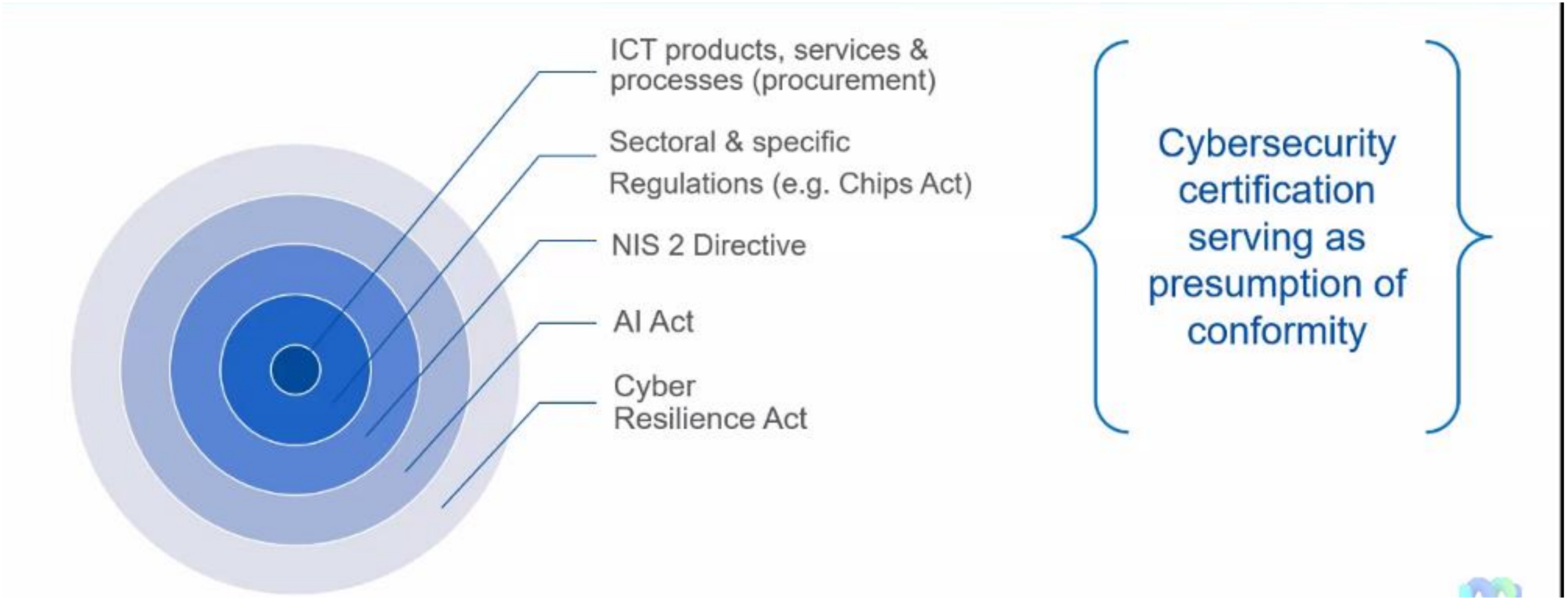
Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

CEN CENELEC is finalizing the standardization of the main EUCS specifications.
After EC approval, it is expected for EUCS to go-live during 2024

Cybersecurity Certification in the EU – the World to Come

- The notion of *EU-cybersecurity certification* is central in upcoming European regulations.



ICT products, services & processes (procurement)

Sectoral & specific Regulations (e.g. Chips Act)

NIS 2 Directive

AI Act

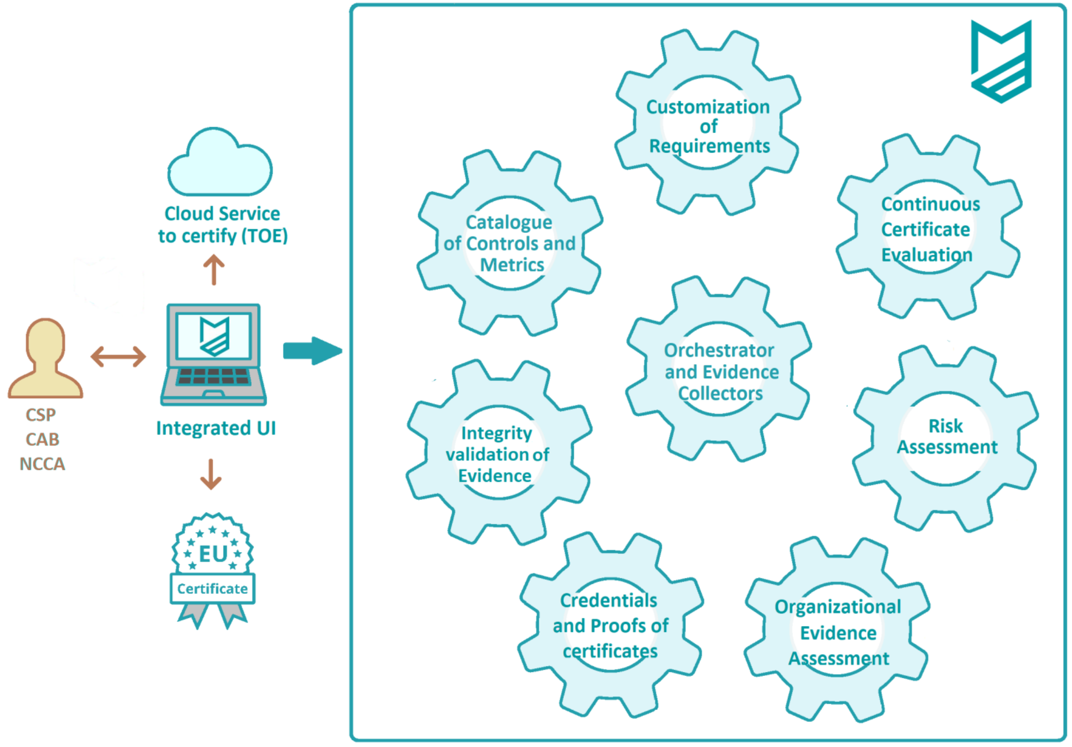
Cyber Resilience Act

Cybersecurity certification serving as presumption of conformity

Borrowed from ENISA's presentation during Cert WS (12.2022)

Overview of the MEDINA Framework

- H2020 MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

EU-funded MEDINA Project

- Goal: provide a security framework for achieving **continuous audit-based certification in EUCS**.
- MEDINA focuses on **automation, standardized metrics and trustworthy** evidence-management methods.
- **MEDINA can be extended** to other certification schemes (e.g., German BSI C5:2020, ISO/IEC 27001).

Continuous (Automated) Monitoring
Continuous Audit-based Certification
MEDINA

Who is who in MEDINA?

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€

Estonia
Latvia
Denmark
Lithuania
Belarus
Ireland
United Kingdom
Netherlands
Poland
Germany
Belgium
Luxembourg
Czechia
Slovakia
Ukraine
Liechtenstein
Austria
Hungary
Moldova
France
Switzerland
Slovenia
Romania
Croatia
Monaco
San Marino
Serbia
Andorra
Italy
Montenegro
Bulgaria
North Macedonia
Spain
Portugal
Albania
Greece
Malta

tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft®

Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Challenges and Approaches

MEDINA

Topic	MEDINA Approach
Automation of compliance assessments	• Automated cloud assessments based on machine-readable metrics • AI-supported security documentation assessment
Trustworthy evidence management	• Blockchain-based evidence vault • RBAC authorization model
Certificate management	• Risk-based automation of certificate life-cycle • Cryptographic verification of EUCS certificates
Standardization	• EUCS: CEN CENELEC EUCS1 • Metrics: ISO/IEC 27004, NIST SP 800-55rev2 • Automation: NIST OSCAL, ETSI CYBER

Expected MEDINA Benefits

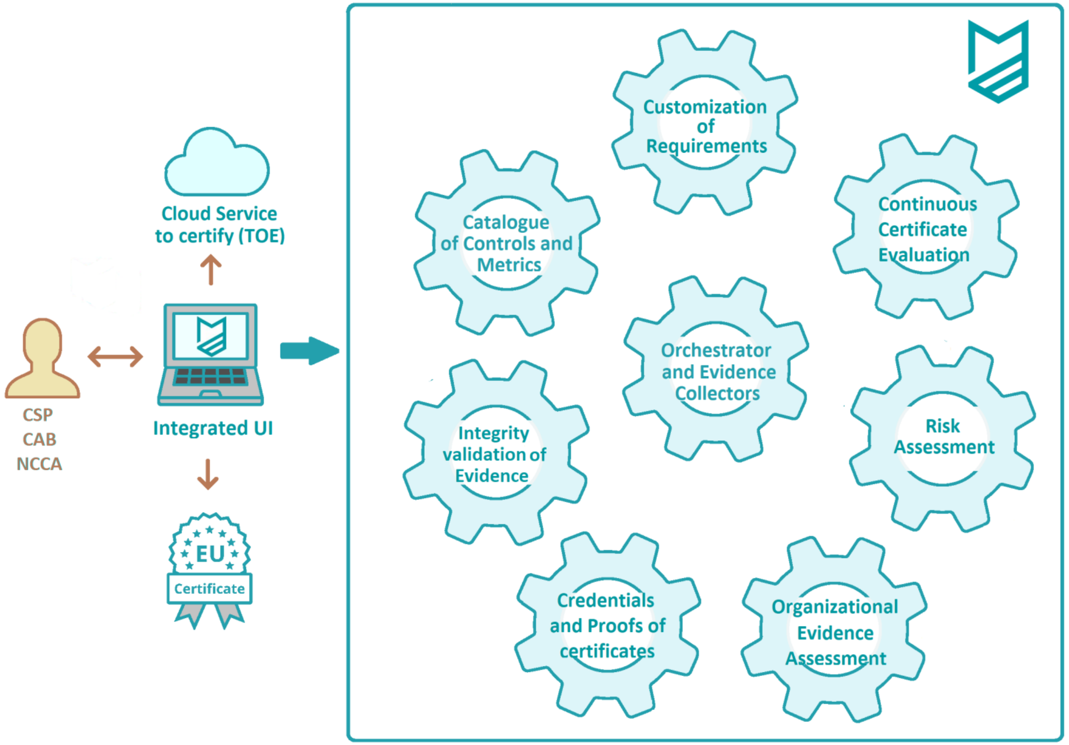
MEDINA

- **Guidance** for the implementation of EUCS requirements and automated compliance metrics
- Extensible **toolbox** for leveraging automated compliance assessments for IaaS, PaaS and SaaS
- **Trustworthy evidence** management in EUCS
- **Standardization and awareness** to pave the road for continuous certification (in particular with **Regulators** in the EU and US)

Overview of the MEDINA Framework

- Framework at a Glance

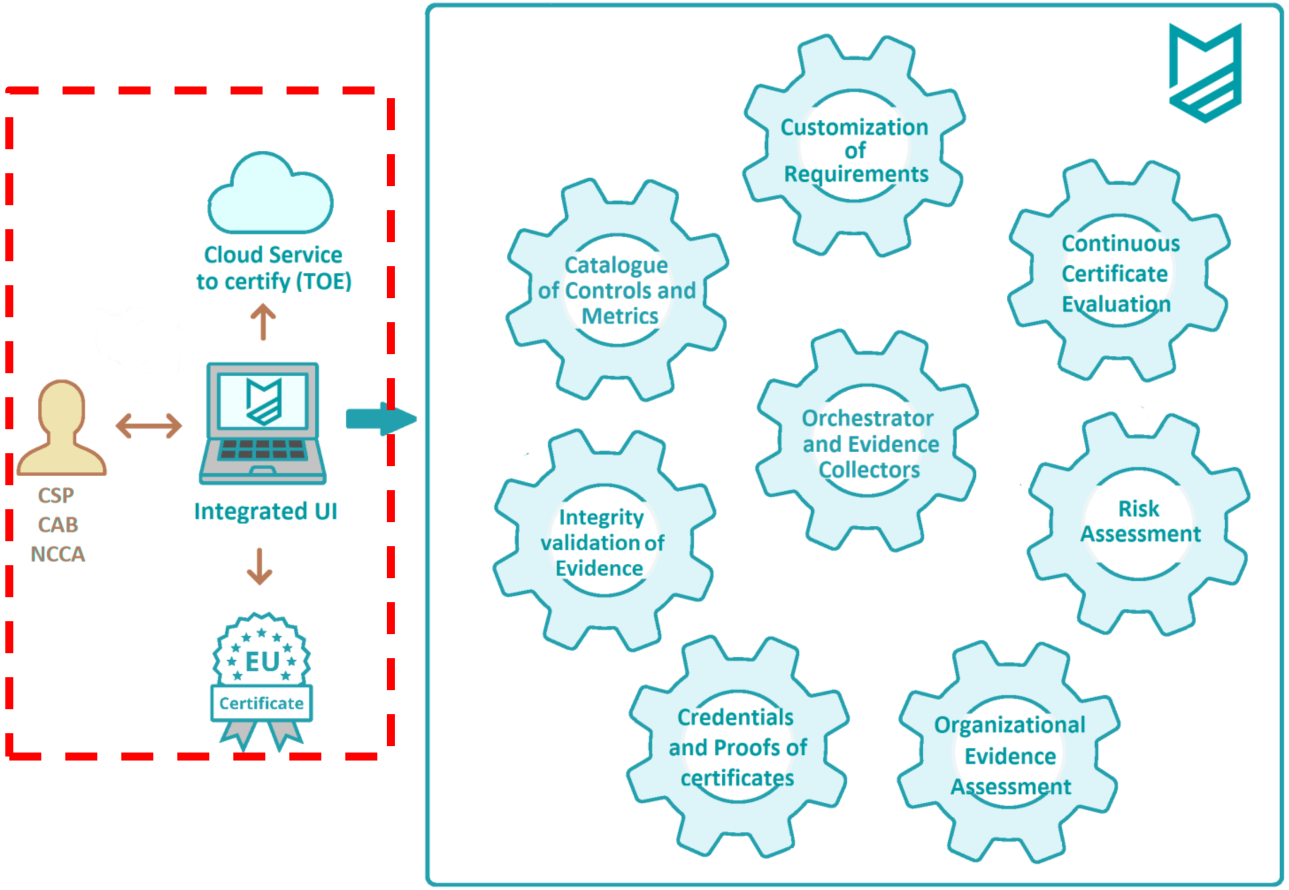
MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Framework At a Glance

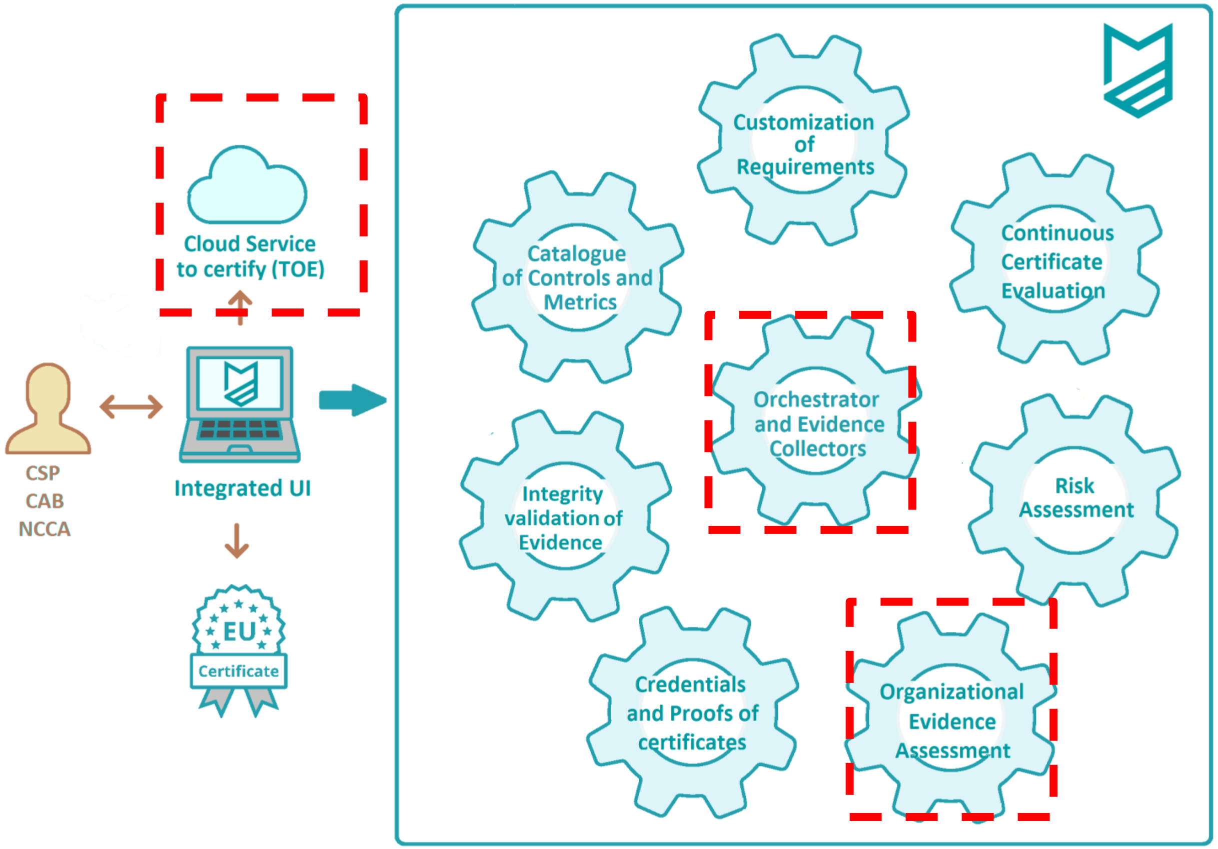
MEDINA

1. Stakeholders.
2. Orchestrator and Evidence Collectors.
3. Catalogue of Controls and Metrics.
4. Customization of Requirements.
5. Continuous Certificate Evaluation.
6. Risk Assessment.
7. Organizational Evidence Assessment.
8. Credentials and Proofs of Certificates.
9. Integrity Validation of Evidence.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

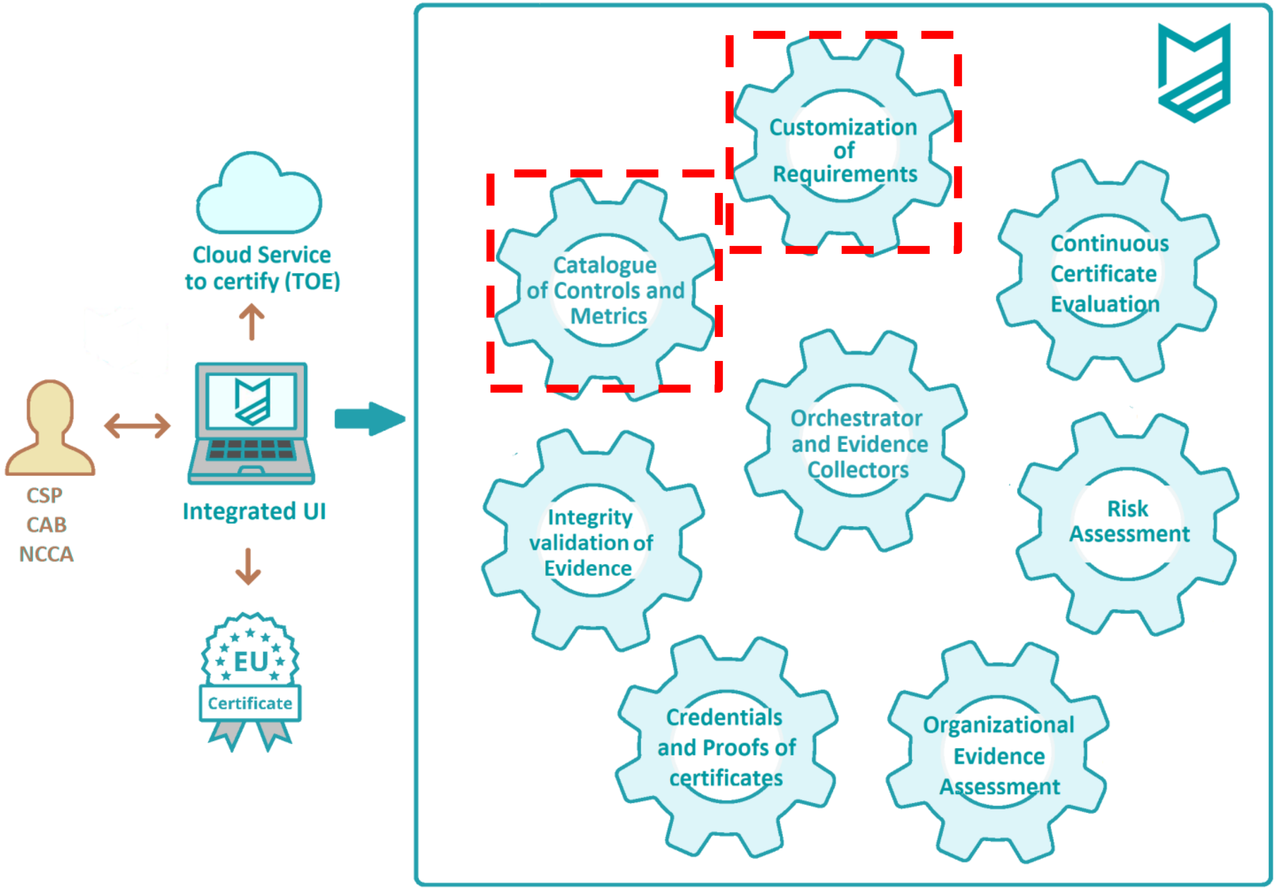
Framework At a Glance

1. Stakeholders.
2. Orchestrator and Evidence Collectors.
3. Catalogue of Controls and Metrics.
4. Customization of Requirements.
5. Continuous Certificate Evaluation.
6. Risk Assessment.
7. Organizational Evidence Assessment.
8. Credentials and Proofs of Certificates.
9. Integrity Validation of Evidence.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Framework At a Glance

1. Stakeholders.
2. Orchestrator and Evidence Collectors.
3. Catalogue of Controls and Metrics.
4. Customization of Requirements.
5. Continuous Certificate Evaluation.
6. Risk Assessment.
7. Organizational Evidence Assessment.
8. Credentials and Proofs of Certificates.
9. Integrity Validation of Evidence.

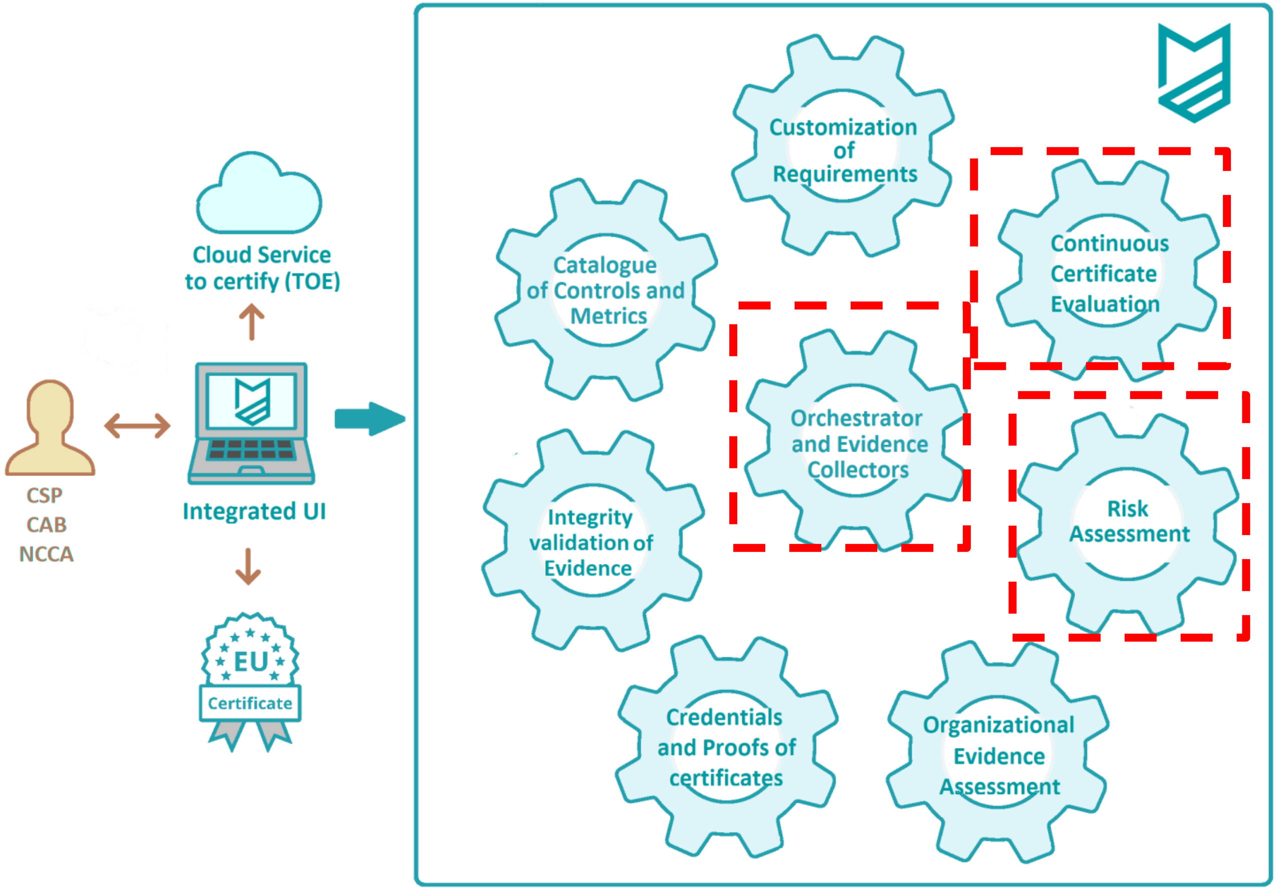


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Framework At a Glance

MEDINA

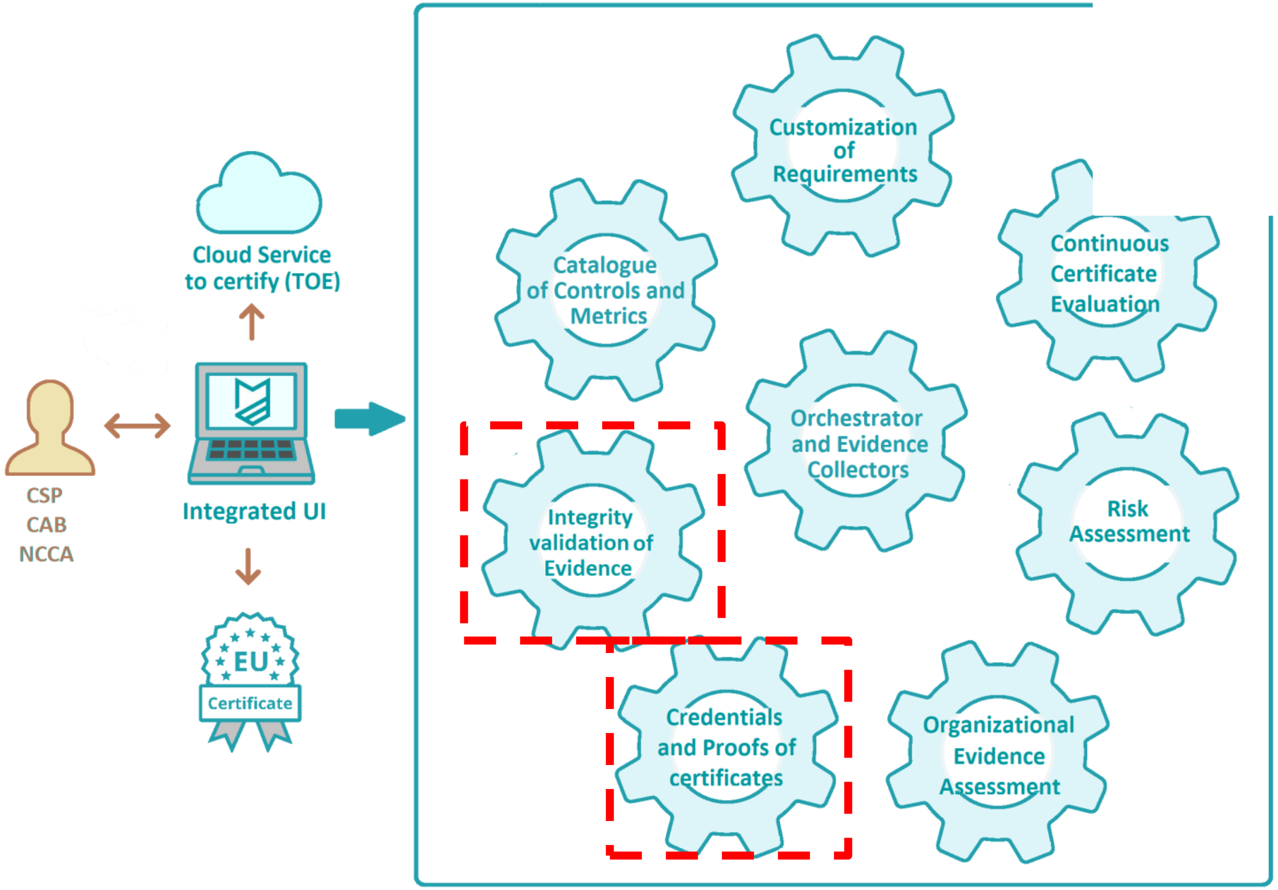
1. Stakeholders.
2. Orchestrator and Evidence Collectors.
3. Catalogue of Controls and Metrics.
4. Customization of Requirements.
5. Continuous Certificate Evaluation.
6. Risk Assessment.
7. Organizational Evidence Assessment.
8. Credentials and Proofs of Certificates.
9. Integrity Validation of Evidence.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Framework At a Glance

MEDINA

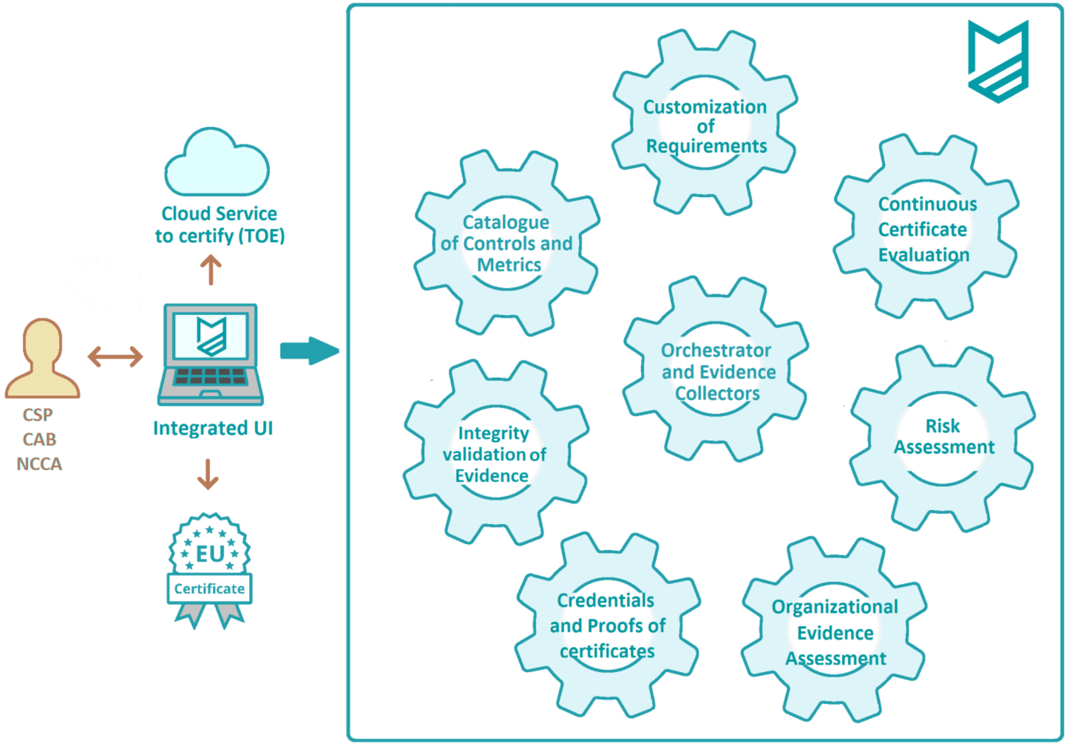
1. Stakeholders.
2. Orchestrator and Evidence Collectors.
3. Catalogue of Controls and Metrics.
4. Customization of Requirements.
5. Continuous Certificate Evaluation.
6. Risk Assessment.
7. Organizational Evidence Assessment.
8. Credentials and Proofs of Certificates.
9. Integrity Validation of Evidence.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Overview of the MEDINA Framework

- ➤ Further information

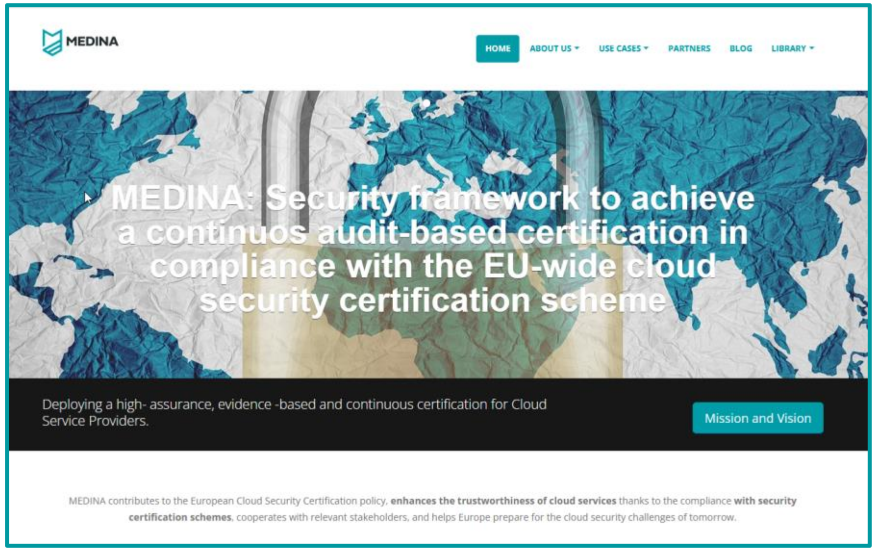
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft

XLAB

nixu cybersecurity.

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

MEDINA

Integrated UI

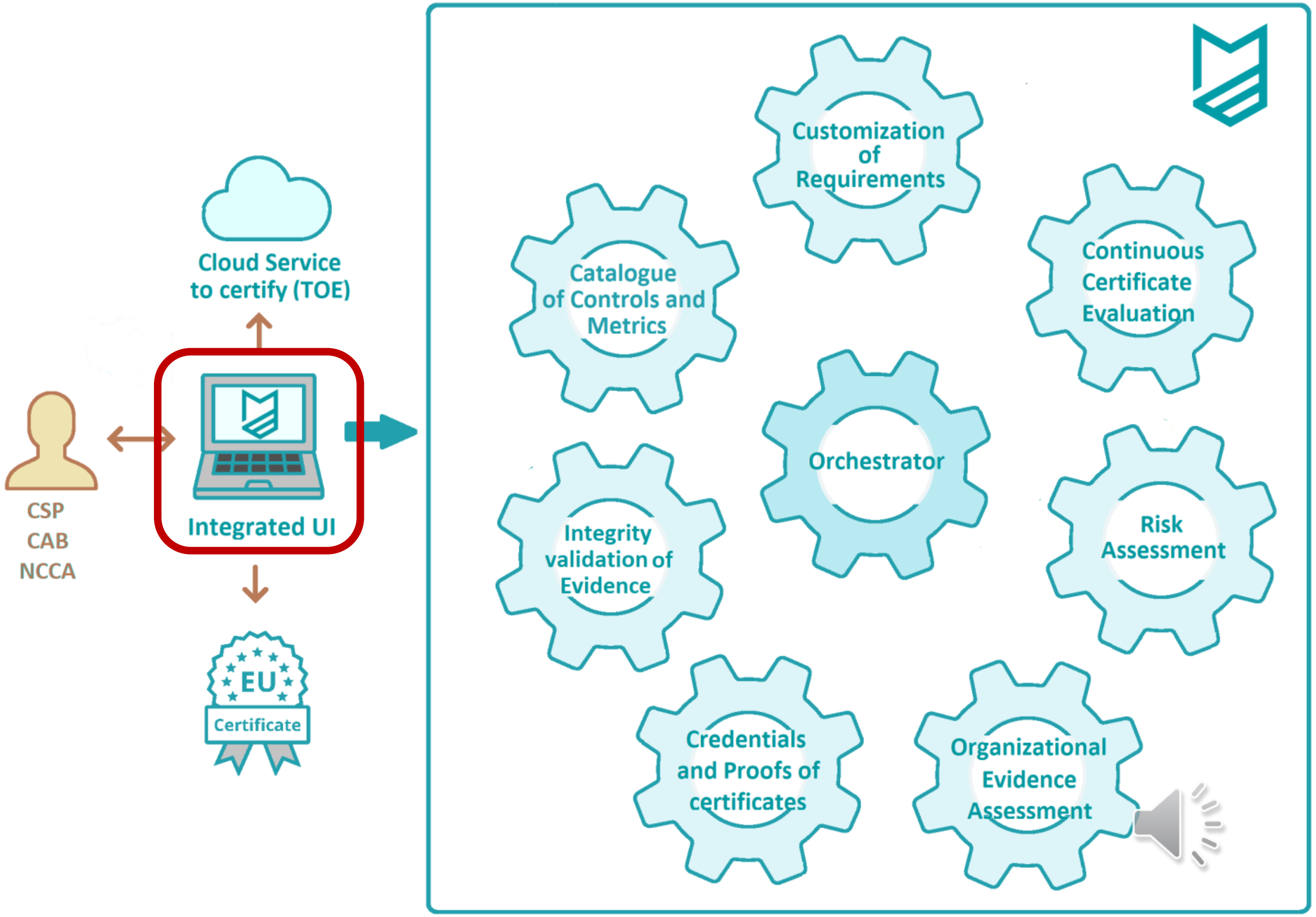
Jesus Luna Garcia, BOSCH

October 2023

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

Chapters

- Overview
- Set Up
- Work Flows
- Further information

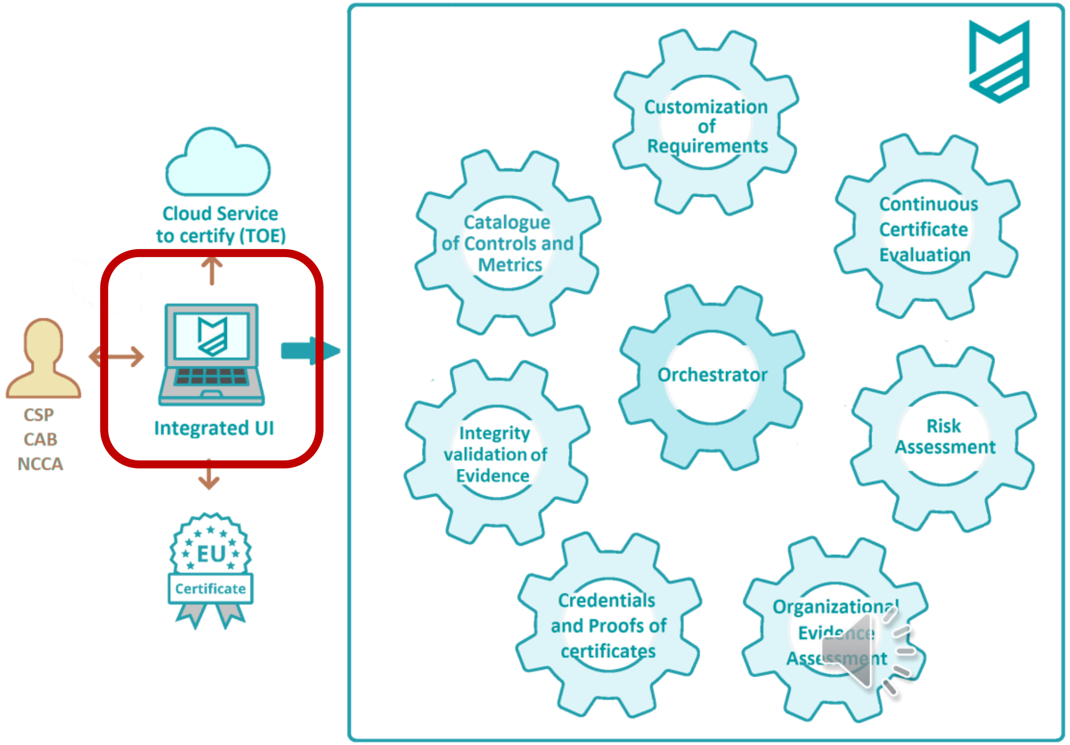


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Integrated UI

- ➤ Overview

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Integrated UI - Overview

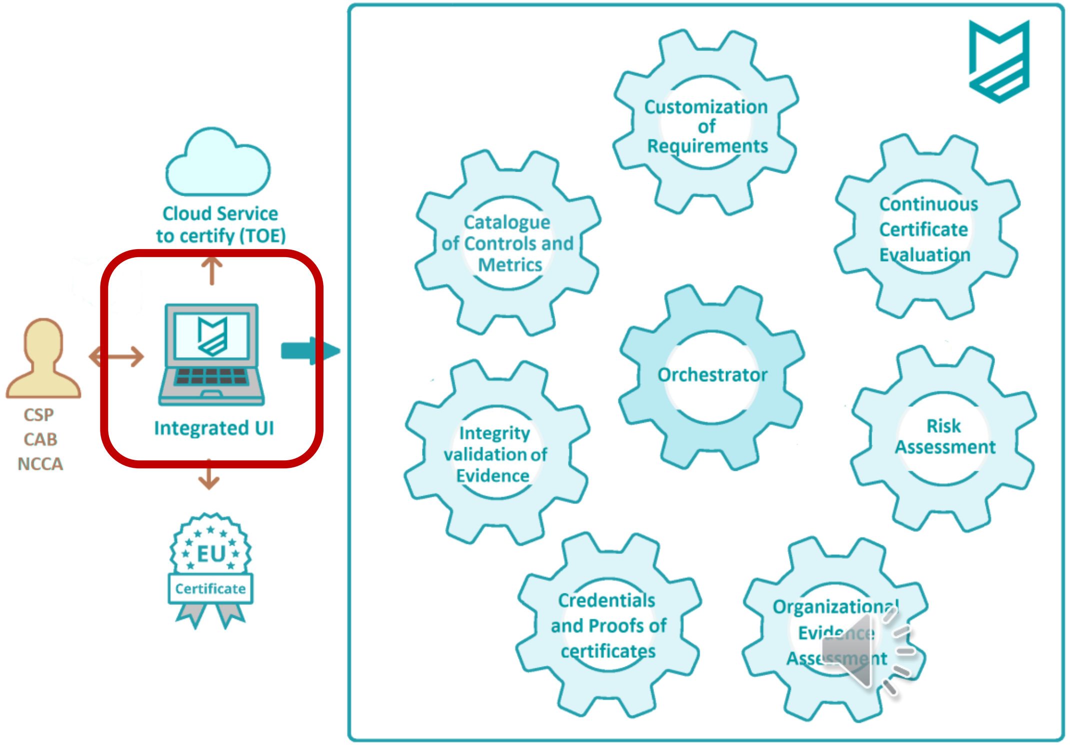
MEDINA

- User Story:
  - As an IT Security Governance responsible,
  - I want to have an up-to-date view on current misconfigurations that lead to non-compliances or certification issues in all Bosch cloud resources and their development over time,
  - so that I can identify common and/or frequently occurring issues and adjust my security controls framework accordingly.
- Benefits include EUCS preparedness, early identification of EUCS issues, and alignment of Bosch internal framework to EUCS.

Integrated UI

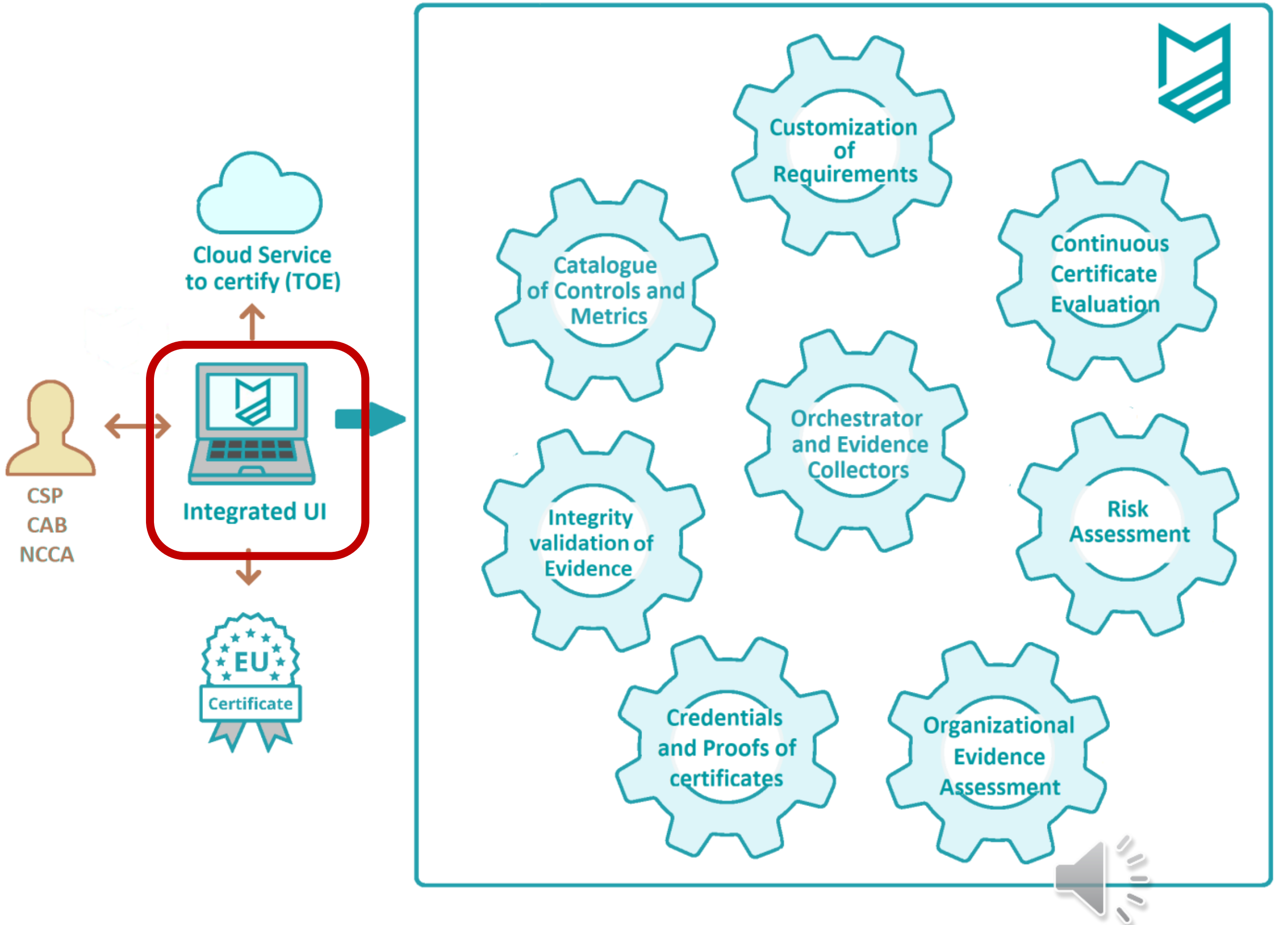
- Set Up

MEDINA


Customization of Requirements
Cloud Service to certify (TOE)
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
CSP
CAB
NCCA
Integrated UI
Orchestrator
Integrity validation of Evidence
Risk Assessment
EU
Certificate
Credentials and Proofs of certificates
Organizational Evidence Assessment

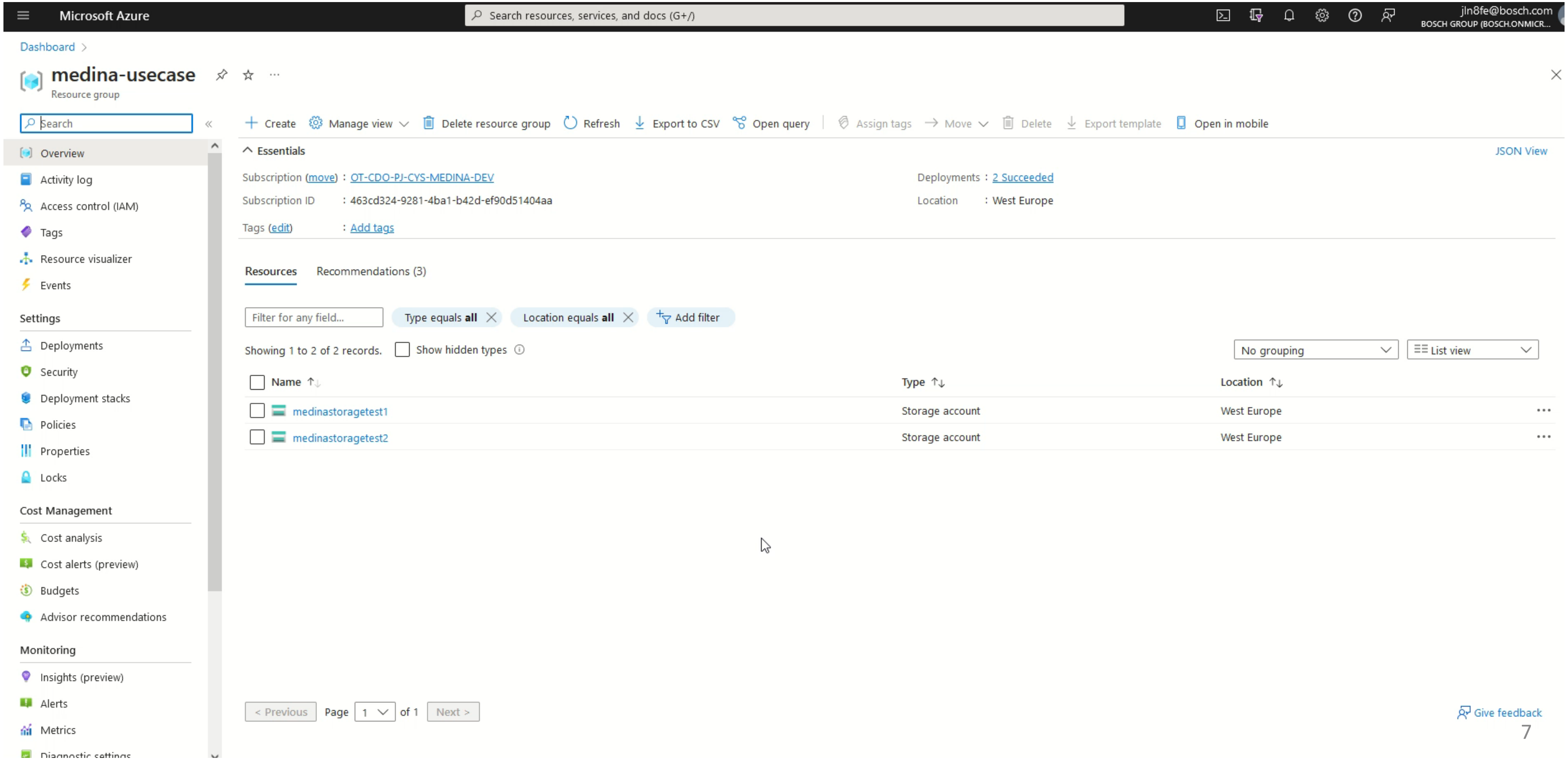
Integrated UI – Set Up

- Cloud Service deployed in Microsoft Azure with **two virtual storages**.
  - **One being non-compliant**
- **Clouditor** as evidence collector.
- **UC1_SecGov** as target user.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Integrated UI – Set Up

MEDINA



Microsoft Azure

Search resources, services, and docs (G+/)

jln8fe@bosch.com
BOSCH GROUP (BOSCH.ONMICR...

Dashboard >

medina-usecase

Resource group

Subscription (move)	: OT-CDO-PJ-CYS-MEDINA-DEV		Deployments	: 2 Succeeded
Subscription ID	: 463cd324-9281-4ba1-b42d-ef90d51404aa		Location	: West Europe
Tags (edit)	: Add tags			

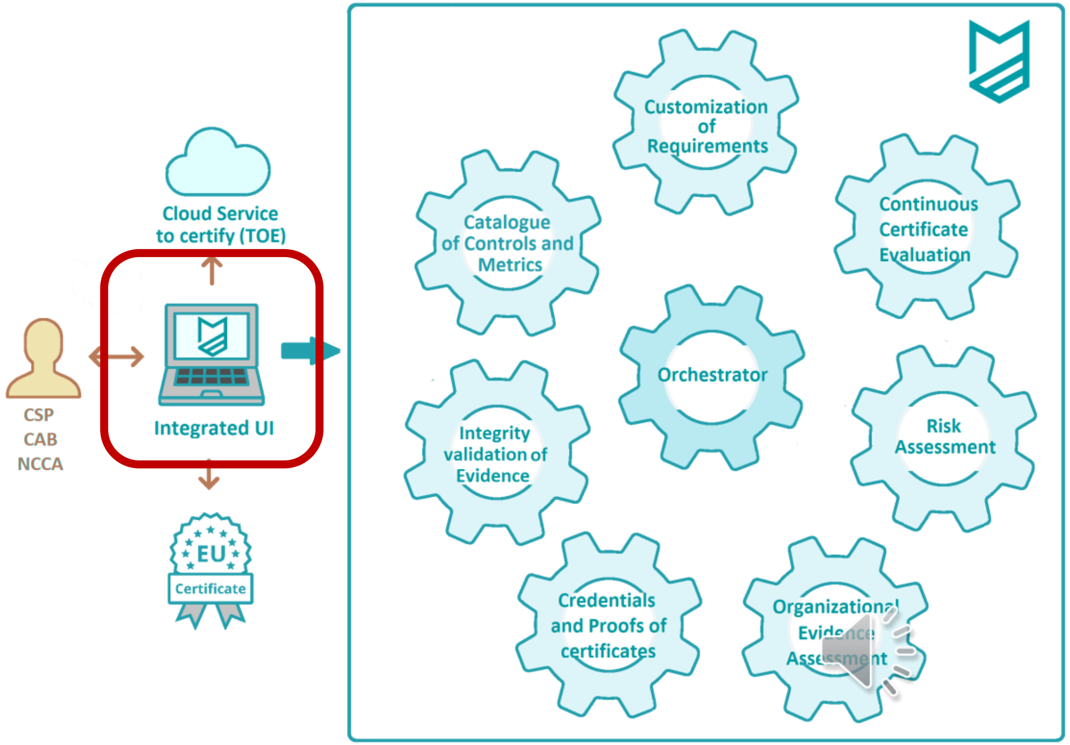
Showing 1 to 2 of 2 records.

□	Name	Type	Location
□	medinastoragetest1	Storage account	West Europe
□	medinastoragetest2	Storage account	West Europe

Integrated UI

- ➤ Work Flows

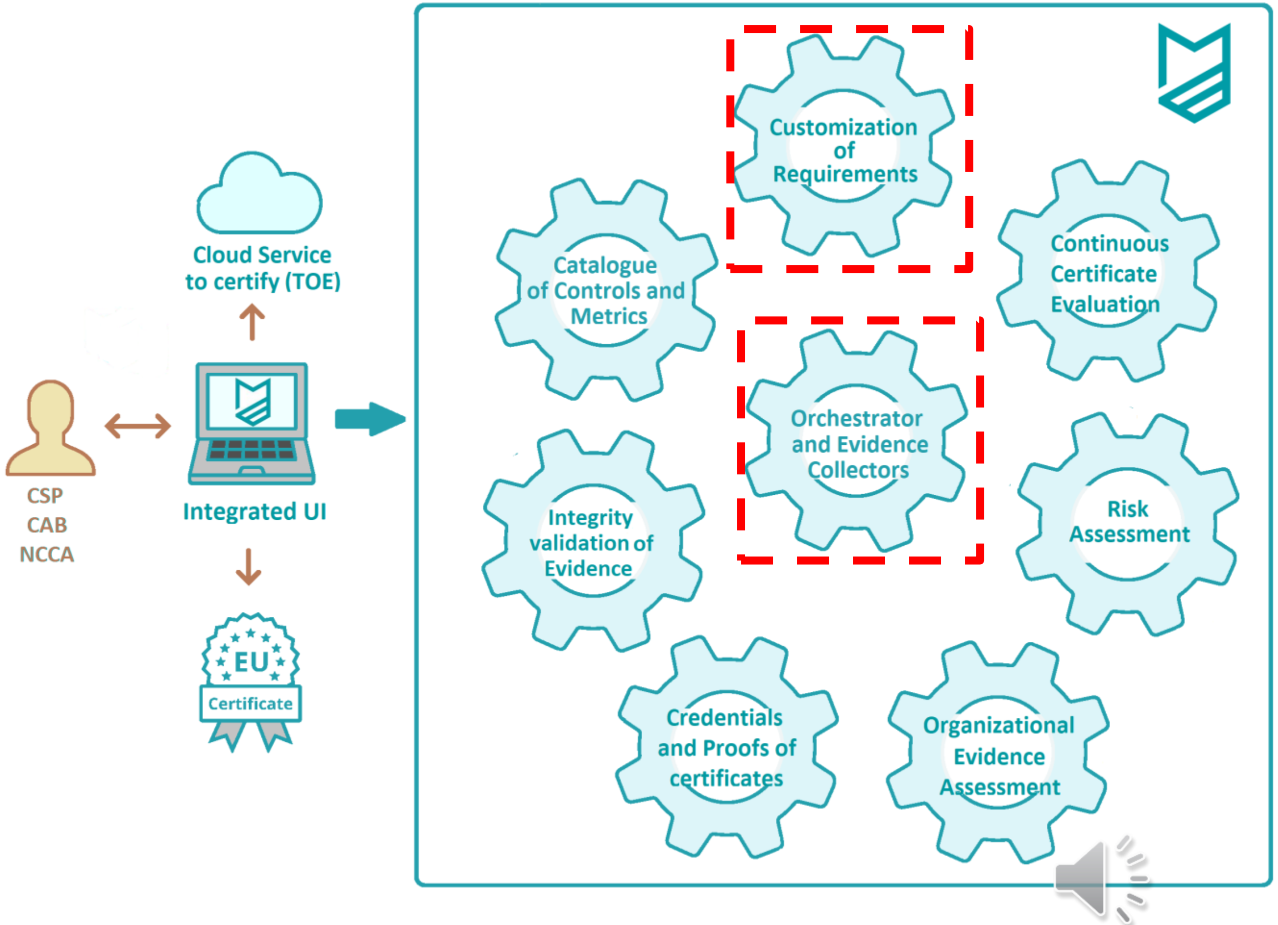
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

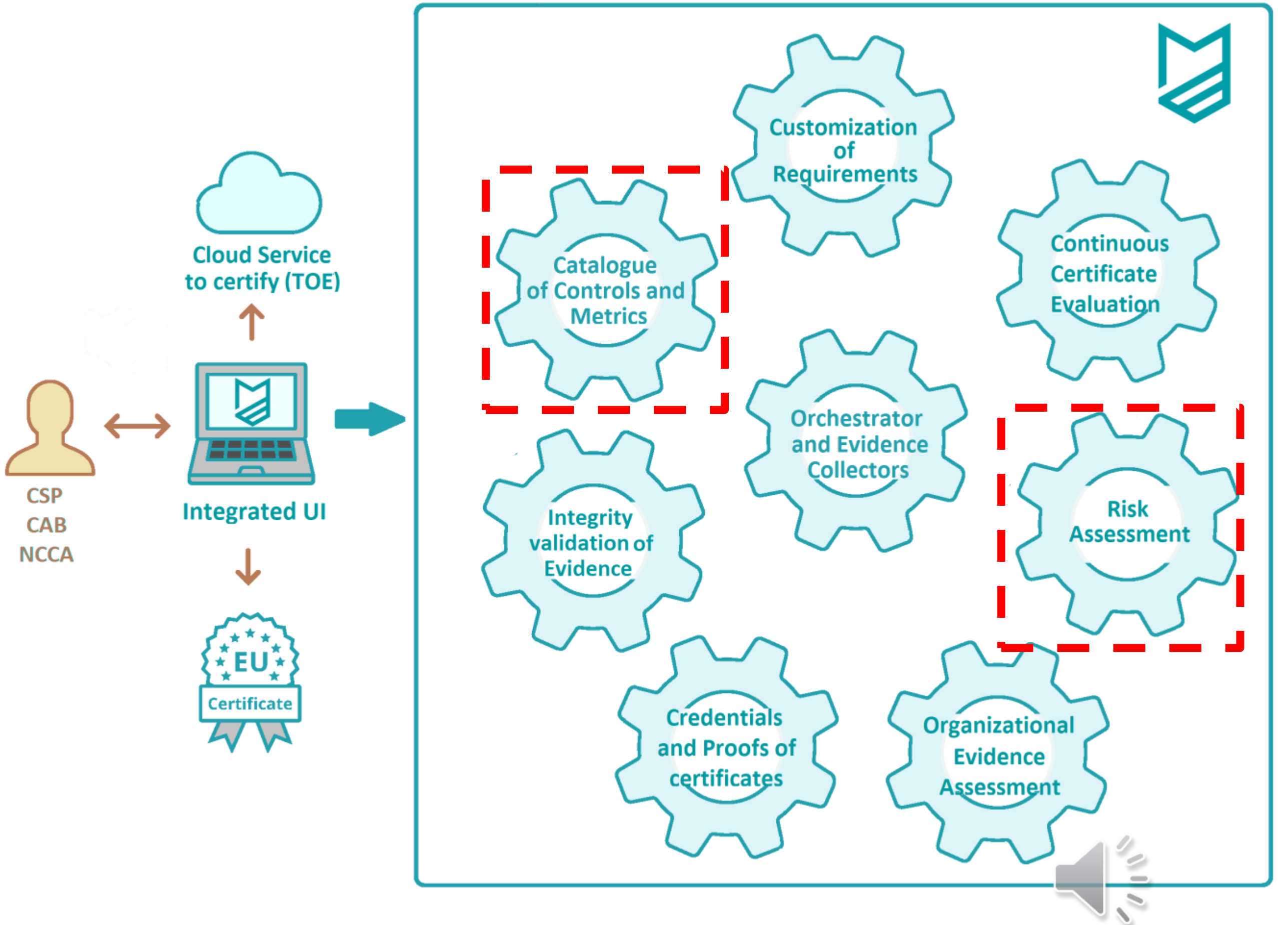
EUCS Misconfiguration Monitoring at Bosch Corporate Level – IUI Components and WFs

- **ToE preparation (WF3):** Orchestrator, Customization of Reqs.
- **Preparedness (WF4):** Catalogue – Questionnaire, SATRA.
- **Assessment (WF5, WF6):** Orchestrator, Organizational Evidence Assessment.
- **Reporting (WF7):** Orchestrator, Continuous Certificate Evaluation.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

EUCS Misconfiguration Monitoring at Bosch Corporate Level – IUI Components and WFs

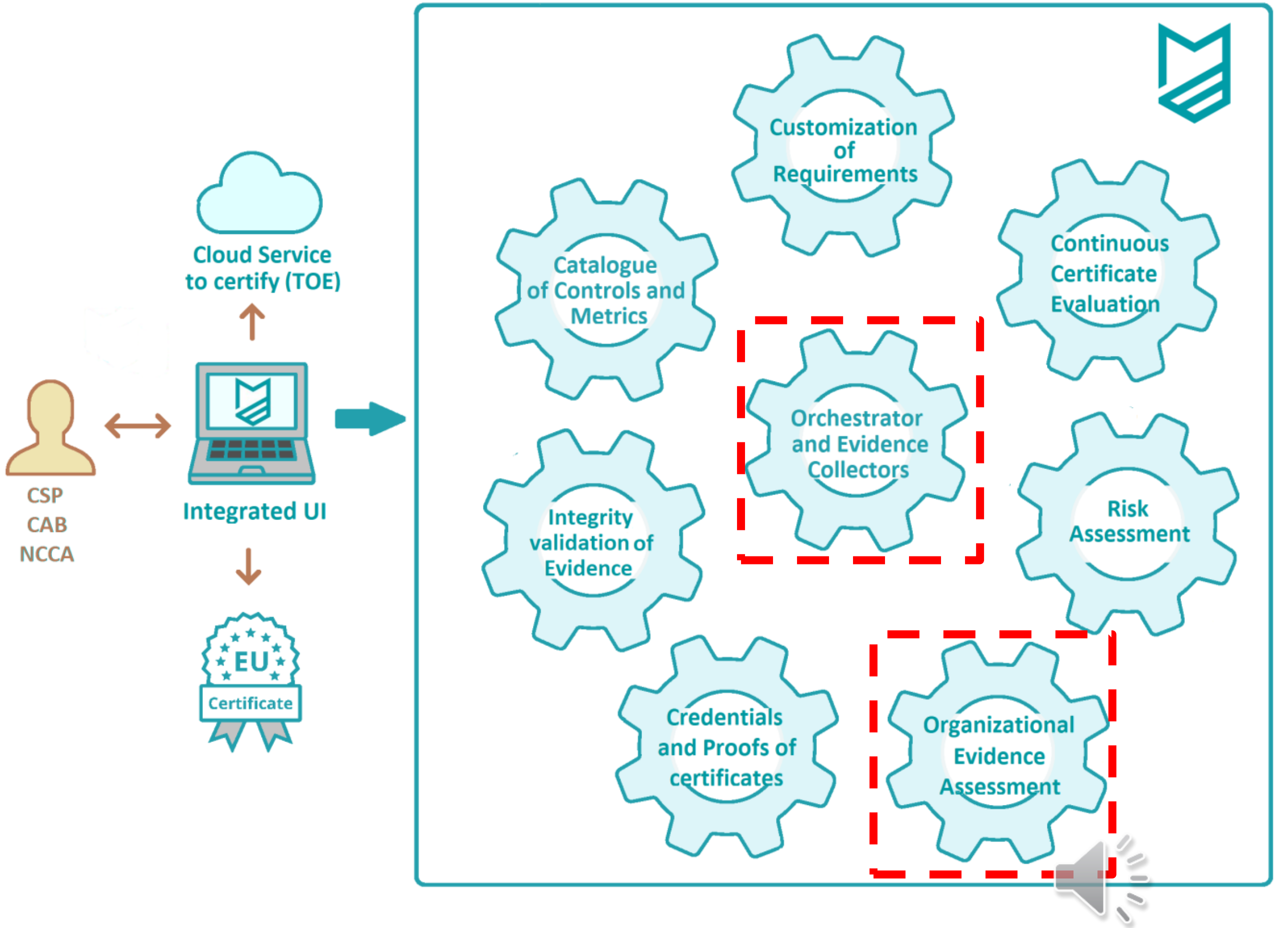
- **ToE preparation (WF3):** Orchestrator, Customization of Reqs.
- **Preparedness (WF4):** Catalogue – Questionnaire, SATRA.
- **Assessment (WF5, WF6):** Orchestrator, Organizational Evidence Assessment.
- **Reporting (WF7):** Orchestrator, Continuous Certificate Evaluation.



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

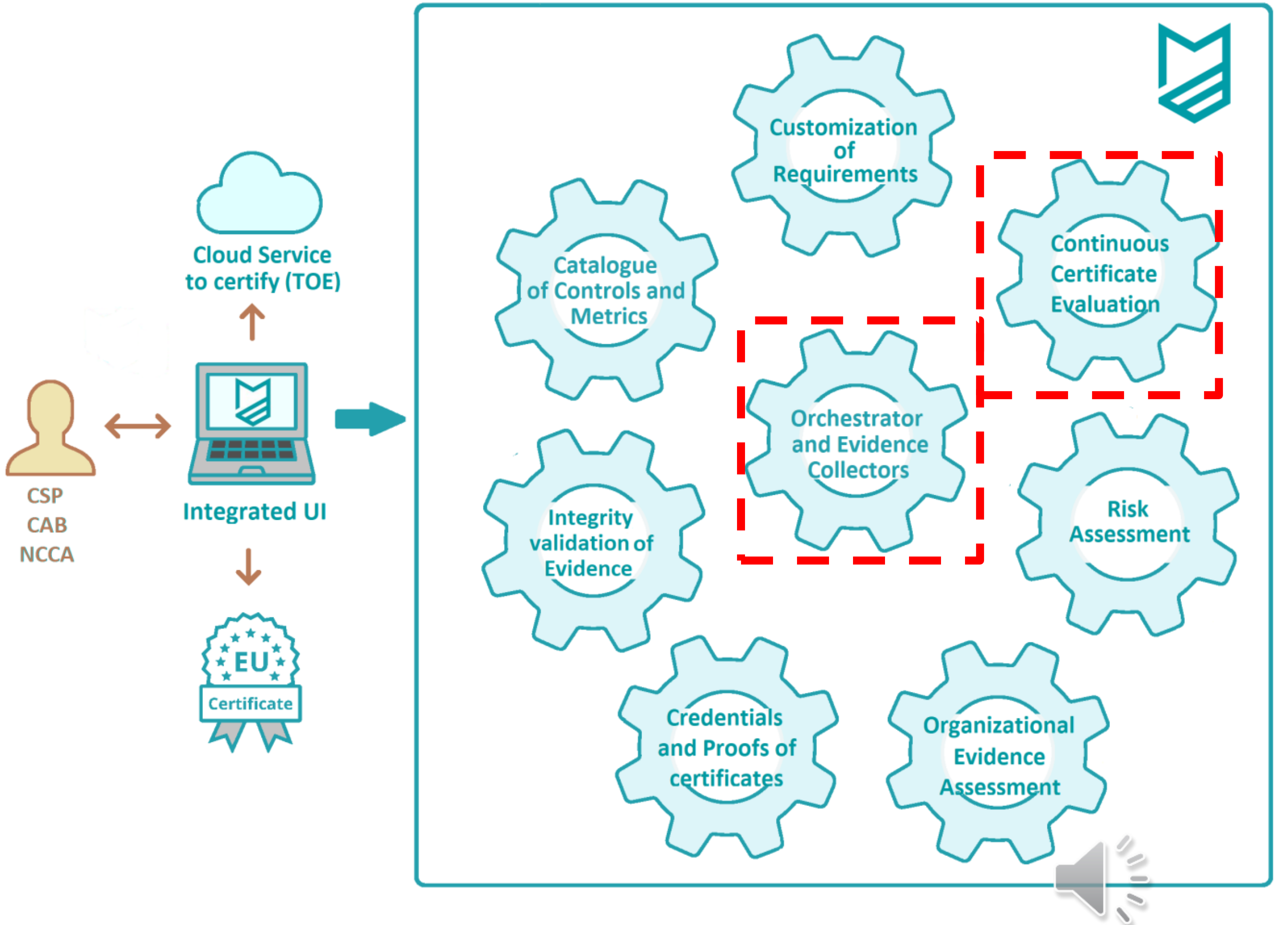
EUCS Misconfiguration Monitoring at Bosch Corporate Level – IUI Components and WFs

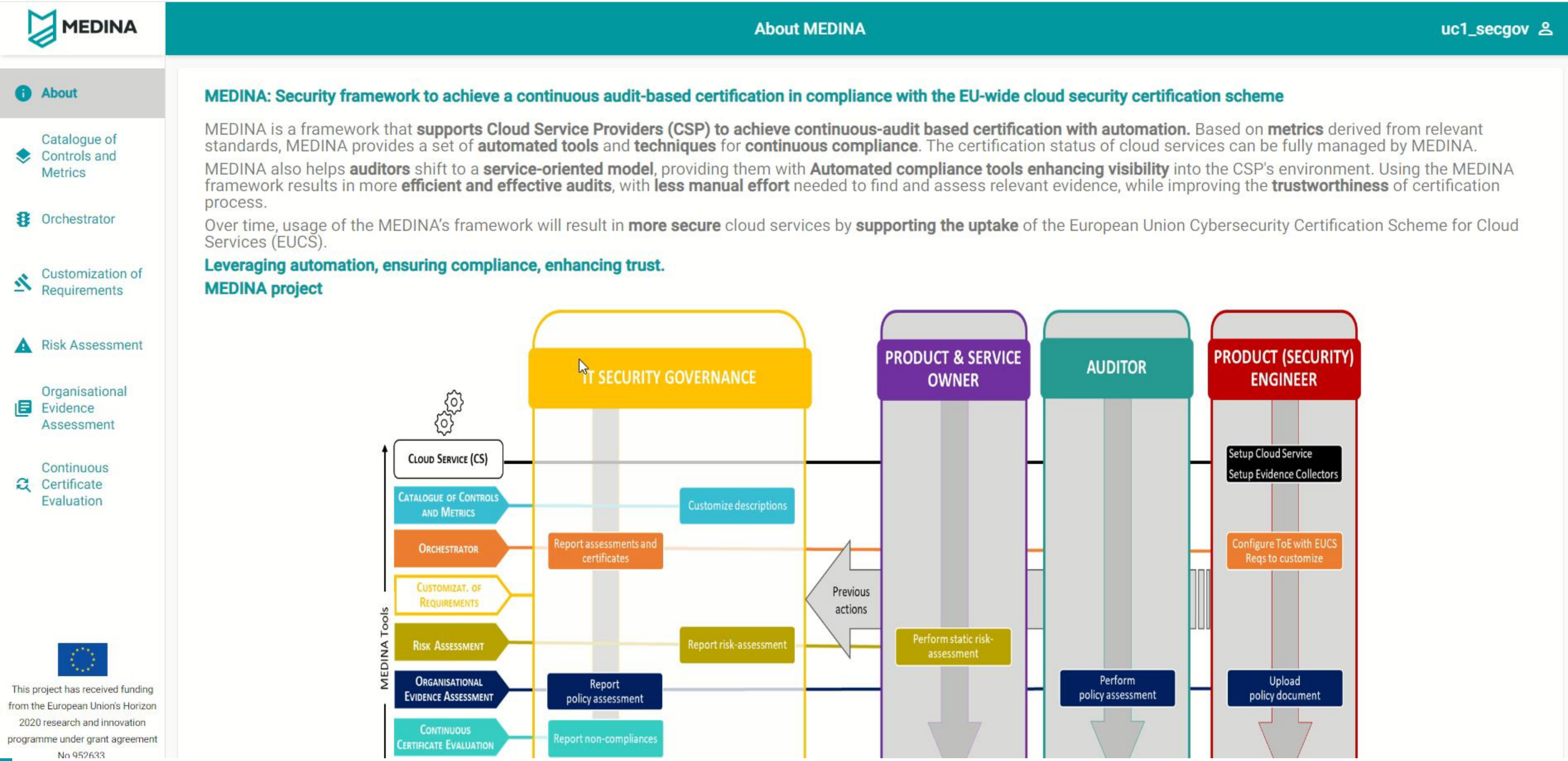
- **ToE preparation (WF3):** Orchestrator, Customization of Reqs.
- **Preparedness (WF4):** Catalogue – Questionnaire, SATRA.
- **Assessment (WF5, WF6):** Orchestrator, Organizational Evidence Assessment.
- **Reporting (WF7):** Orchestrator, Continuous Certificate Evaluation.


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

EUCS Misconfiguration Monitoring at Bosch Corporate Level – IUI Components and WFs

- **ToE preparation (WF3):** Orchestrator, Customization of Reqs.
- **Preparedness (WF4):** Catalogue – Questionnaire, SATRA.
- **Assessment (WF5, WF6):** Orchestrator, Organizational Evidence Assessment.
- **Reporting (WF7):** Orchestrator, Continuous Certificate Evaluation.

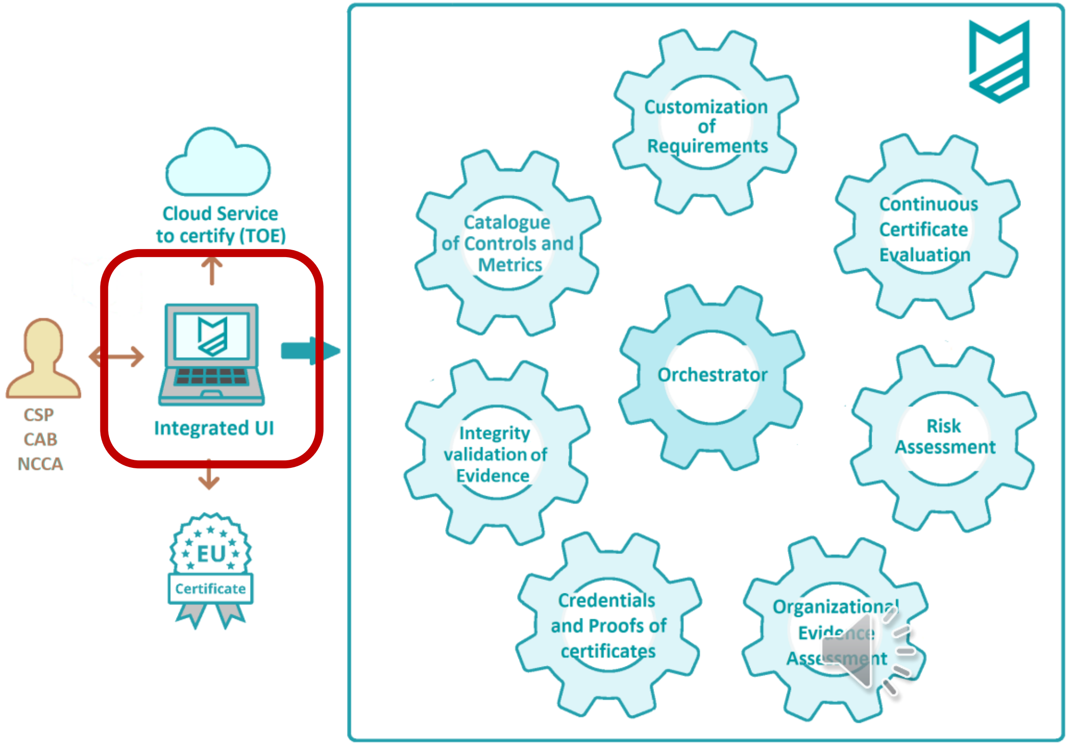

Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment



Integrated UI

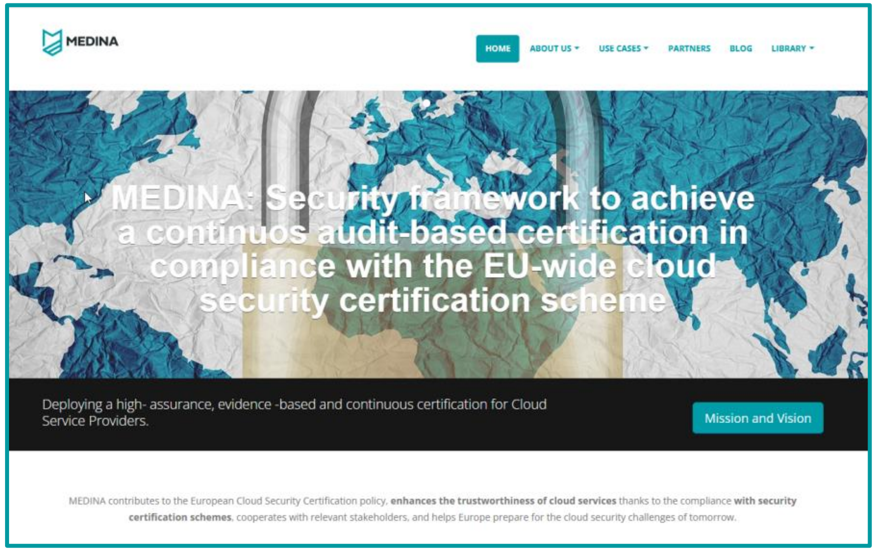
- Further information

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

NIXU cybersecurity.

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

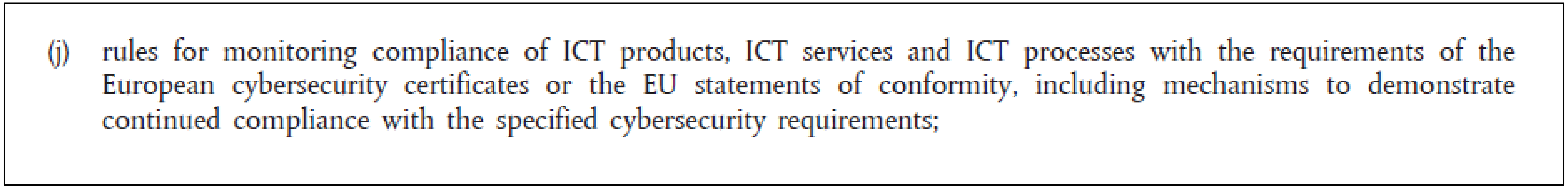
EUCS Automation with MEDINA – An IoT Cloud Use Case

Dr. Jesus Luna Garcia (Robert Bosch GmbH)

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

What is an EU-cybersecurity certification?

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation of cybersecurity certification schemes which include the notions of:
  - Levels of assurance (***Basic, Substantial, High***)
  - ***Continuous cybersecurity compliance (Art. 54(j))***



(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

- Three EUCSA-derived certification schemes are under preparation by ENISA:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - **EUCS - Cybersecurity Certification Scheme for Cloud Services** → BOSCH
  - EU5G - Cybersecurity Certification Scheme for 5G

A Few Words About EUCS

MEDINA

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks (**low risk profile**)

- Limited assurance
- Self-assessment reviewed by a third-party
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources (medium risk profile)**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

‘high’ level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources (elevated risk profile)**

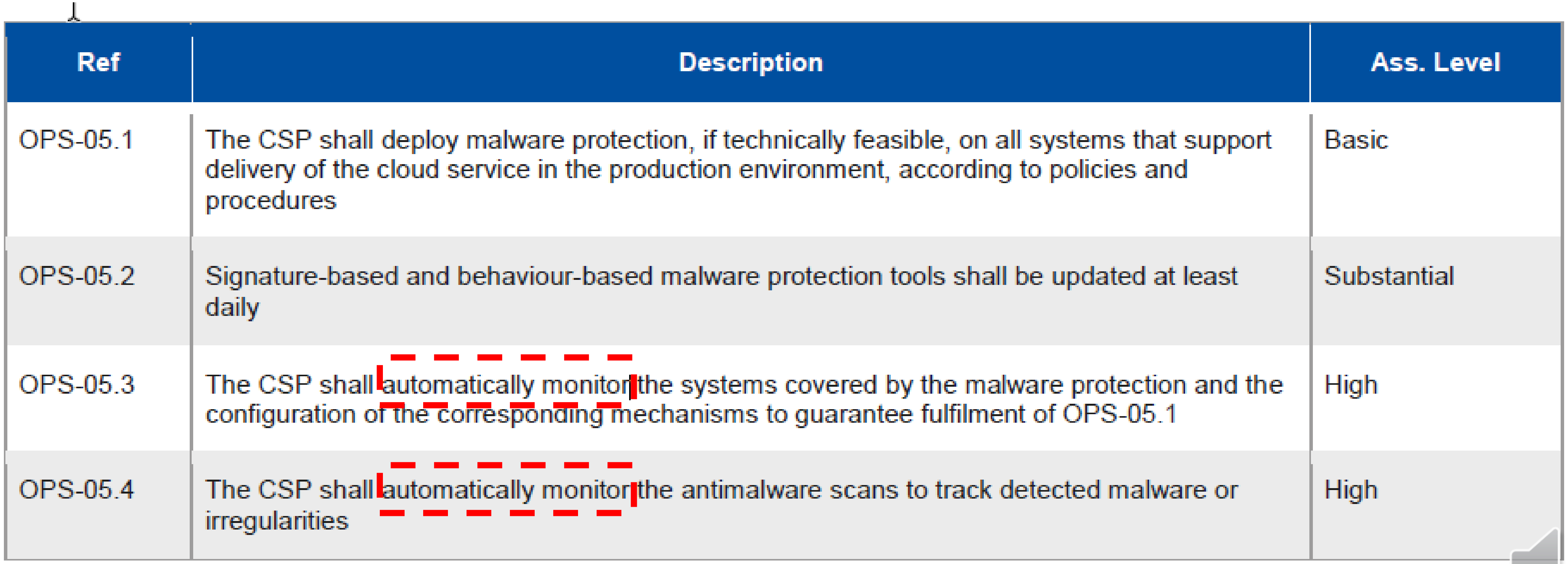
- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

CEN CENELEC is finalizing the standardization of the main EUCS specifications.
After EC approval, it is expected for EUCS to go-live during 2024

Automated Monitoring in EUCS

MEDINA

- Example: OPS-05 Protection Against Malware - Implementation

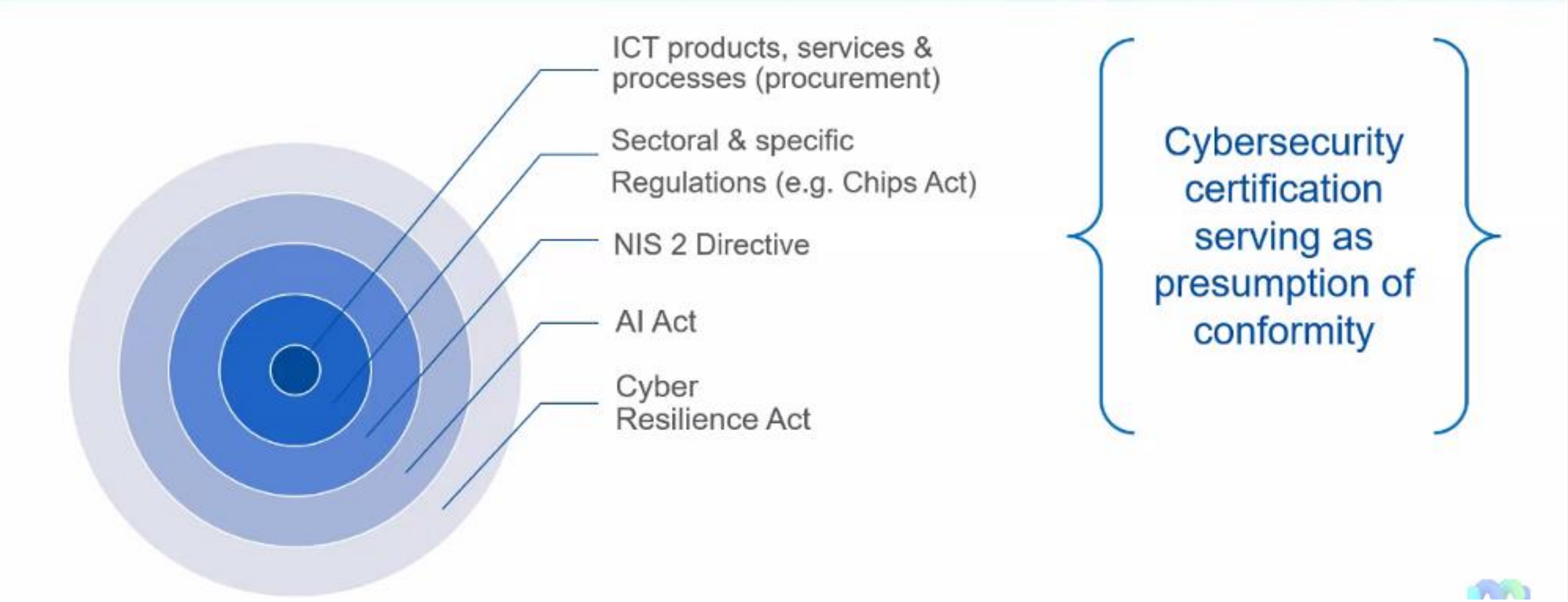


Ref	Description	Ass. Level
OPS-05.1	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures	Basic
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial
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	High
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	High

Source: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Cybersecurity Certification in the EU – the World to Come

- The notion of *EU-cybersecurity certification* is central in upcoming European regulations.



ICT products, services & processes (procurement)

Sectoral & specific Regulations (e.g. Chips Act)

NIS 2 Directive

AI Act

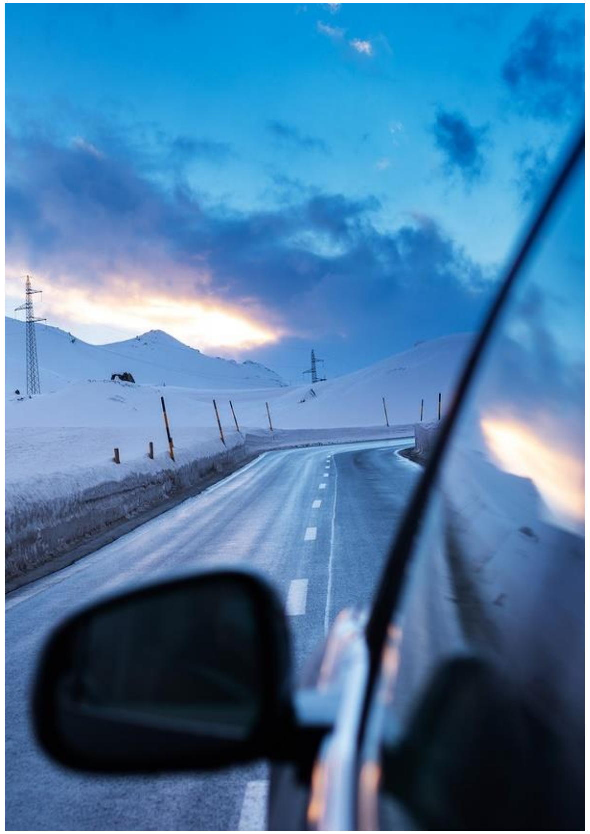
Cyber Resilience Act

Cybersecurity certification serving as presumption of conformity

Borrowed from ENISA's presentation during Cert WS (12.2022)

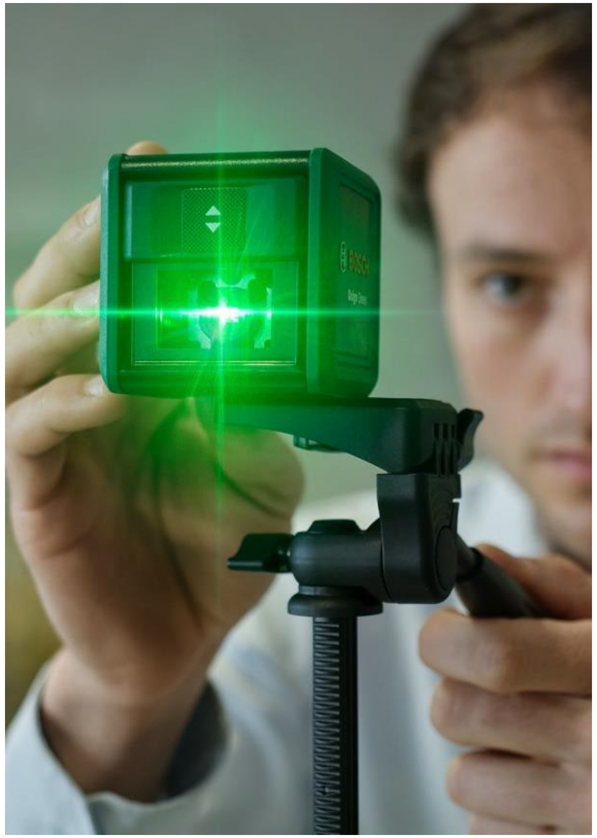
Who we are
Our business sectors

BOSCH

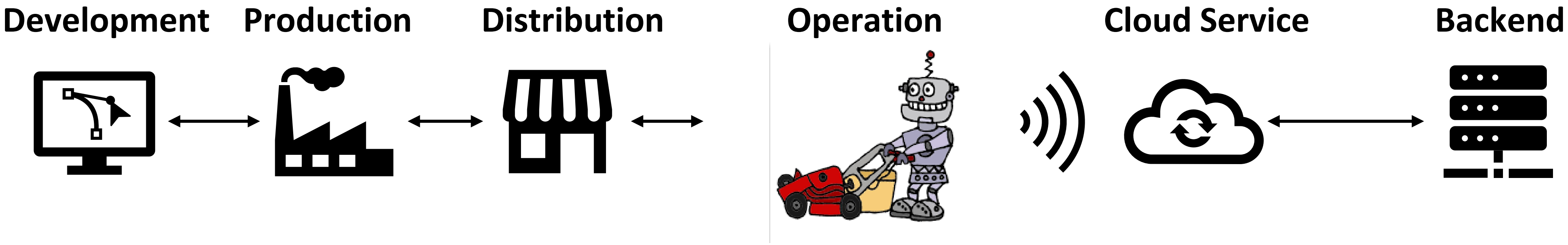

Mobility Solutions

Industrial Technology

Energy and Building Technology

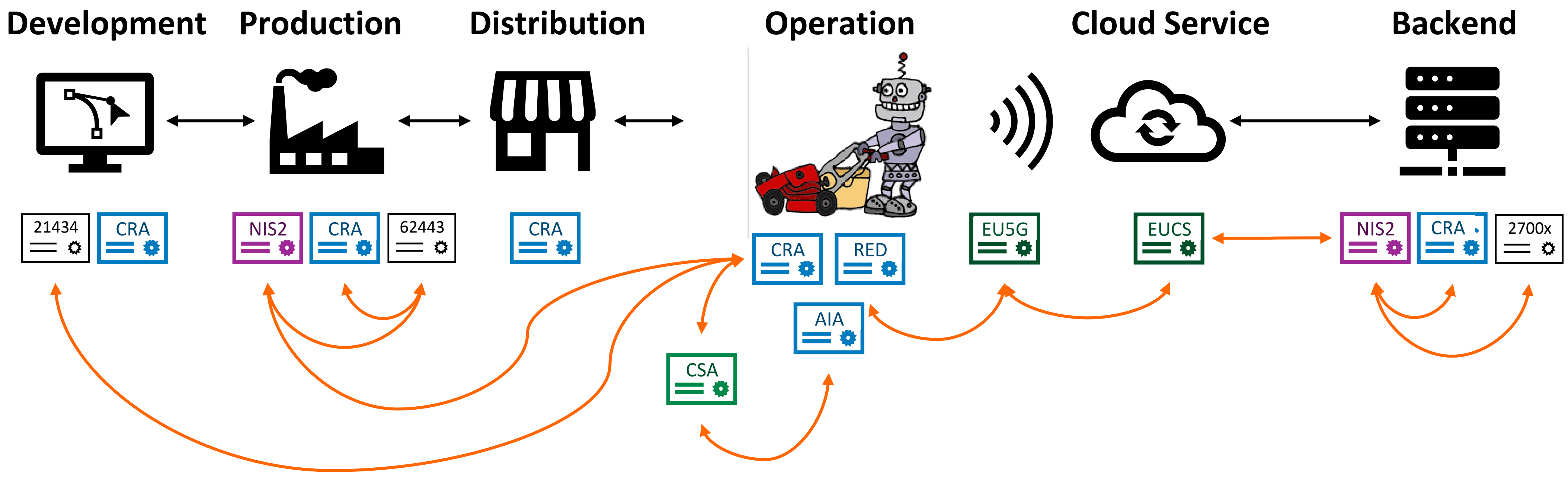

Consumer Goods

EU Certification of a Smart Lawn Mower



Development Production Distribution Operation Cloud Service Backend

EU Certification of a Smart Lawn Mower



Development

21434 CRA

Production

NIS2 CRA 62443

Distribution

CRA

Operation

CRA RED

AIA

CSA

EU5G

Cloud Service

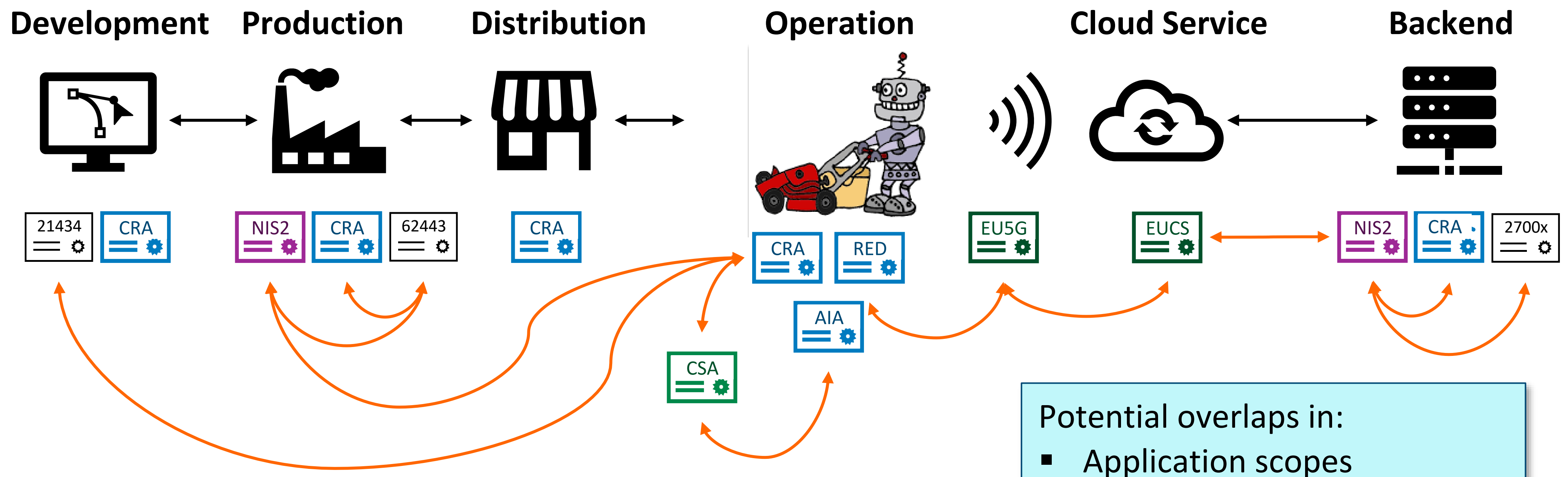
EUCS

Backend

NIS2 CRA 2700x

- Product regulation
- Infrastructure regulation
- Certification scheme
- Other

EU Certification of a Smart Lawn Mower



Development: 21434, CRA

Production: NIS2, CRA, 62443

Distribution: CRA

Operation: CRA, RED, AIA, CSA

EU5G

Cloud Service: EUCS

Backend: NIS2, CRA, 2700x

- XYZ Product regulation
- XYZ Infrastructure regulation
- XYZ Certification scheme
- XYZ Other

Potential overlaps in:

- Application scopes
- Security requirements
- Reporting obligations
- Evidence provisions
- Classifications etc.

Automation and the Utopia of Cybersecurity Certification

MEDINA

- Traditional cybersecurity certification is…
  - Point-in-time based
  - Mostly relying on manual conformance assessment processes
  - Costly and time consuming
  - High level of subjectiveness
  - Audit-once BUT certify-once

- Automation in cybersecurity certification can…
  - Reduce time-to-certificate and associated costs
  - Add objectiveness and repeatability
  - Increase assurance and enable “continuous” certification
  - Audit-once AND certify-many

EU-funded MEDINA Project

MEDINA

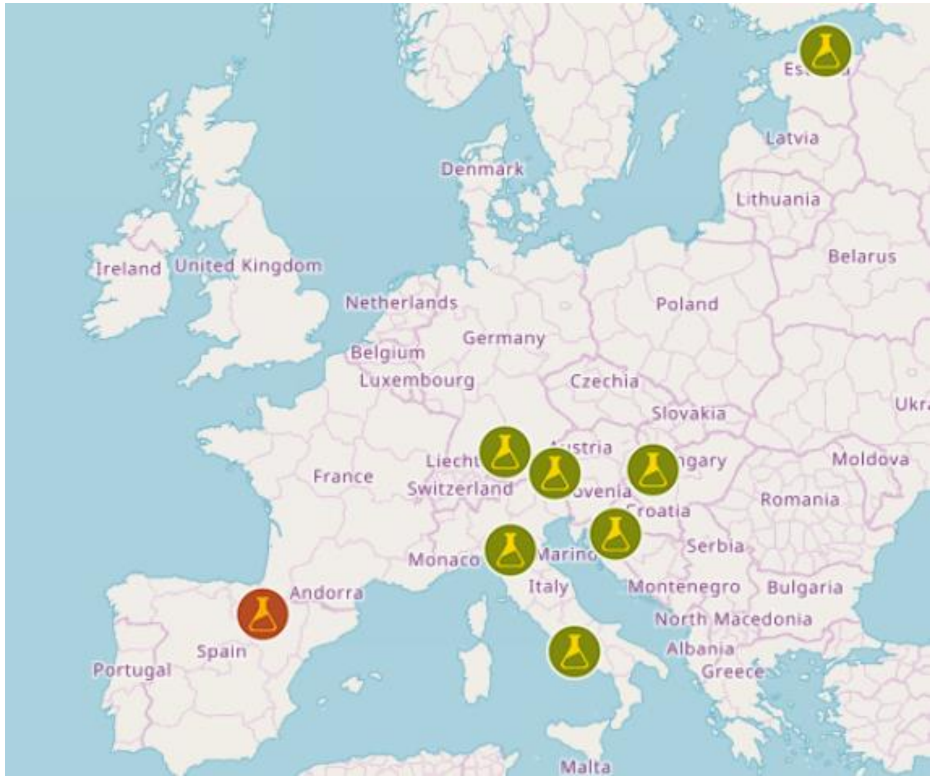
- Goal: provide a security framework for achieving **continuous audit-based certification in EUCS**.
- MEDINA focuses on **automation, standardized metrics and trustworthy** evidence-management methods.
- **MEDINA can be extended** to other certification schemes (e.g., German BSI C5:2020, ISO/IEC 27001).

Continuous (Automated) Monitoring
Continuous Audit-based Certification
MEDINA

Who is who in MEDINA?

MEDINA

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€



tecnalia Inspiring Business

BOSCH

Fraunhofer AISEC

Fabasoft®

Hewlett Packard Enterprise

XLAB

nixu cybersecurity.

Consiglio Nazionale delle Ricerche

Challenges and Approaches

MEDINA

Topic	MEDINA Approach
Automation of compliance assessments	• Automated cloud assessments based on machine-readable metrics • AI-supported security documentation assessment
Trustworthy evidence management	• Blockchain-based evidence vault • RBAC authorization model
Certificate management	• Risk-based automation of certificate life-cycle • Cryptographic verification of EUCS certificates
Standardization	• EUCS: CEN CENELEC EUCS1 • Metrics: ISO/IEC 27004, NIST SP 800-55rev2 • Automation: NIST OSCAL, ETSI CYBER

Summary and Next Steps

MEDINA

- MEDINA aims to **facilitate adoption of EUCS**, while **paving the road for automated cybersecurity certification**.
- Regulators play a critical role in the adoption of automated cybersecurity certification processes.
- Are we there yet?

MEDINA

Leveraging automation, ensuring compliance, enhancing trust.

www.medina-project.eu // jesus.lunagarcia@de.bosch.com

MEDINA

Company Compliance Dashboard

Bernhard Cermak & Niklas Furtlehner, Fabasoft

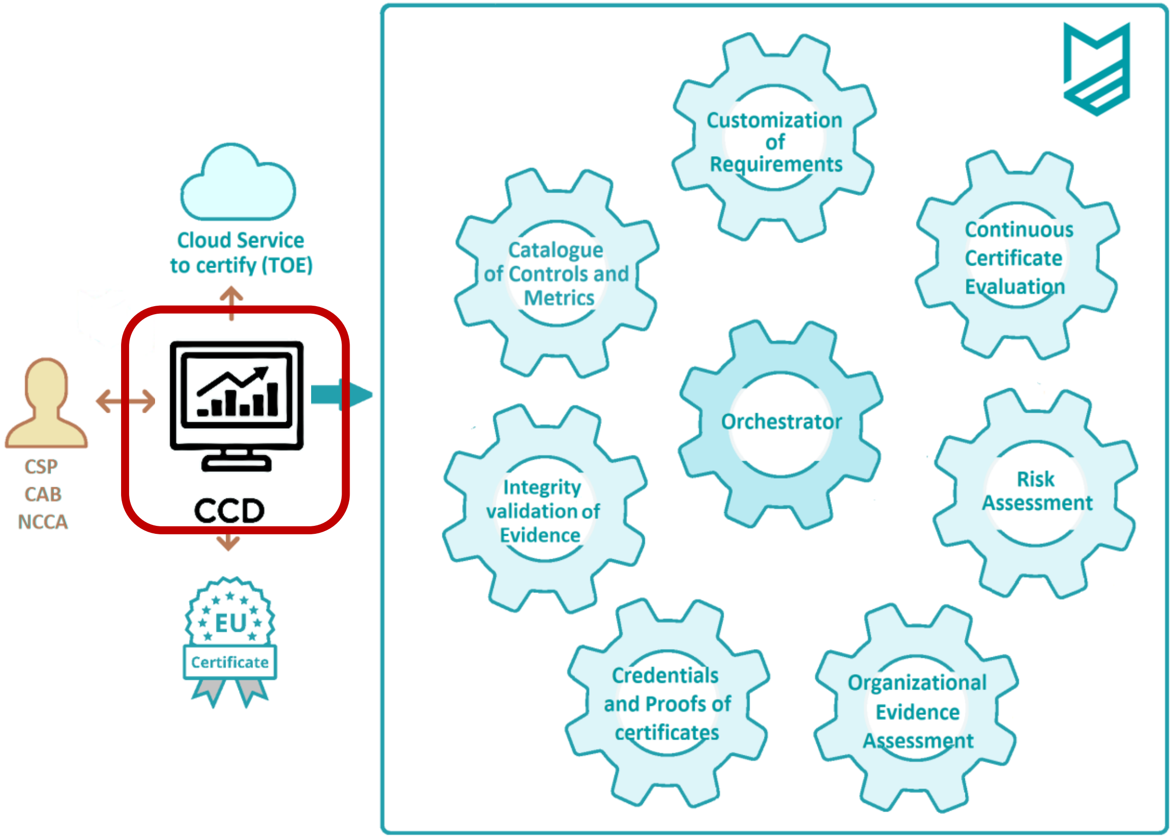
September 2023

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

Chapters

MEDINA

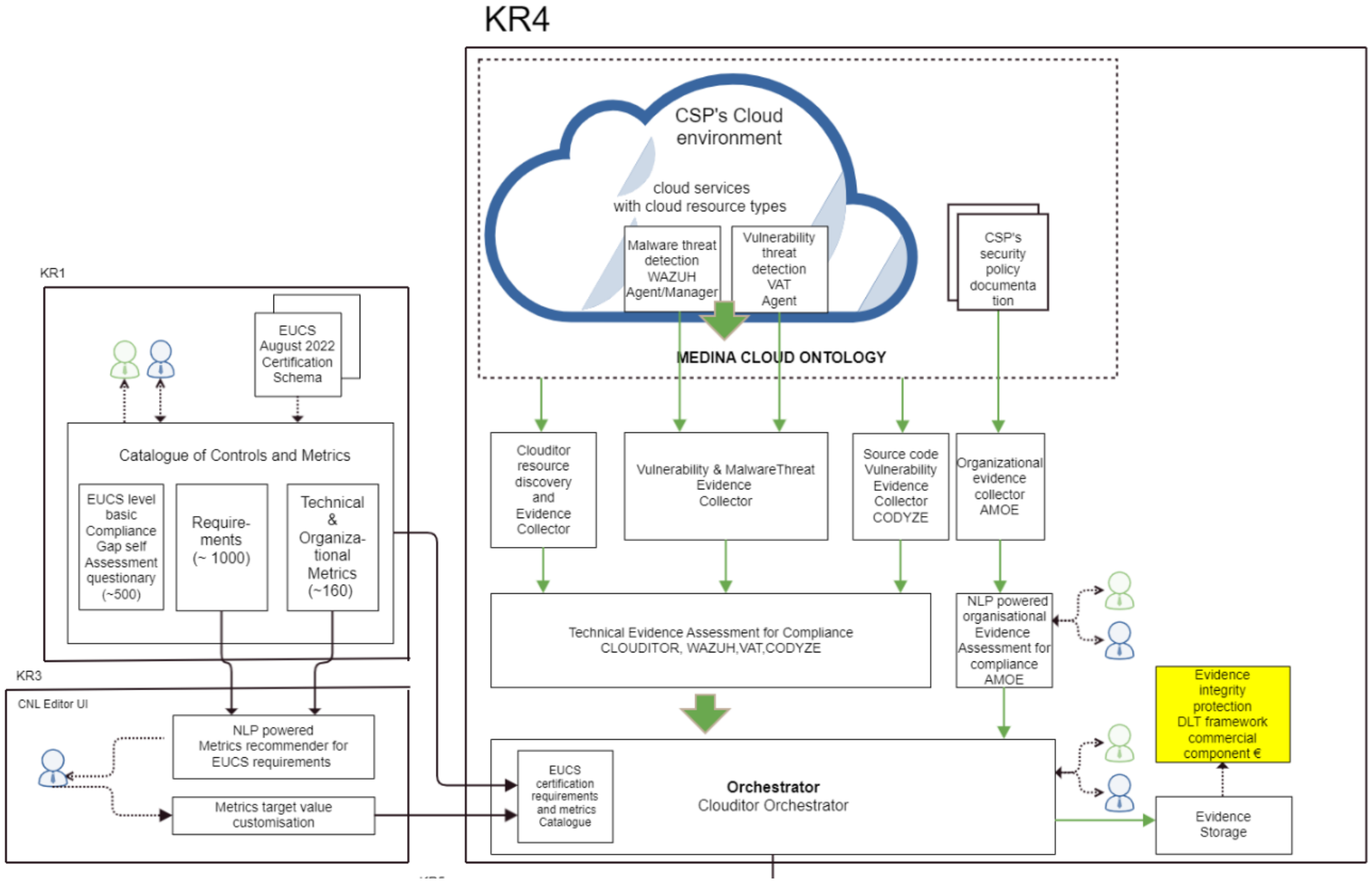
- What is the CCD
  - Orientation
  - Benefits
- How to use it
  - Funtionalities
  - Demo
- Installation
- Further information


Cloud Service
to certify (TOE)
CSP
CAB
NCCA
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

What is the CCD?

- Use case 2 integration
  - company specific system
  - technical perspective
  - as well as a user perspective.
- Company Compliance Dashboard (CCD)
- strong consideration of
  - users and their processes
- represented
  - by roles
  - and personas

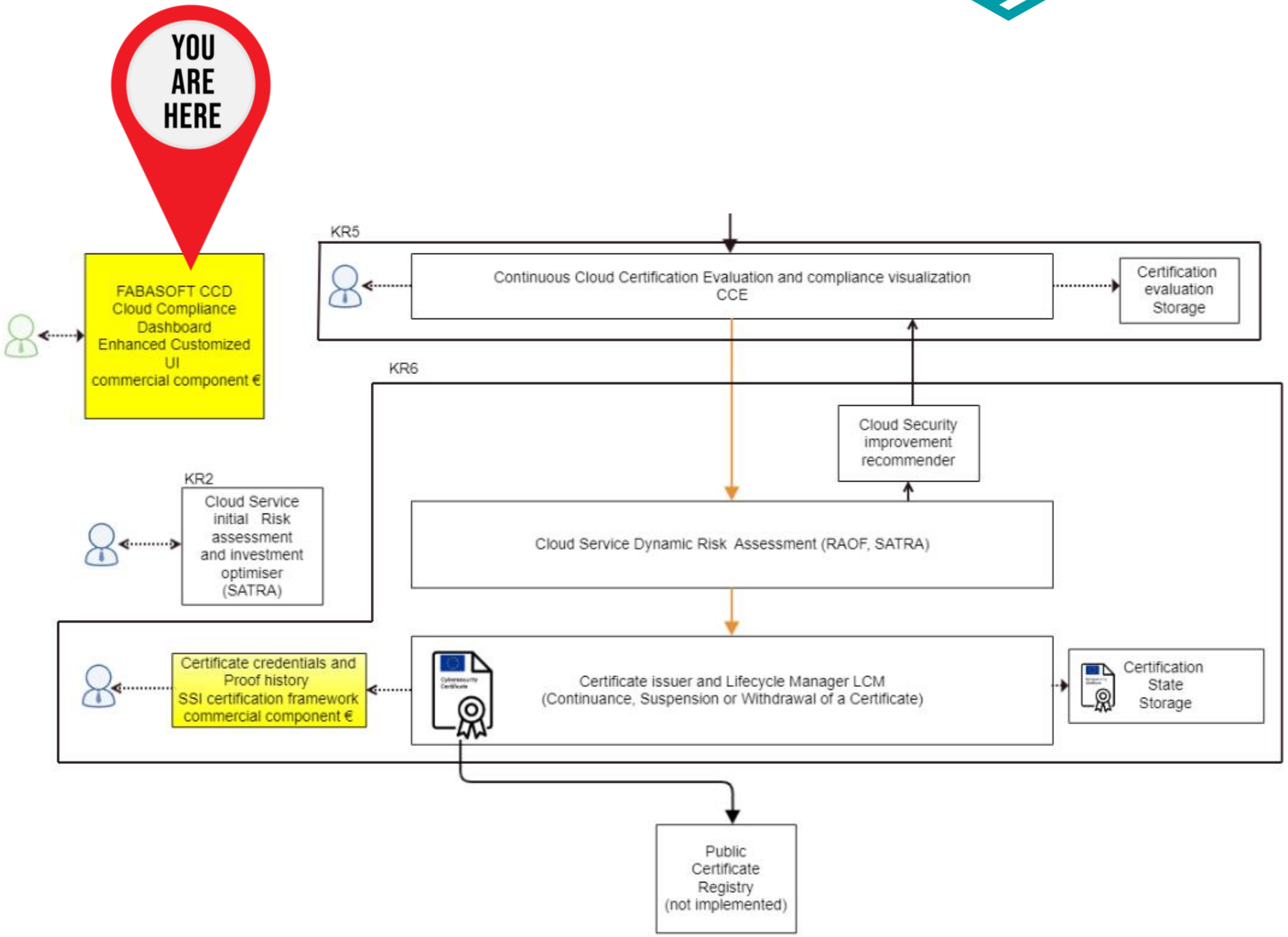
Where is the CCD?

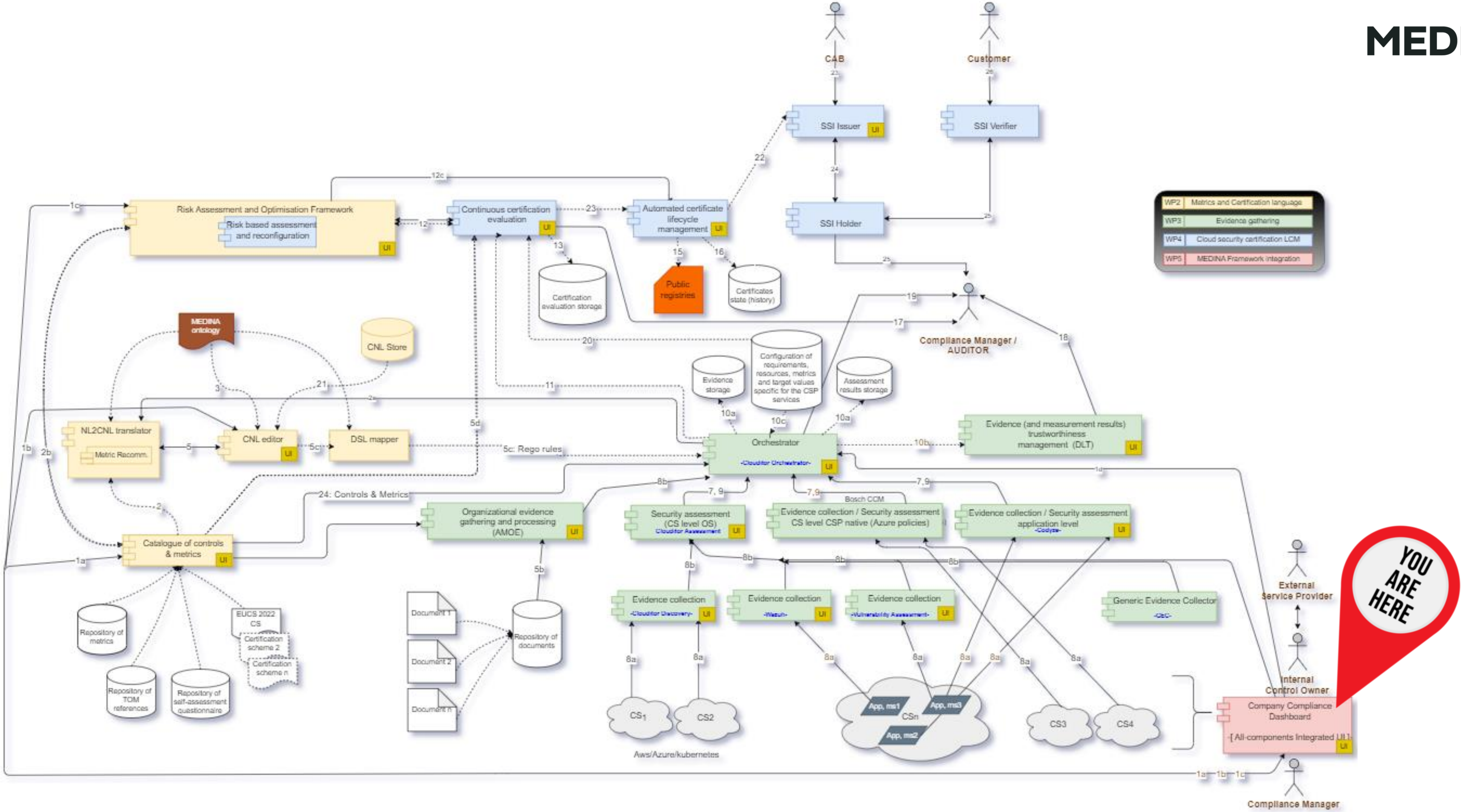

KR4
CSP's Cloud environment
cloud services with cloud resource types
Malware threat detection WAZUH Agent/Manager
Vulnerability threat detection VAT Agent
CSP's security policy documentation
MEDINA CLOUD ONTOLOGY
Clouditor resource discovery and Evidence Collector
Vulnerability & MalwareThreat Evidence Collector
Source code Vulnerability Evidence Collector CODYZE
Organizational evidence collector AMOE
Technical Evidence Assessment for Compliance CLOUDITOR, WAZUH,VAT,CODYZE
NLP powered organisational Evidence Assessment for compliance AMOE
Evidence integrity protection DLT framework commercial component €
Orchestrator
Clouditor Orchestrator
EUCS certification requirements and metrics Catalogue
Evidence Storage
KR1
EUCS August 2022 Certification Schema
Catalogue of Controls and Metrics
EUCS level basic Compliance Gap self Assessment questionary (~500)
Require-ments (~ 1000)
Technical & Organiza-tional Metrics (~160)
KR3
CNL Editor UI
NLP powered Metrics recommender for EUCS requirements
Metrics target value customisation

Orientation

MEDINA

Location of the CCD within the Medina framework

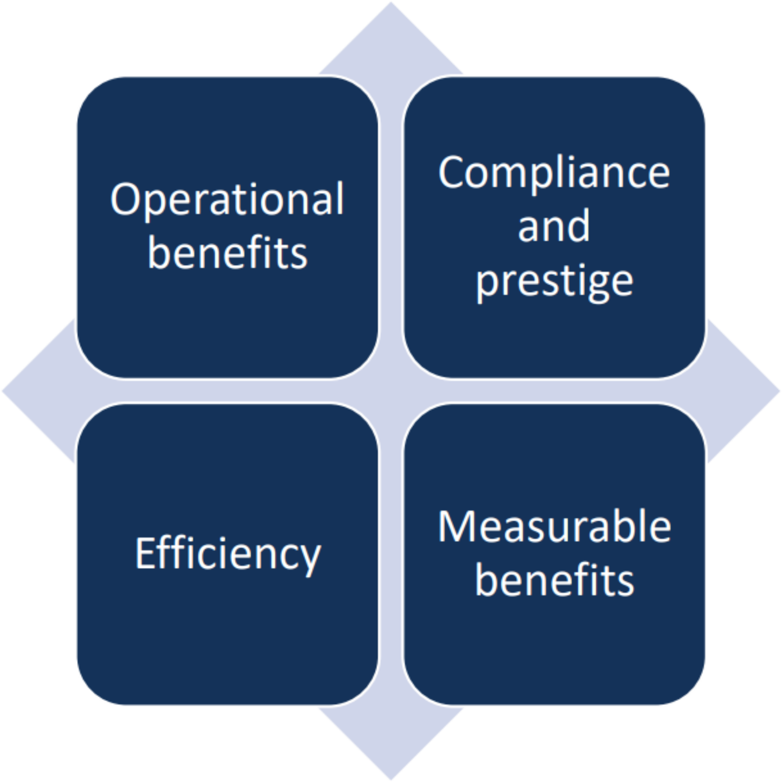

YOU ARE HERE
FABASOFT CCD Cloud Compliance Dashboard Enhanced Customized UI commercial component €
KR5
Continuous Cloud Certification Evaluation and compliance visualization CCE
Certification evaluation Storage
KR6
Cloud Security improvement recommender
KR2
Cloud Service initial Risk assessment and investment optimiser (SATRA)
Cloud Service Dynamic Risk Assessment (RAOF, SATRA)
Certificate credentials and Proof history SSI certification framework commercial component €
Certificate issuer and Lifecycle Manager LCM (Continuance, Suspension or Withdrawal of a Certificate)
Certification State Storage
Public Certificate Registry (not implemented)


CAB
Customer
SSI Issuer
SSI Verifier
SSI Holder
UI
22
23
24
25
26
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
Continuous certification evaluation
Automated certificate lifecycle management
12c
1c
12
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
Compliance Manager / AUDITOR
17
18
19
20
MEDINA ontology
CNL Store
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
11
21
3
2a
2b
1b
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5
5c
5d
5c: Rego rules
10a
10c
10b
Orchestrator
-Clouditor Orchestrator-
Evidence (and measurement results) trustworthiness management (DLT)
1d
24: Controls & Metrics
2
Catalogue of controls & metrics
1a
Organizational evidence gathering and processing (AMOE)
5b
8b
7, 9
7,9
Bosch CCM
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
Evidence collection
-Clouditor Discovery-
-Wazuh-
-Vulnerability Assessment-
Generic Evidence Collector
-CbC-
8a
Repository of metrics
Repository of TOM references
Repository of self-assessment questionnaire
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
CS1
CS2
App, ms1
App, ms2
App, ms3
CSn
CS3
CS4
Aws/Azure/kubernetes
External Service Provider
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
1a
1b
1c
Compliance Manager
YOU ARE HERE

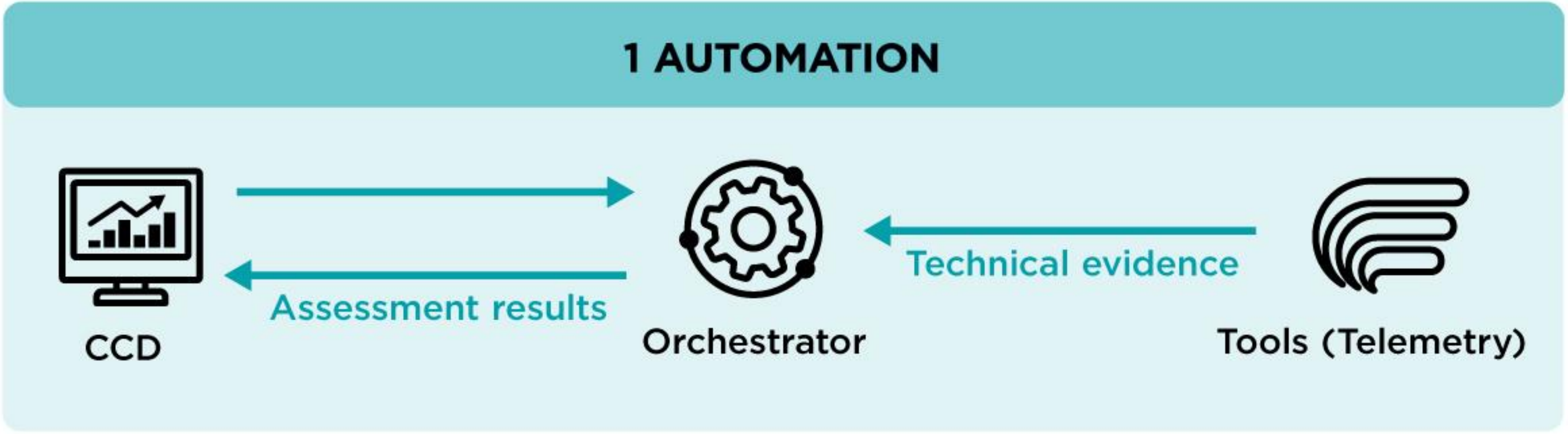
WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

What are the Benefits of the CCD?

- Audit Automation
- Supported Audit
- Audit Standardisation
- Audit Management
- Audit Insights

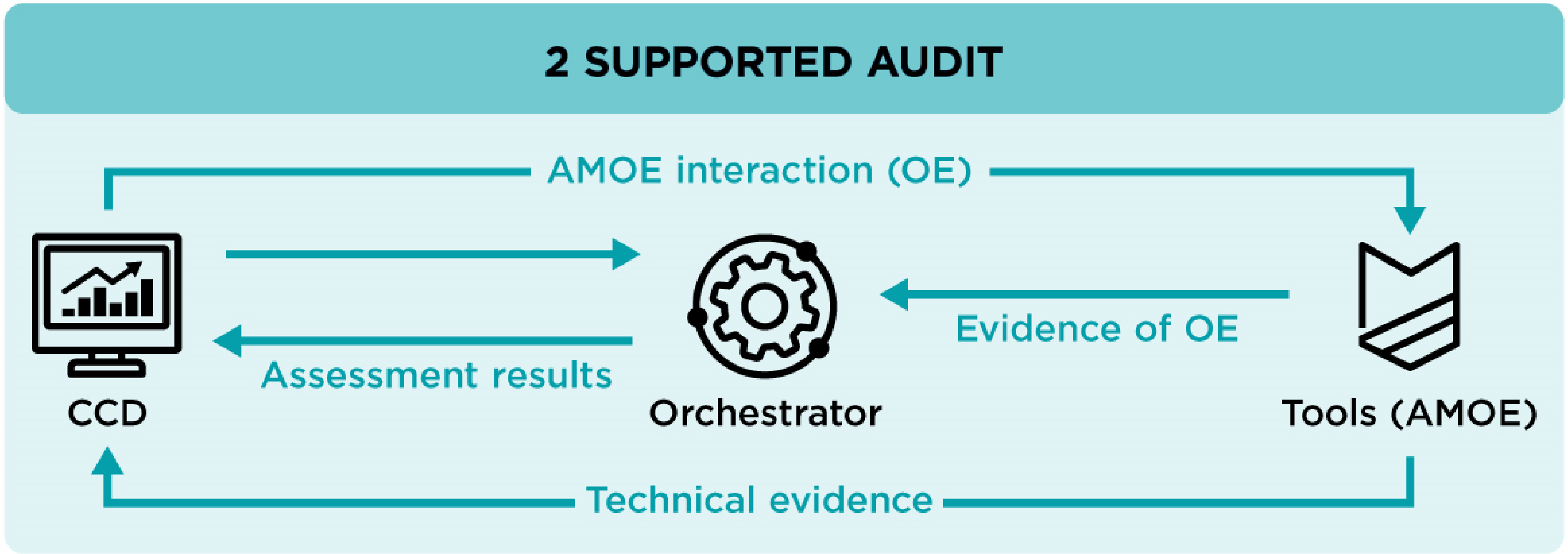


Audit Automation



CCD Company Compliance Dashboard

Supported Audit

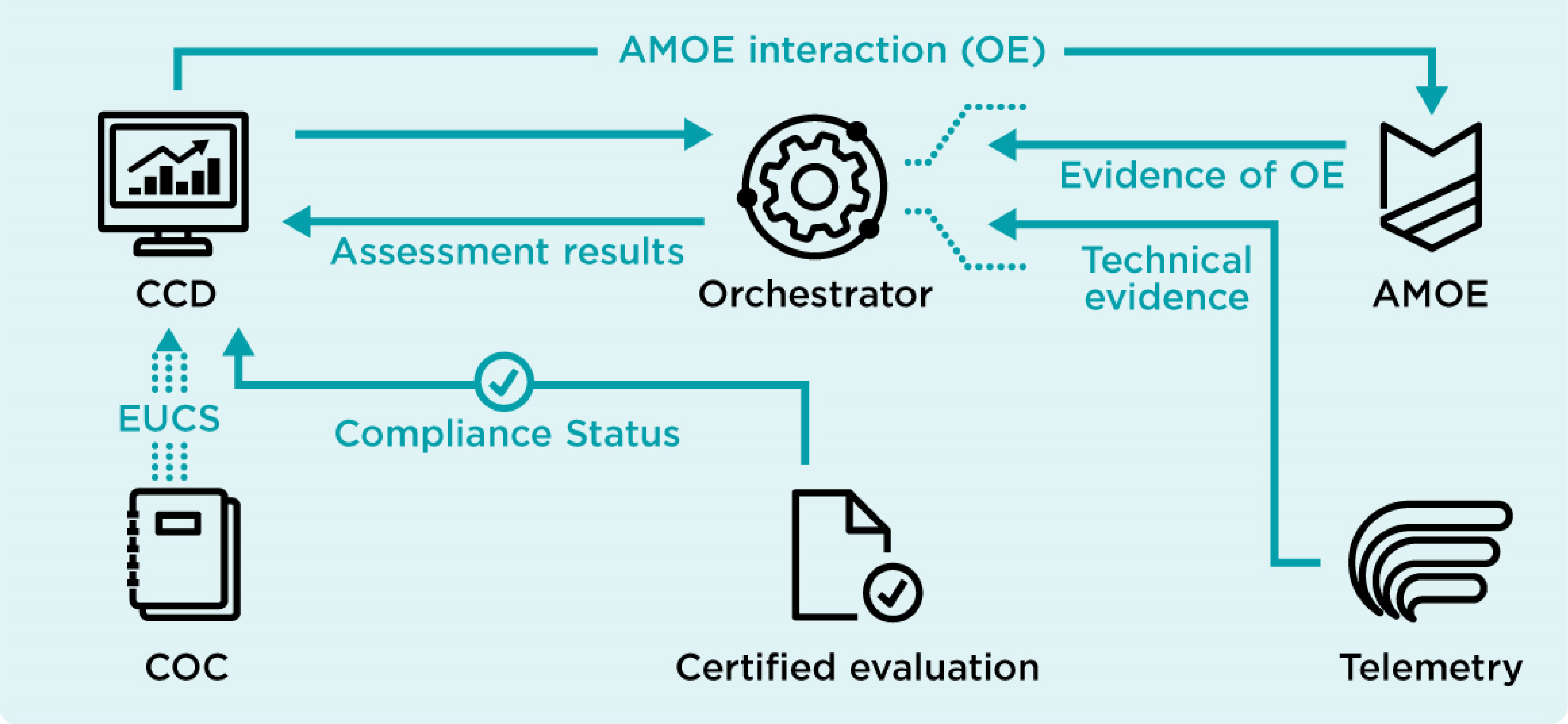


CCD Company Compliance Dashboard

AMOE Tool to Automatically Extract and Assess Organizational Evidence for Continuous Cloud Audit

3 STANDARDIZED AUDIT

MEDINA



AMOE interaction (OE)

CCD

Assessment results

Orchestrator

Evidence of OE

Technical evidence

AMOE

EUCS

Compliance Status

COC

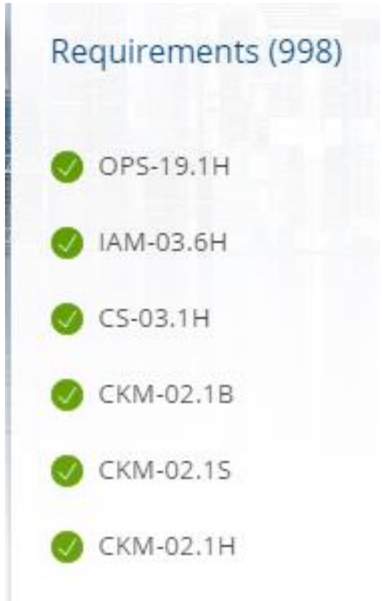
Certified evaluation

Telemetry

CCD	Company Compliance Dashboard	AMOE	Tool to Automatically Extract and Assess Organizational Evidence for Continuous Cloud Audit
OE	Organizational Evidence	⋱⋮⋰	One Pipeline for OE and TE
TE	Technical Evidence	⁞⁞⁞⁞	Fixed structure for each Catalogue
CoC	Catalogue of Controls	✓	Compliance Information based on whole ToE context
ToE	Target of Evaluation		

Audit insights

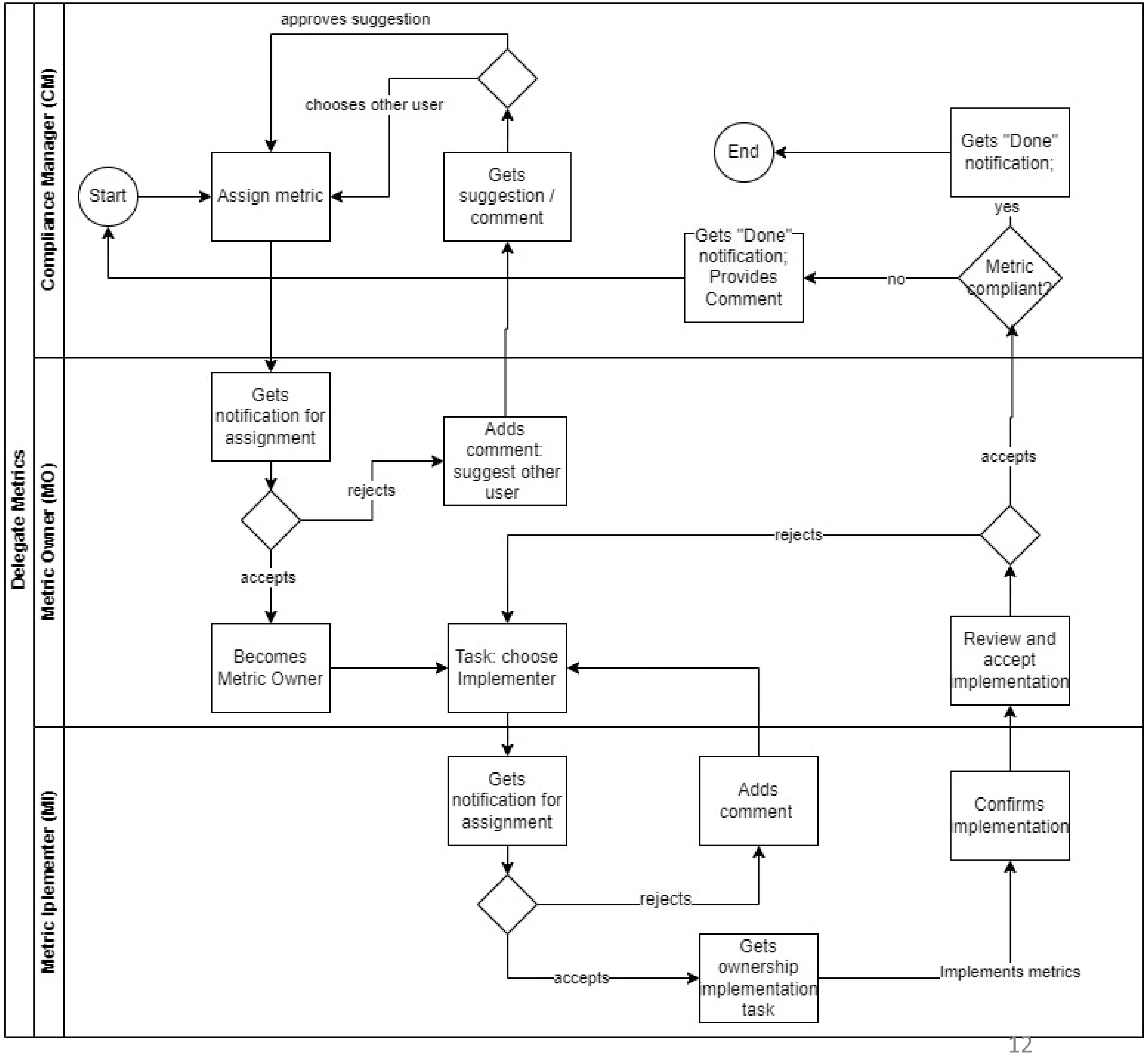
- Enforce the tracking capabilities of cloud solutions for Audit evidence.
- Following Options to track changes:
  - Signature
  - Process
  - Timeline
  - Activities
  - Object Changes



Requirements (998)

- ✓ OPS-19.1H
- ✓ IAM-03.6H
- ✓ CS-03.1H
- ✓ CKM-02.1B
- ✓ CKM-02.1S
- ✓ CKM-02.1H

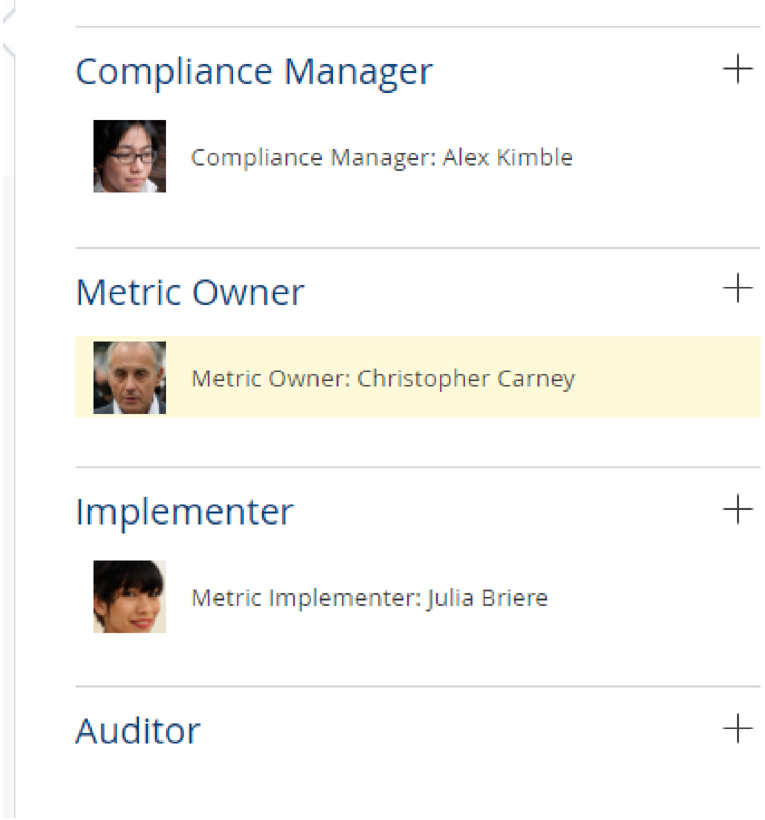
Audit Management



Who works with the CCD?

Very short intro of Roles.

- Compliance Manager – assigns task
- Metric Owner – plans & assigns implementation
- Metric implementer –implements metrics
- Auditor (under construction) – Reviews & Reacts



Compliance Manager +

Compliance Manager: Alex Kimble

Metric Owner +

Metric Owner: Christopher Carney

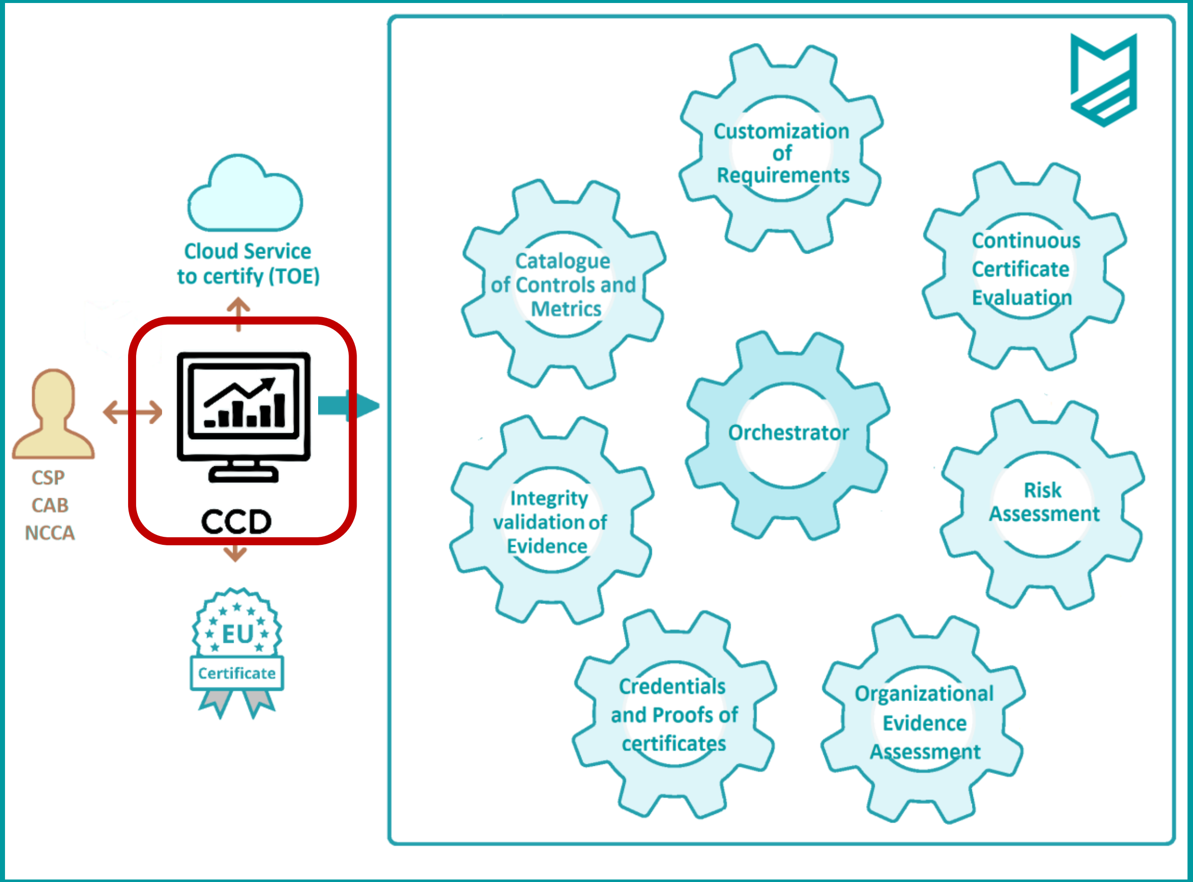
Implementer +

Metric Implementer: Julia Briere

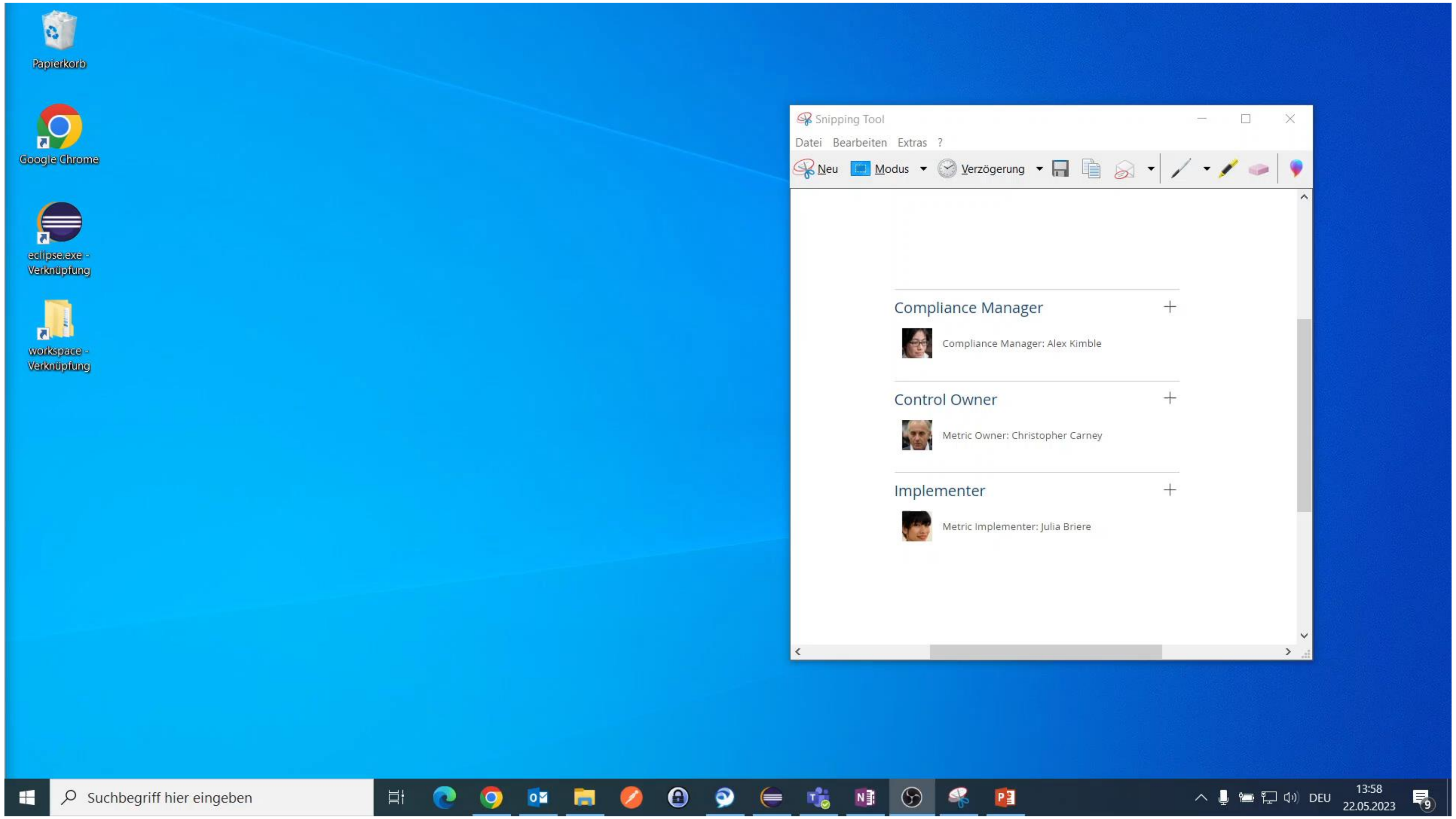
Auditor +

Compliance Manager

RESPONSIBLE FOR AUDIT | ASSIGNS COMPLIANCE TASKS


Cloud Service to certify (TOE)
CSP
CAB
NCCA
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Log in as compliance manager



Compliance Manager +

Compliance Manager: Alex Kimble

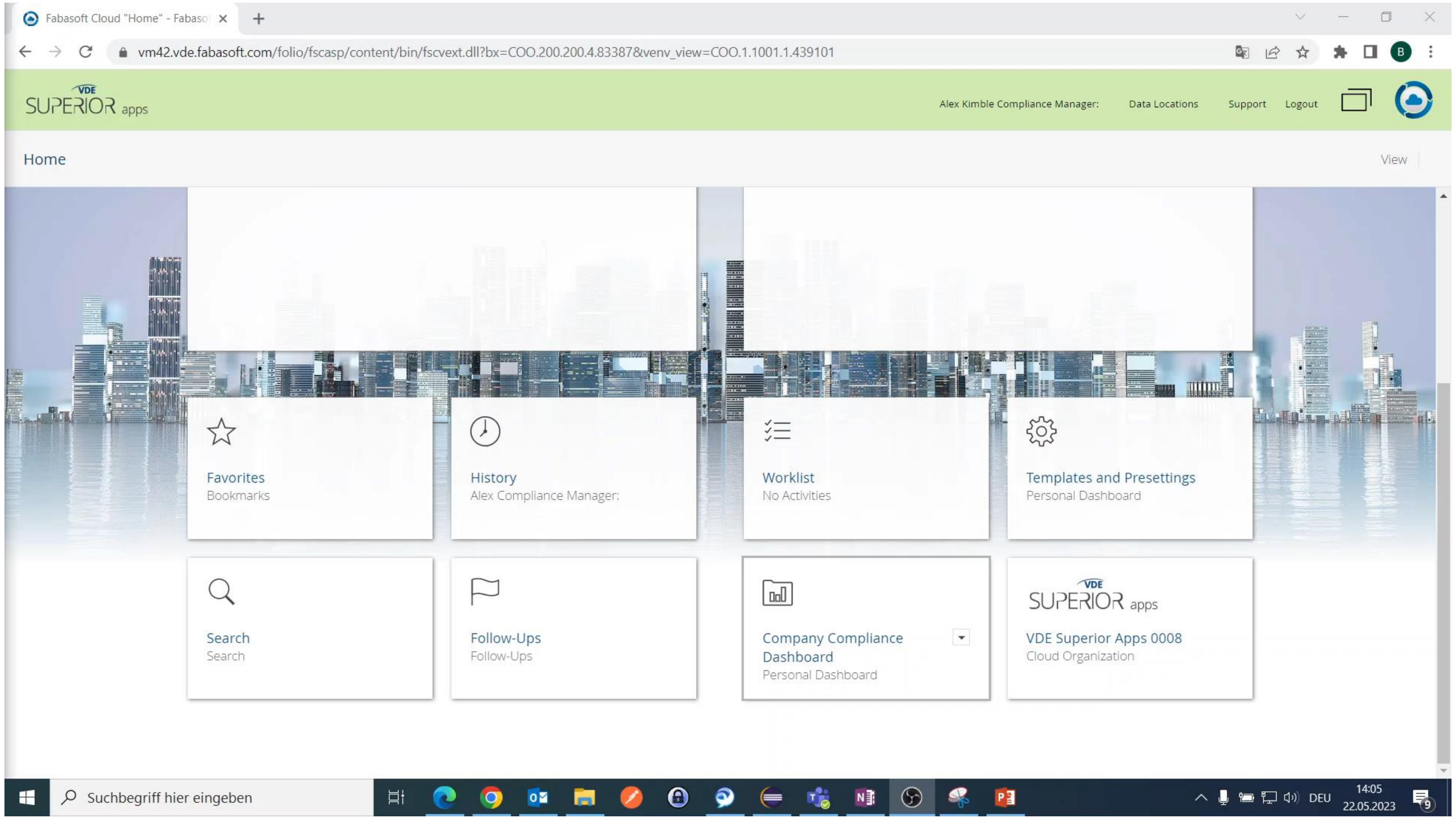
Control Owner +

Metric Owner: Christopher Carney

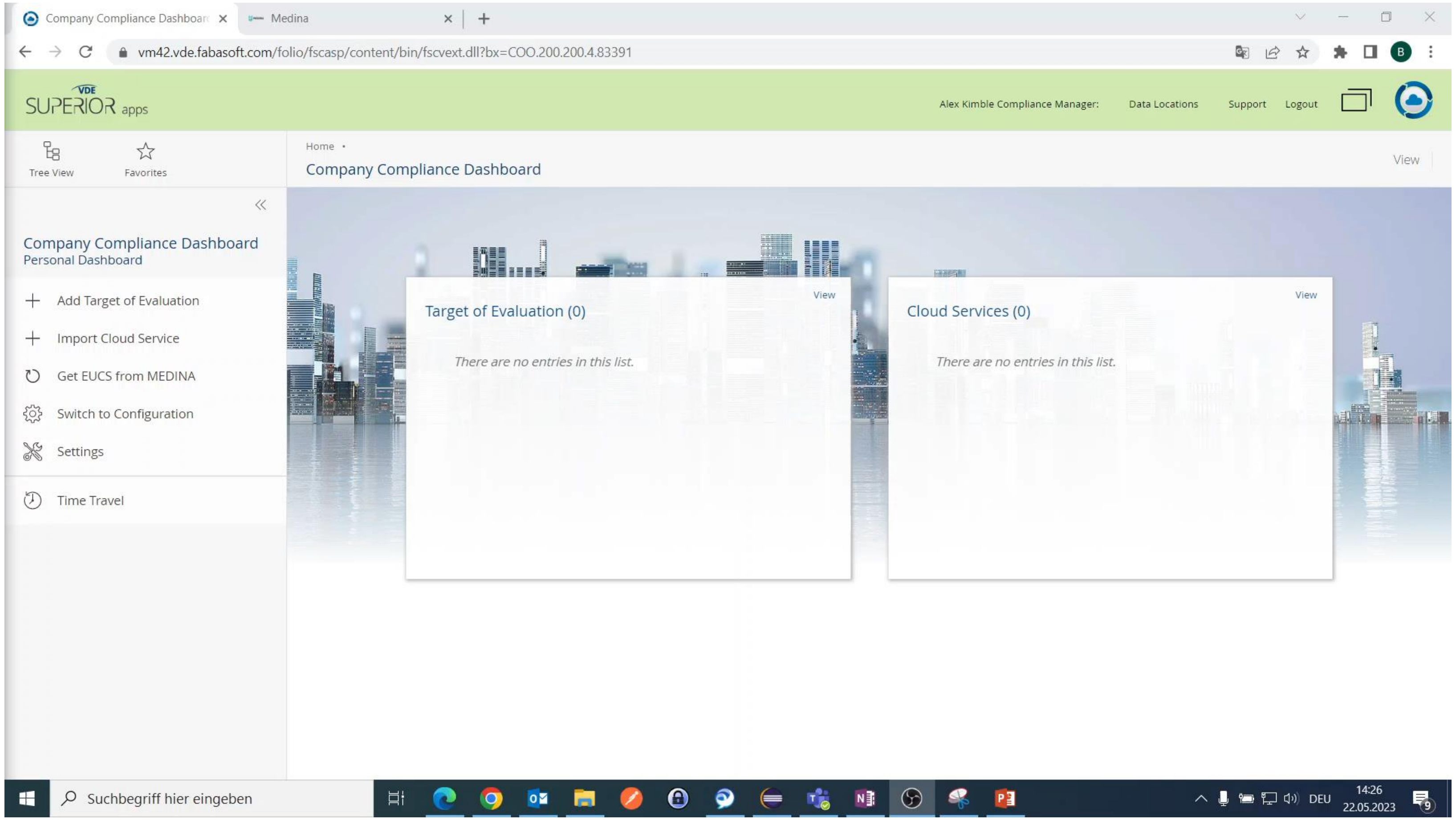
Implementer +

Metric Implementer: Julia Briere

Import Data from MEDINA


Fabasoft Cloud "Home" - Fabaso
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83387&venv_view=COO.1.1001.1.439101
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Home
View
Favorites
Bookmarks
History
Alex Compliance Manager:
Worklist
No Activities
Templates and Presettings
Personal Dashboard
Search
Search
Follow-Ups
Follow-Ups
Company Compliance Dashboard
Personal Dashboard
VDE Superior Apps 0008
Cloud Organization
Suchbegriff hier eingeben
DEU
14:05
22.05.2023

Import Cloud Service



Company Compliance Dashboard

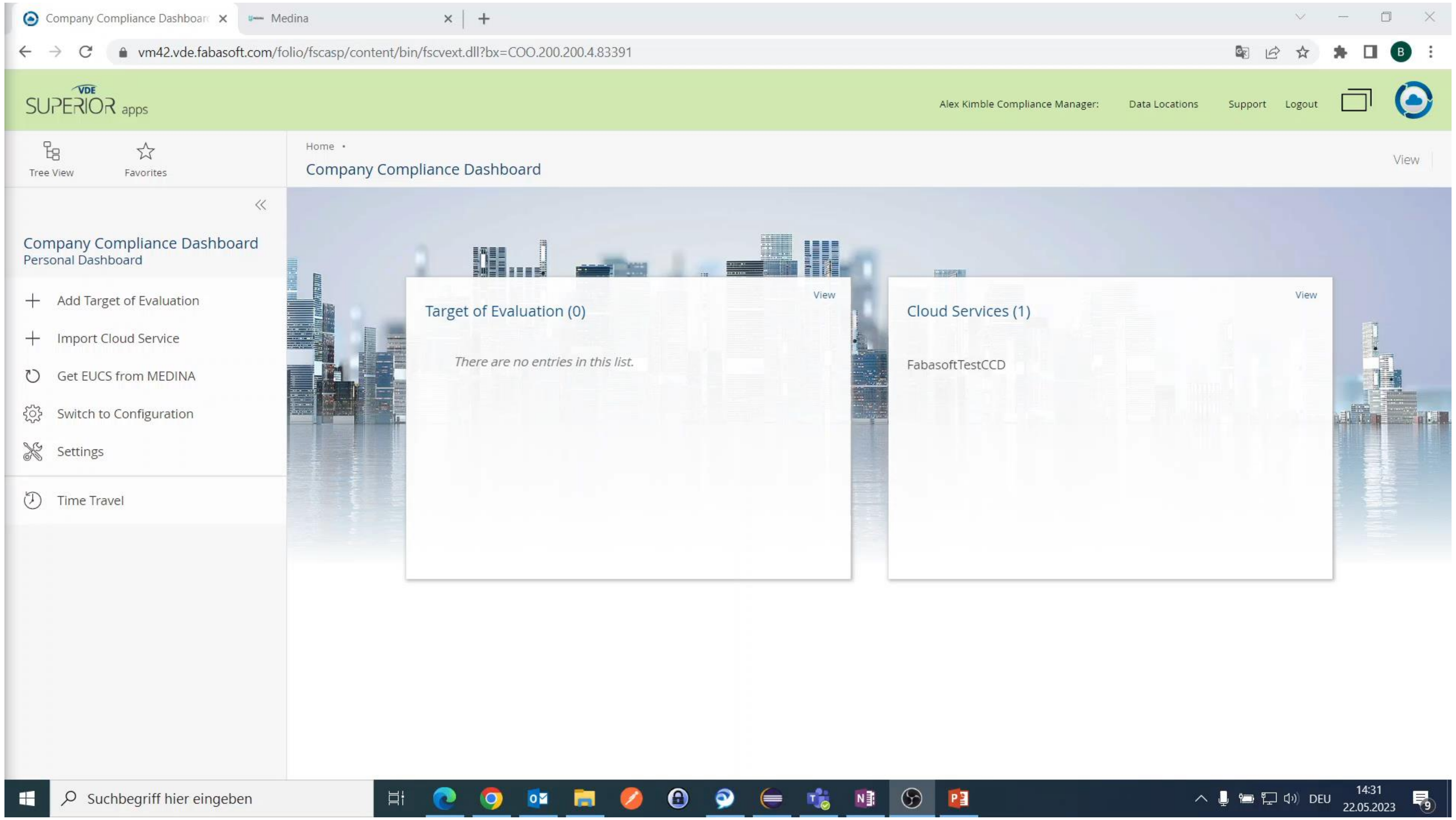
Target of Evaluation (0)

There are no entries in this list.

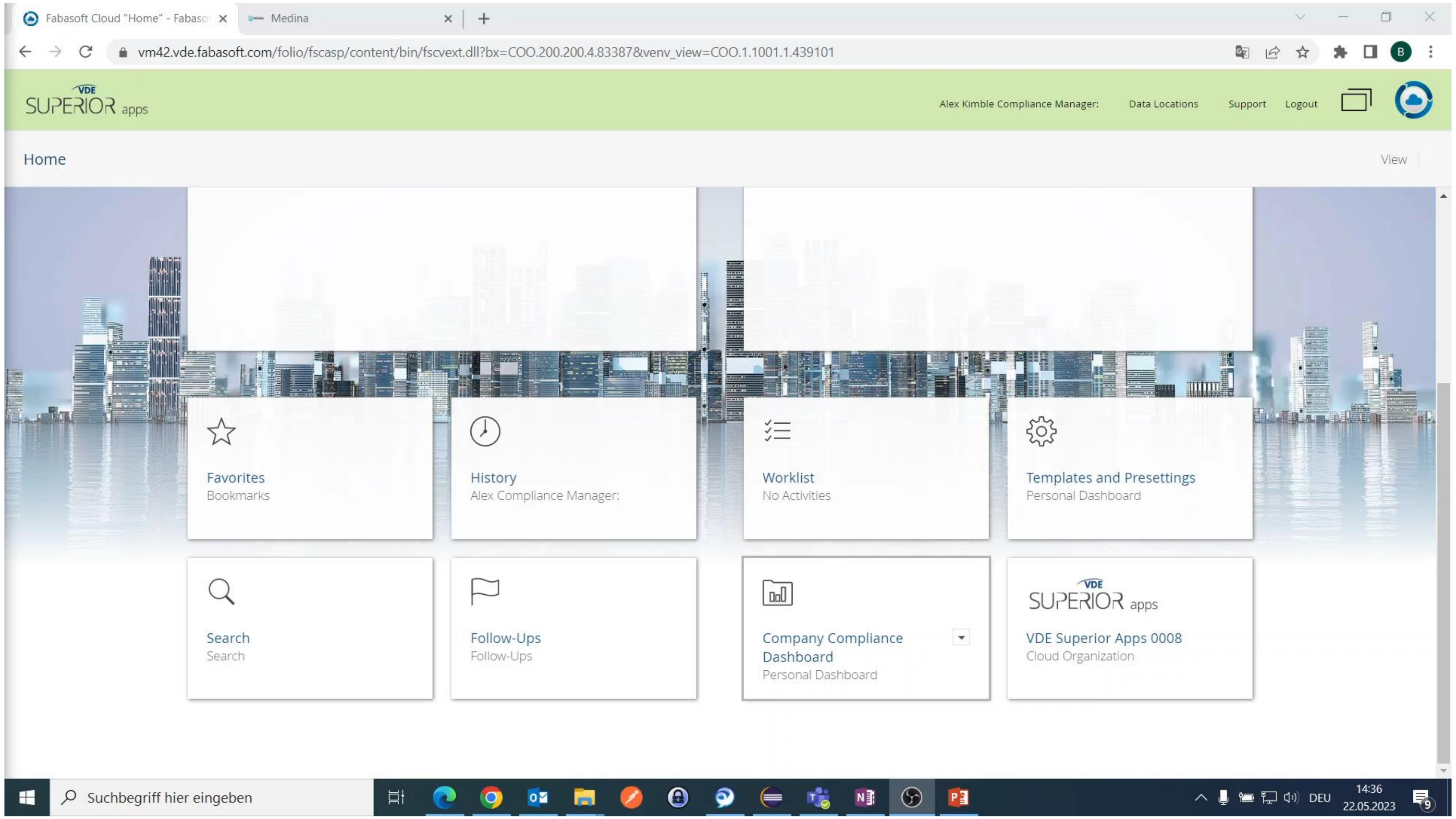
Cloud Services (0)

There are no entries in this list.

Upload Evidence Document

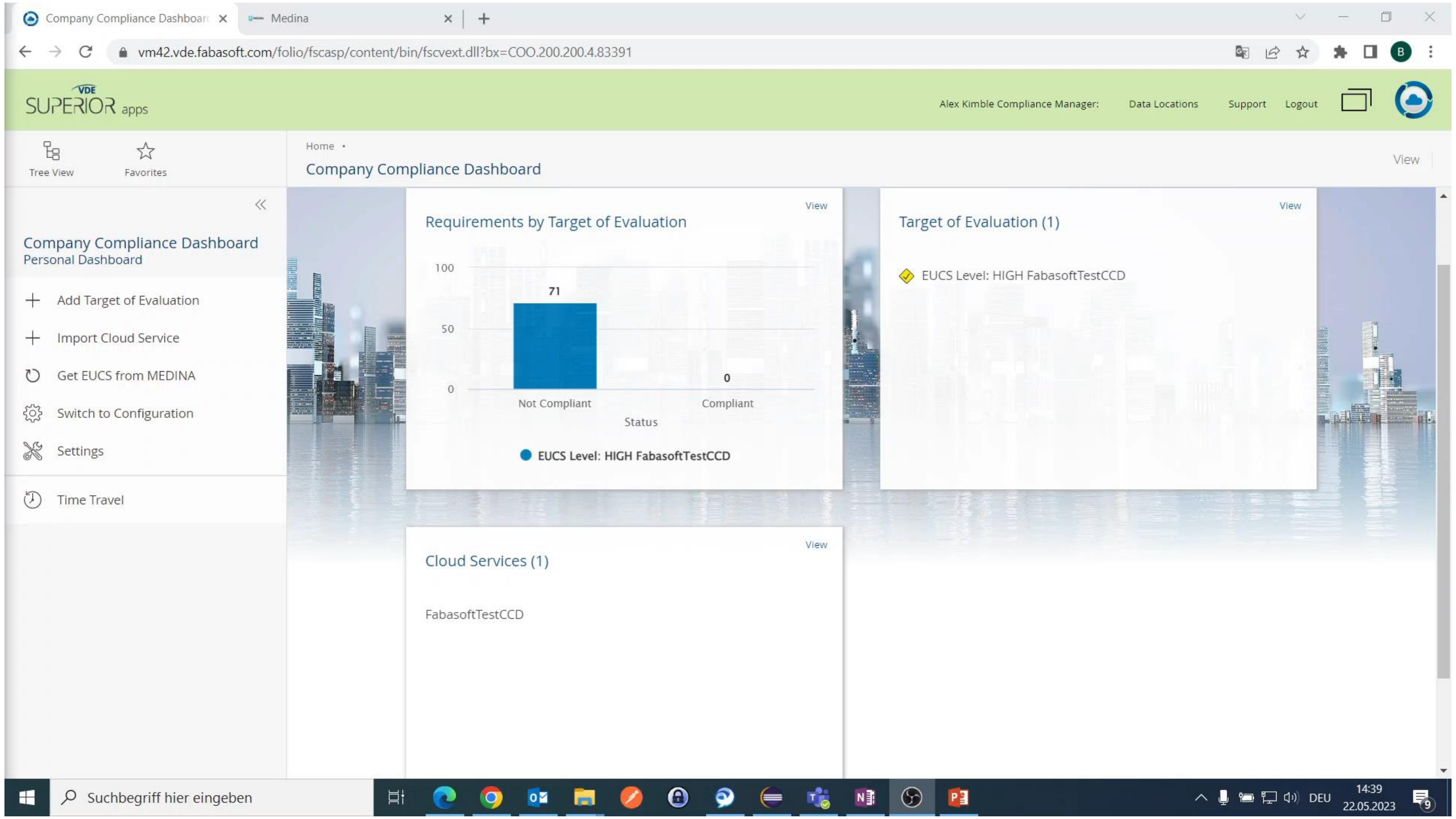


Create ToE



Fabasoft Cloud "Home" - Fabaso
Medina
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83387&venv_view=COO.1.1001.1.439101
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Home
View
Favorites
Bookmarks
History
Alex Compliance Manager:
Worklist
No Activities
Templates and Presettings
Personal Dashboard
Search
Search
Follow-Ups
Follow-Ups
Company Compliance Dashboard
Personal Dashboard
VDE SUPERIOR apps
VDE Superior Apps 0008
Cloud Organization
Suchbegriff hier eingeben
DEU
14:36
22.05.2023

Dashboard of ToE



Company Compliance Dashboard
Medina
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83391
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Tree View
Favorites
Home
View
Suchbegriff hier eingeben
DEU
14:39
22.05.2023

Company Compliance Dashboard

Personal Dashboard

- Add Target of Evaluation
- Import Cloud Service
- Get EUCS from MEDINA
- Switch to Configuration
- Settings
- Time Travel

Requirements by Target of Evaluation

100
50
0
71
0
Not Compliant
Compliant
Status
● EUCS Level: HIGH FabasoftTestCCD

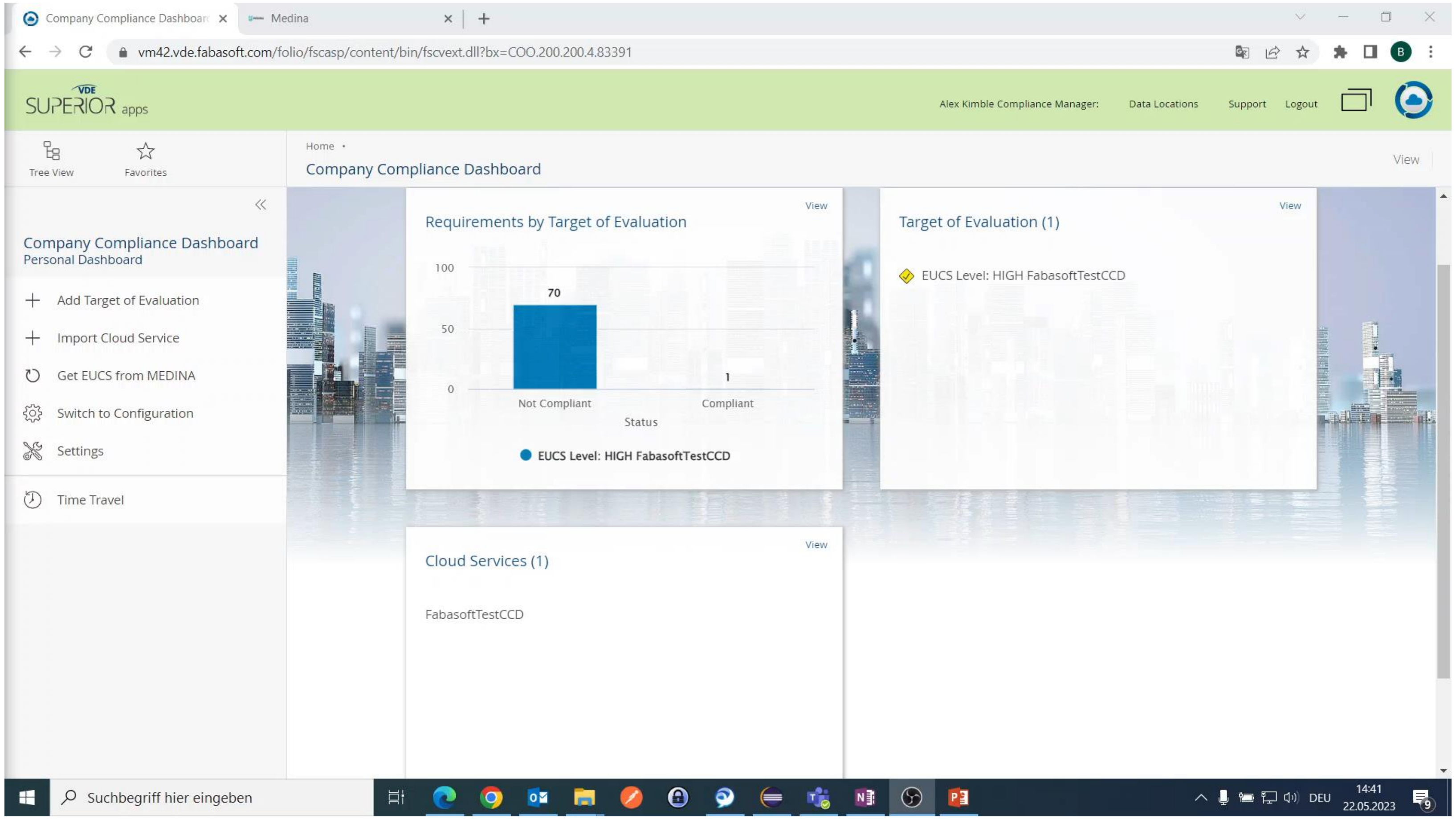
Target of Evaluation (1)

EUCS Level: HIGH FabasoftTestCCD

Cloud Services (1)

FabasoftTestCCD

ToE & Worklist



Company Compliance Dashboard

vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83391

Alex Kimble Compliance Manager: Data Locations Support Logout

Home •

Company Compliance Dashboard

Company Compliance Dashboard
Personal Dashboard

- Add Target of Evaluation
- Import Cloud Service
- Get EUCS from MEDINA
- Switch to Configuration
- Settings
- Time Travel

Requirements by Target of Evaluation

Target of Evaluation (1)

EUCS Level: HIGH FabasoftTestCCD

Cloud Services (1)

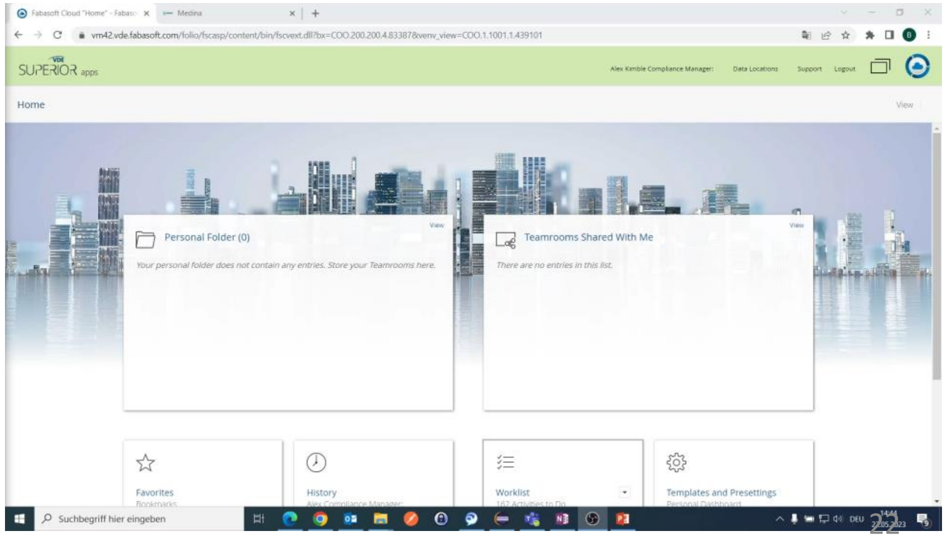
FabasoftTestCCD

Go to the risk assessment and show what can be done in the CCD

Use more slides/short videos if necessary

“could not get results from SATRA”

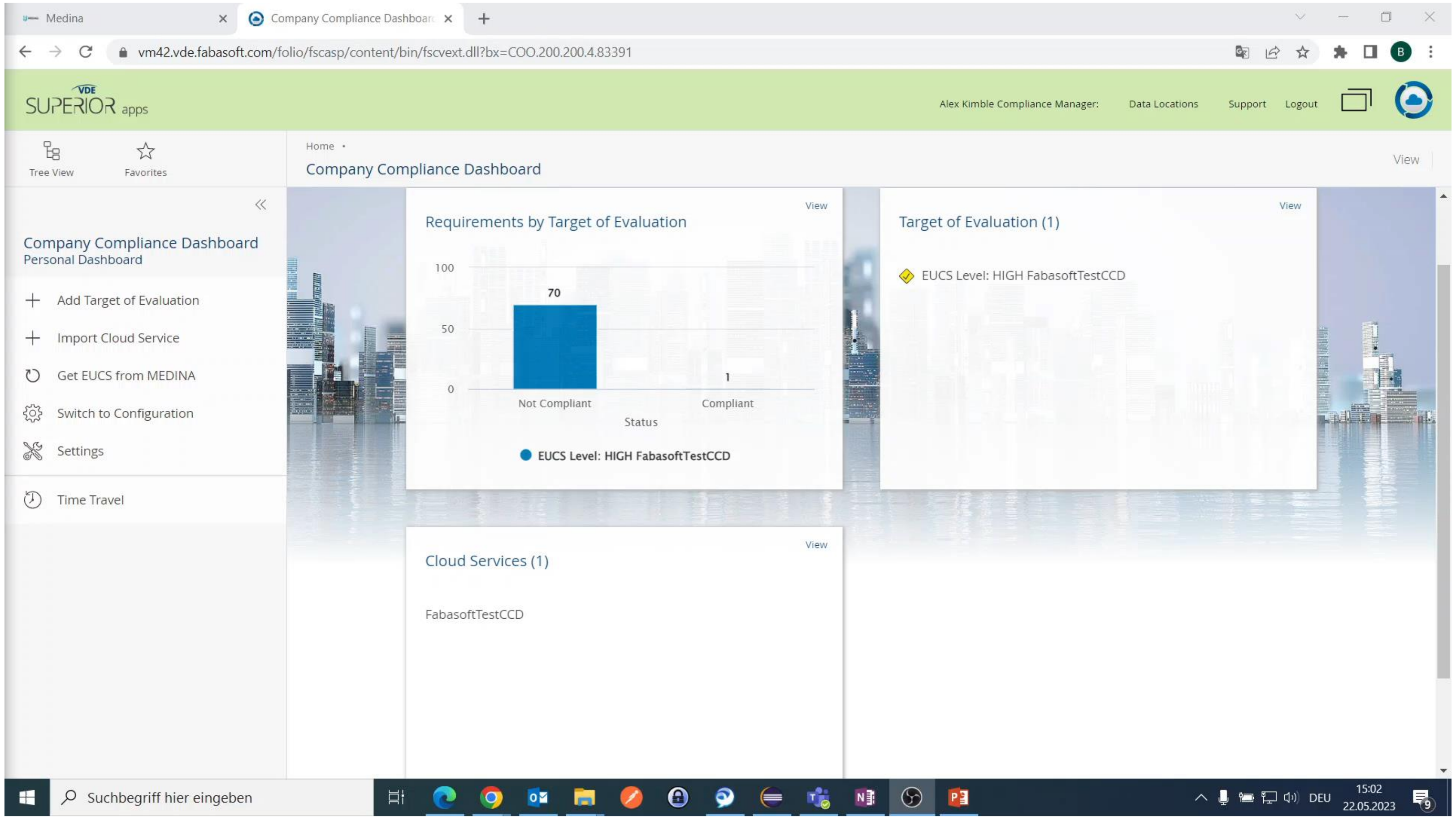
https://integrated-ui-dev.k8s.medina.esilab.org/satra


Fabasoft Cloud "Home" - Fabaso
Medina
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83387&venv_view=COO.1.1001.1.439101
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Home
View
Personal Folder (0)
View
Teamrooms Shared With Me
View
Favorites
Bookmarks
History
Alex Compliance Manager
Worklist
162 Activities to Do
Templates and Presettings
Personal Dashboard
Suchbegriff hier eingeben
DEU
14:44
22.05.2023

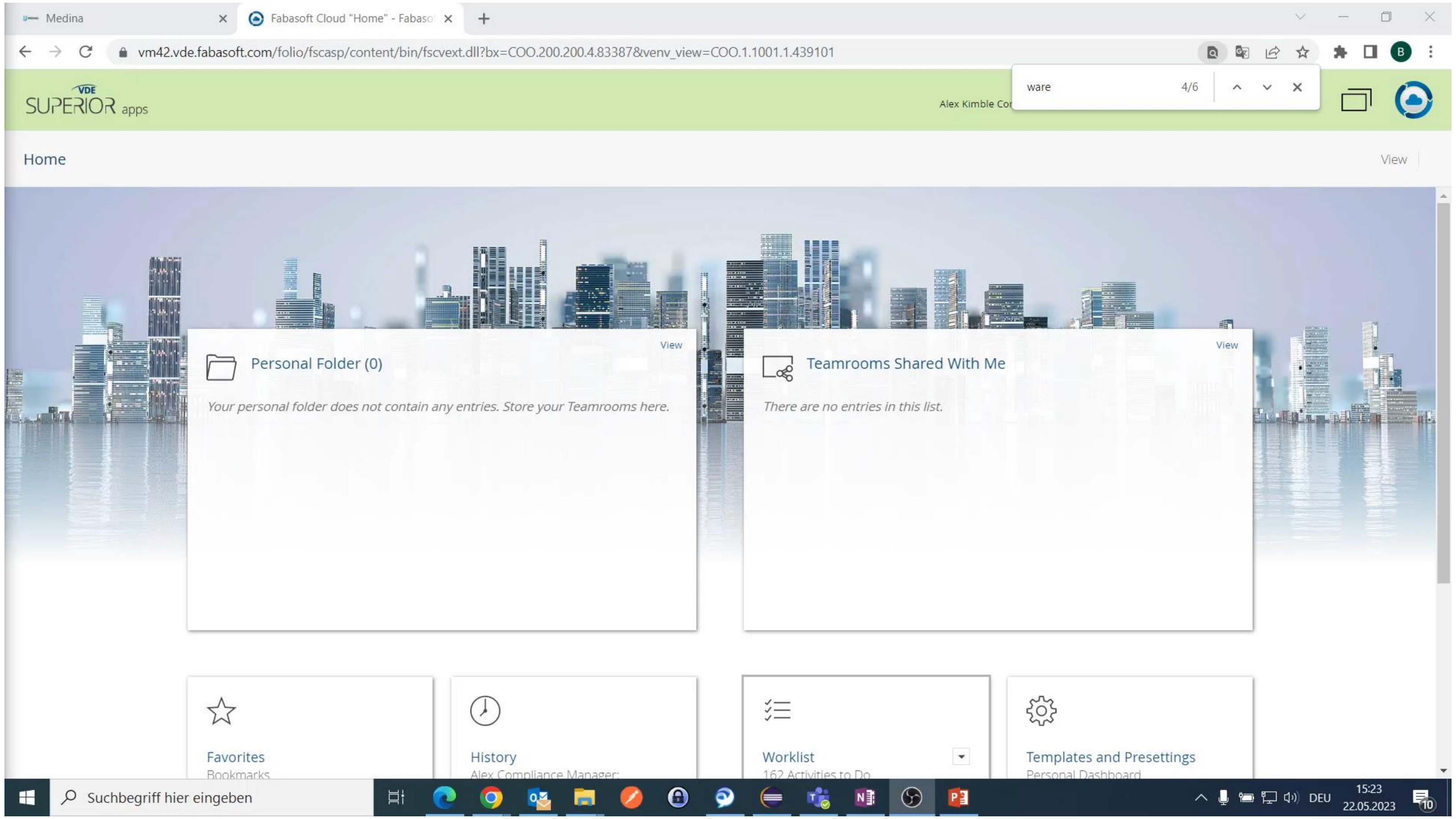
Your personal folder does not contain any entries. Store your Teamrooms here.

There are no entries in this list.

Metrics: Representation, search & state



Assign metric to owner

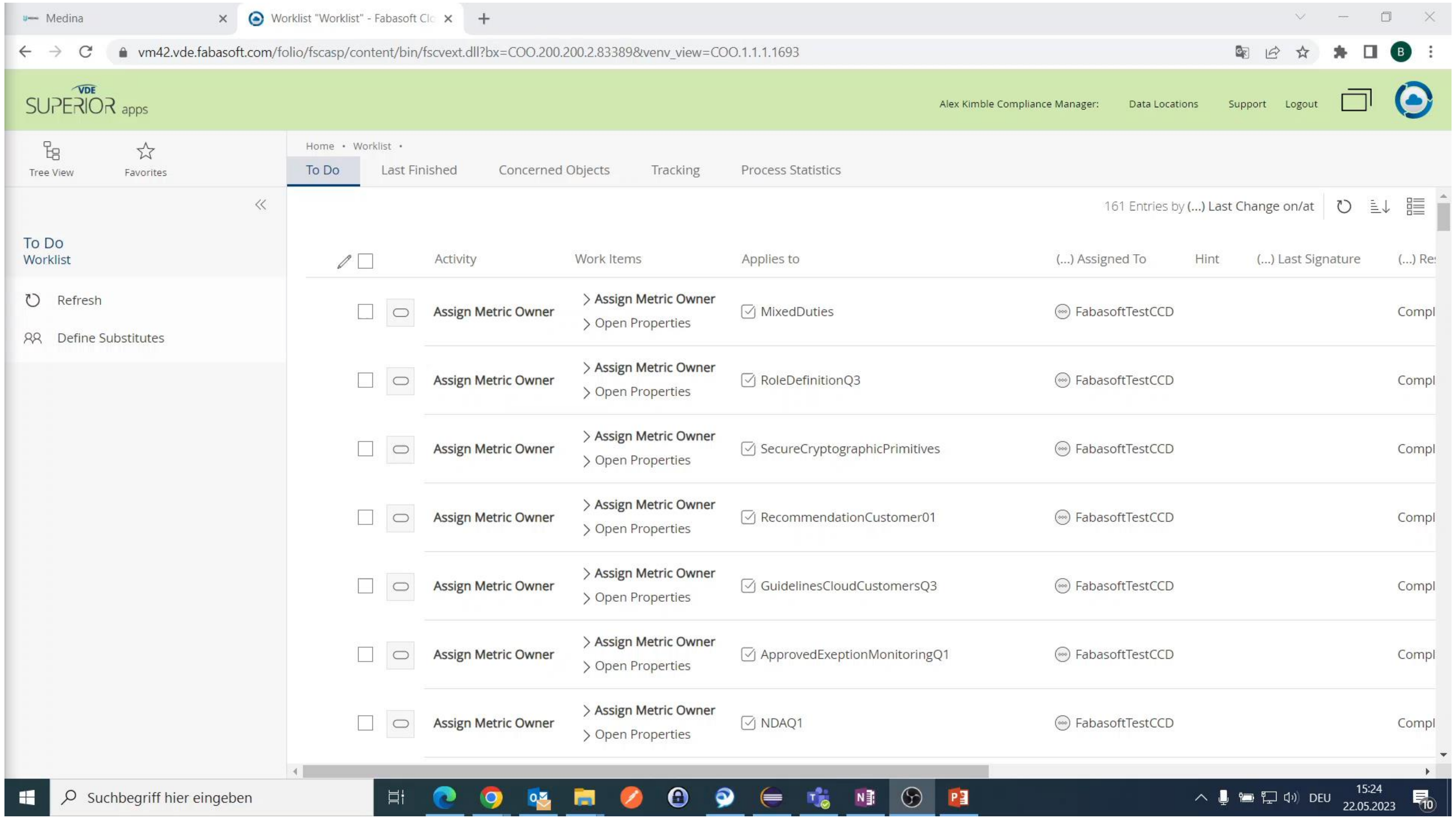


vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.83387&venv_view=COO.1.1001.1.439101

Your personal folder does not contain any entries. Store your Teamrooms here.

There are no entries in this list.

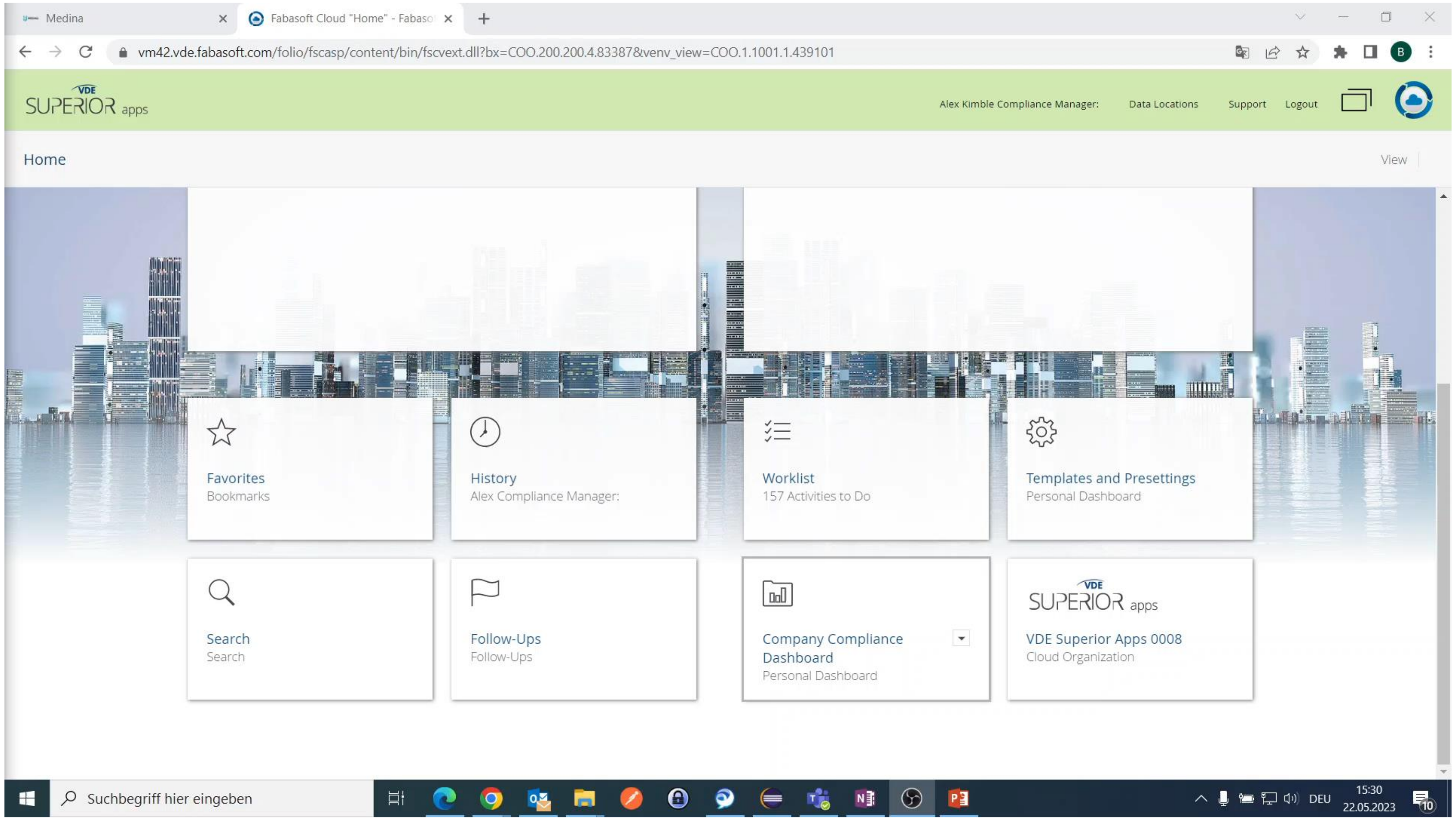
Assign several metrics to owner



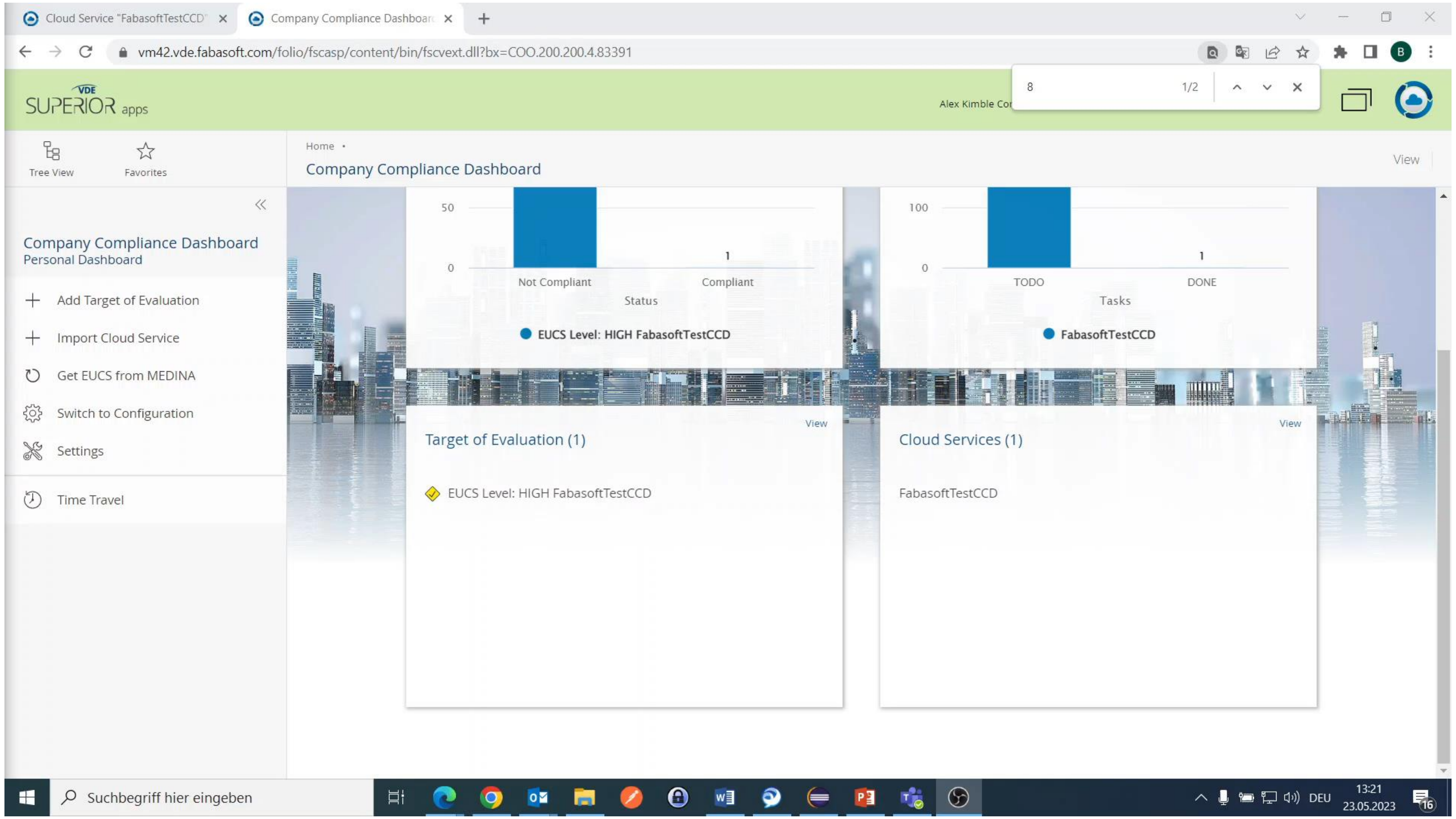
Medina
Worklist "Worklist" - Fabasoft Clo
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.2.83389&venv_view=COO.1.1.1.1693
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Tree View
Favorites
Home • Worklist •
To Do
Last Finished
Concerned Objects
Tracking
Process Statistics
To Do
Worklist
Refresh
Define Substitutes
161 Entries by (...) Last Change on/at
Suchbegriff hier eingeben
DEU
15:24
22.05.2023

□	Activity	Work Items	Applies to	(...) Assigned To	Hint	(...) Last Signature	(...) Re
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	MixedDuties	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	RoleDefinitionQ3	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	SecureCryptographicPrimitives	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	RecommendationCustomer01	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	GuidelinesCloudCustomersQ3	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	ApprovedExeptionMonitoringQ1	FabasoftTestCCD			Compl
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	NDAQ1	FabasoftTestCCD			Compl

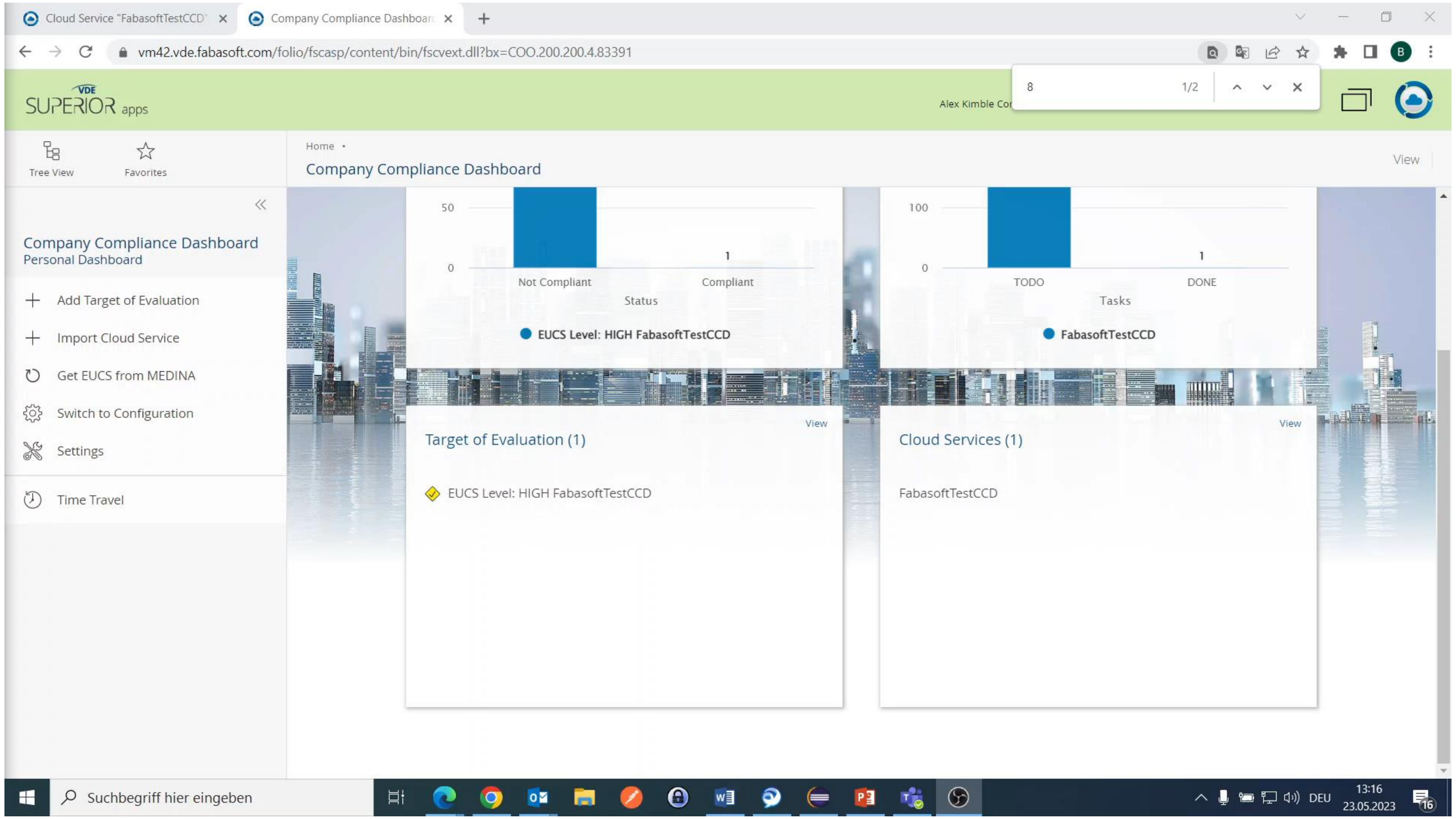
Assign metric to self as Owner & Implementer



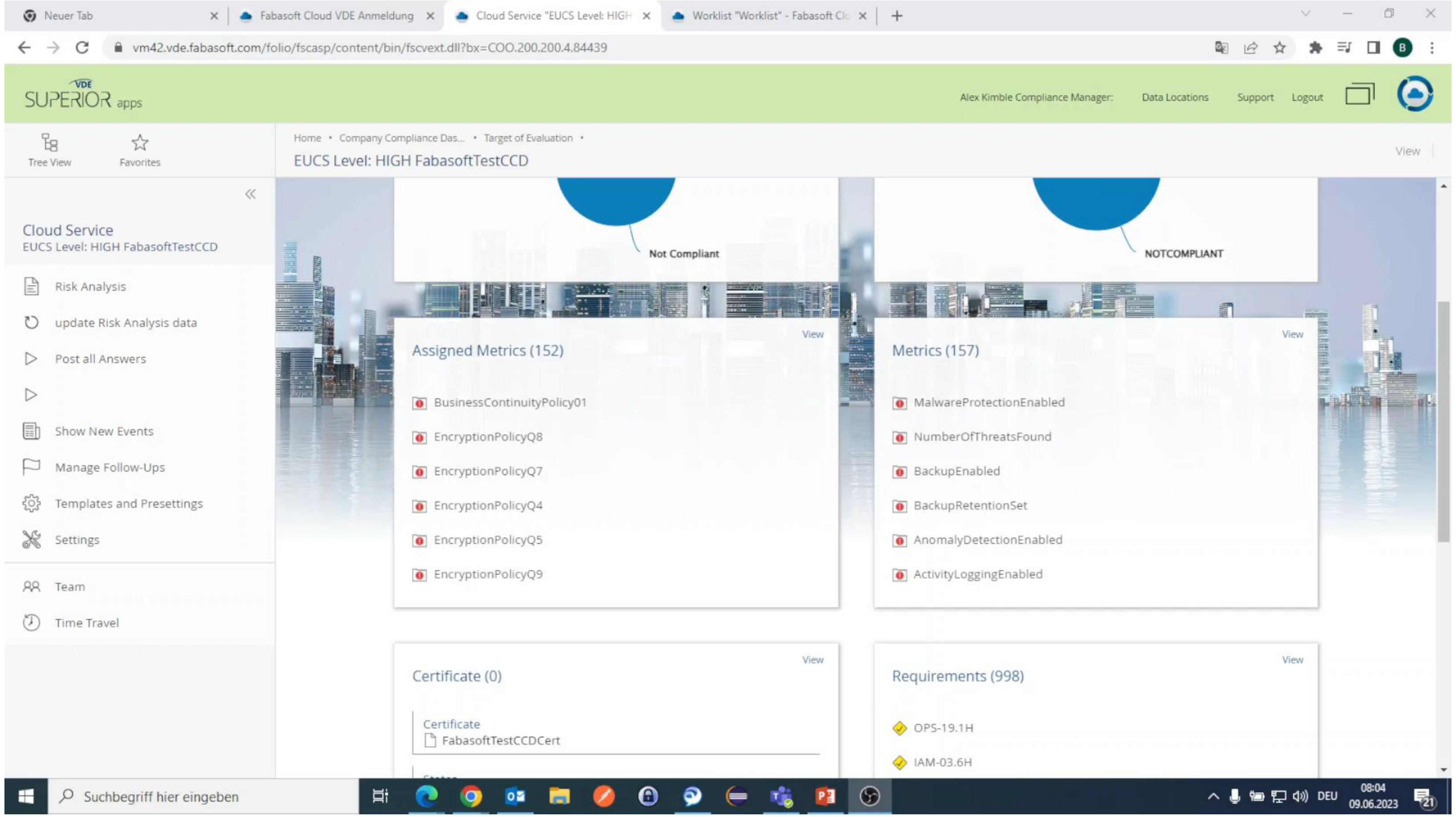
Get AMOE evidence for Metric



Set & Confirm AMOE Evidence



Show Metric implementation (self assignment)


Neuer Tab
Fabasoft Cloud VDE Anmeldung
Cloud Service "EUCS Level: HIGH
Worklist "Worklist" - Fabasoft Cl
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.84439
VDE SUPERIOR apps
Alex Kimble Compliance Manager:
Data Locations
Support
Logout
Tree View
Favorites
View
Suchbegriff hier eingeben
DEU
08:04
09.06.2023

Home • Company Compliance Das... • Target of Evaluation •

EUCS Level: HIGH FabasoftTestCCD

Cloud Service
EUCS Level: HIGH FabasoftTestCCD

- Risk Analysis
- update Risk Analysis data
- Post all Answers
- Show New Events
- Manage Follow-Ups
- Templates and Presettings
- Settings
- Team
- Time Travel

Not Compliant

NOTCOMPLIANT

Assigned Metrics (152) View

- BusinessContinuityPolicy01
- EncryptionPolicyQ8
- EncryptionPolicyQ7
- EncryptionPolicyQ4
- EncryptionPolicyQ5
- EncryptionPolicyQ9

Metrics (157) View

- MalwareProtectionEnabled
- NumberOfThreatsFound
- BackupEnabled
- BackupRetentionSet
- AnomalyDetectionEnabled
- ActivityLoggingEnabled

Certificate (0) View

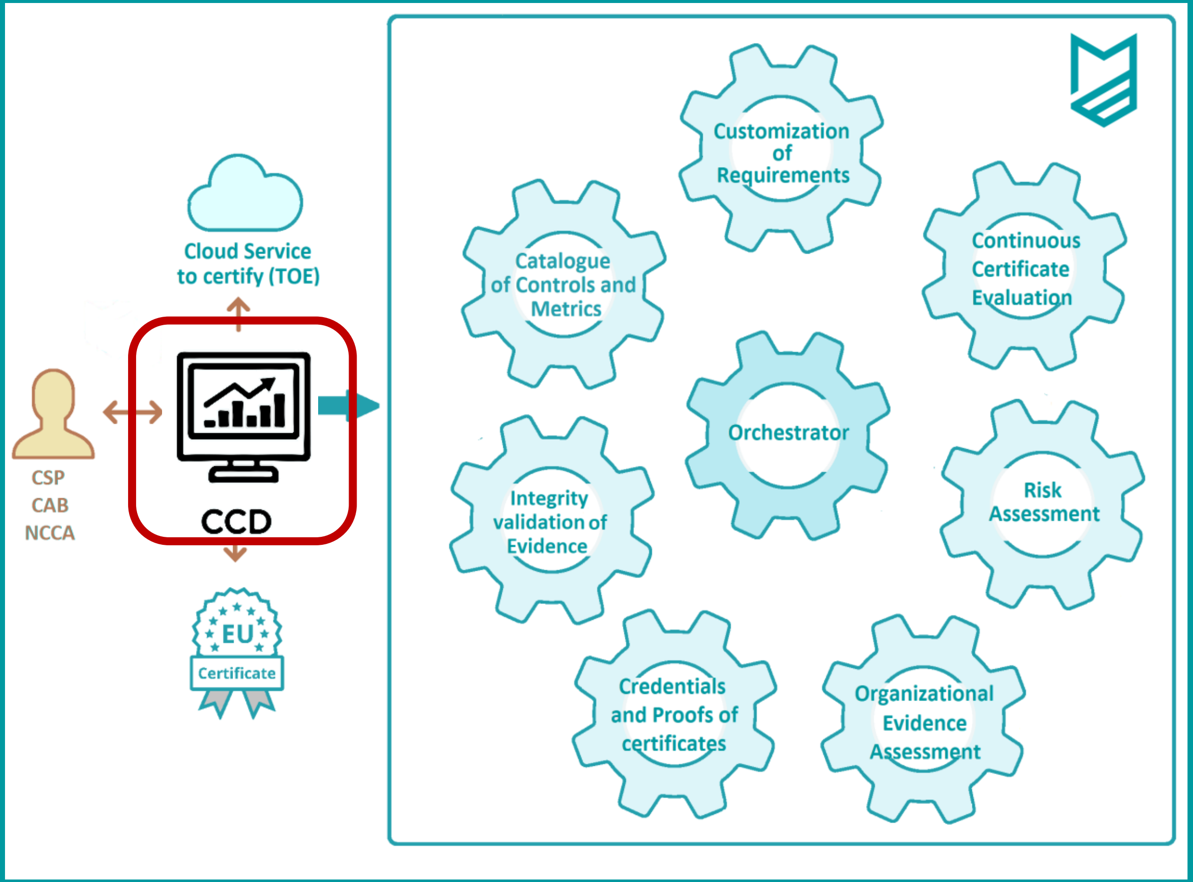
Certificate
FabasoftTestCCDCert

Requirements (998) View

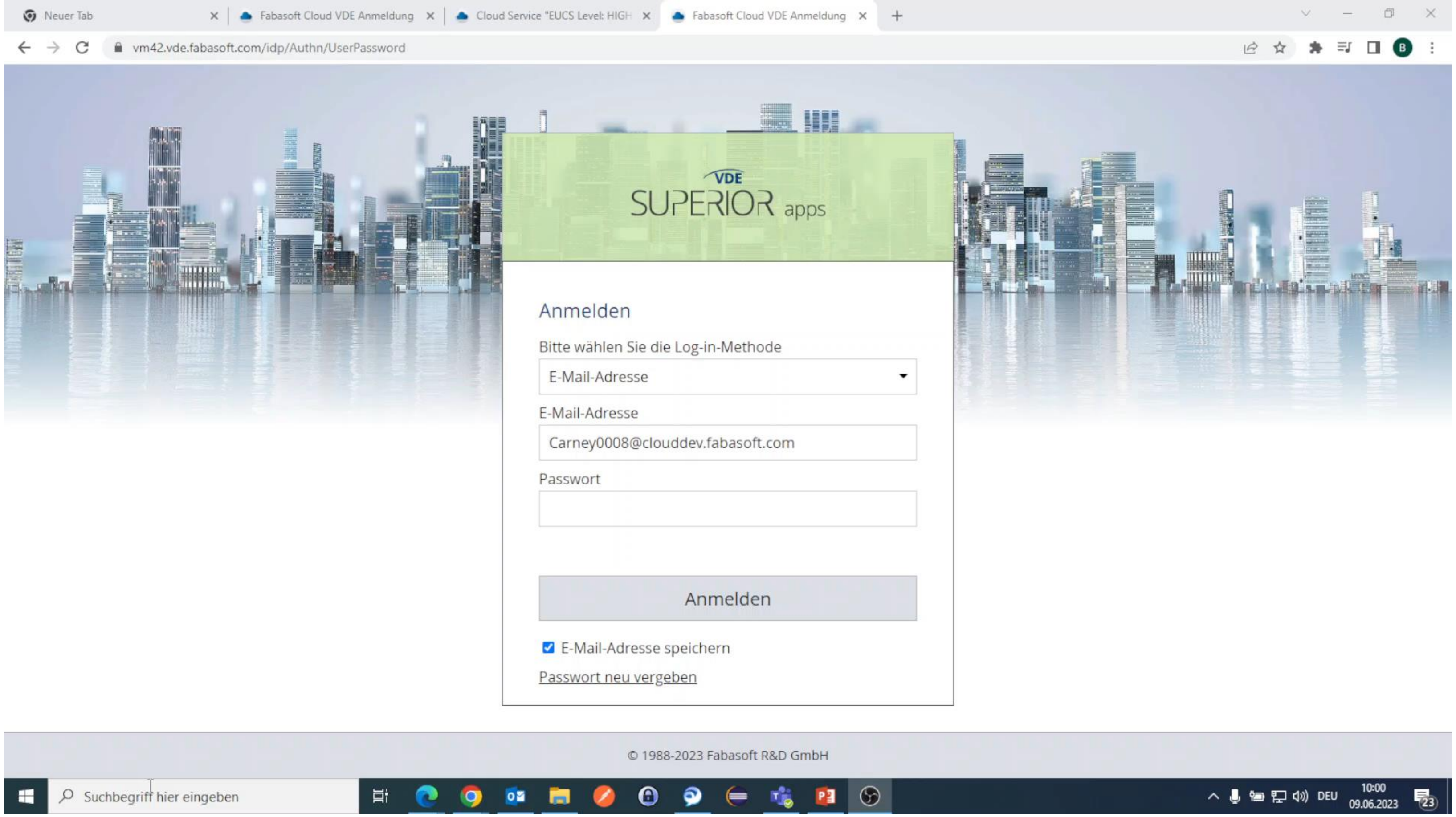
- OPS-19.1H
- IAM-03.6H

METRIC OWNER

RESPONSIBLE FOR IMPLEMENTATION OF A SET OF METRICS | ASSIGNS METRICS


Cloud Service to certify (TOE)
CSP
CAB
NCCA
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Switch to Metric Owner



Anmelden

Bitte wählen Sie die Log-in-Methode

E-Mail-Adresse

E-Mail-Adresse: Carney0008@clouddev.fabasoft.com

Passwort

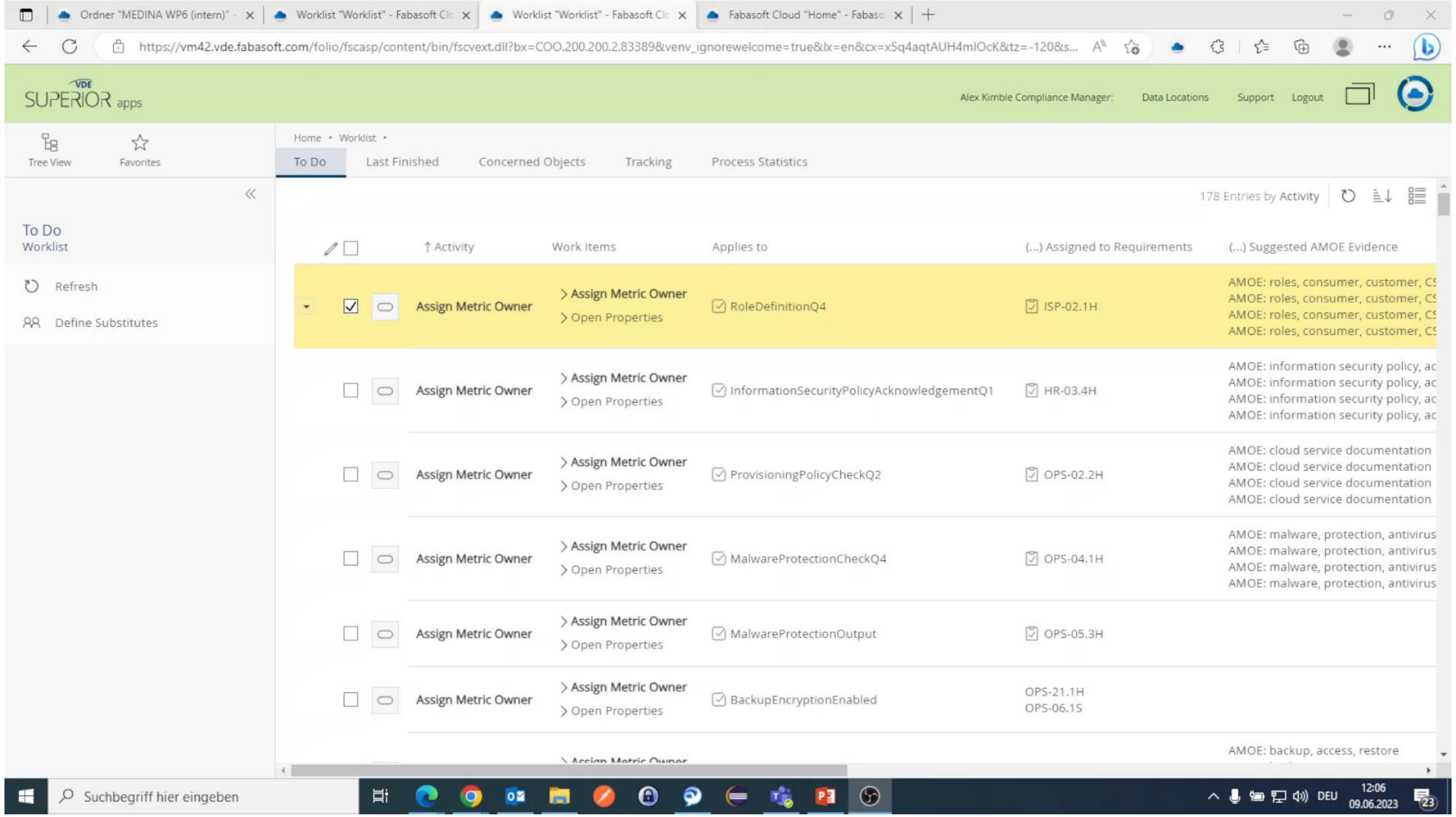
☑ E-Mail-Adresse speichern

Passwort neu vergeben

© 1988-2023 Fabasoft R&D GmbH

Neuer Tab
Fabasoft Cloud VDE Anmeldung
Cloud Service "EUCS Level: HIGH
Fabasoft Cloud VDE Anmeldung
vm42.vde.fabasoft.com/idp/Authn/UserPassword
VDE
SUPERIOR apps
Anmelden
Suchbegriff hier eingeben
DEU
10:00
09.06.2023

Accept and Assign Metric Implementer



Ordner "MEDINA WP6 (intern)" · Worklist "Worklist" - Fabasoft Cl · Worklist "Worklist" - Fabasoft Cl · Fabasoft Cloud "Home" - Fabaso

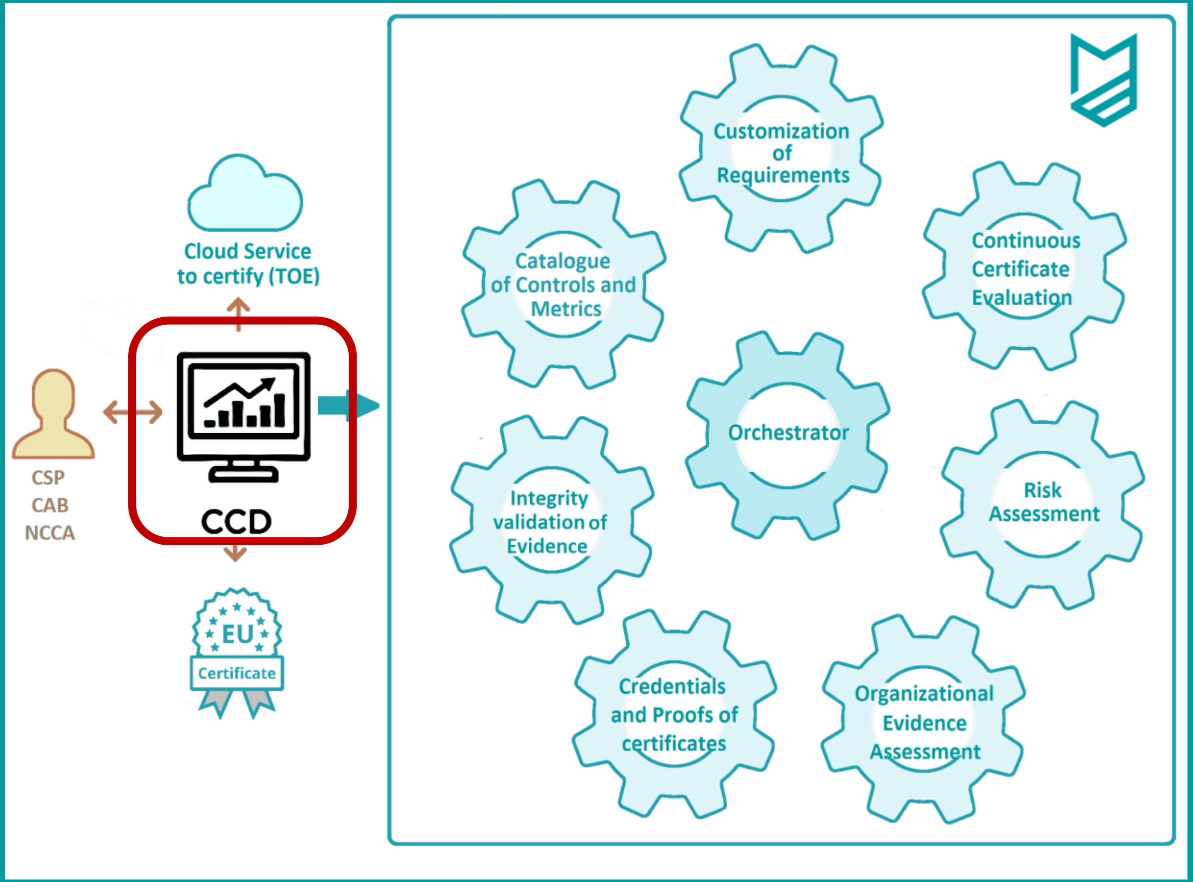
https://vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.2.83389&venv_ignorewelcome=true&lx=en&cx=x5q4aqtAUH4mlOcK&tz=-120&s...

□	↑ Activity	Work Items	Applies to	(...) Assigned to Requirements	(...) Suggested AMOE Evidence
☑	Assign Metric Owner	> Assign Metric Owner > Open Properties	RoleDefinitionQ4	ISP-02.1H	AMOE: roles, consumer, customer, CS AMOE: roles, consumer, customer, CS AMOE: roles, consumer, customer, CS AMOE: roles, consumer, customer, CS
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	InformationSecurityPolicyAcknowledgementQ1	HR-03.4H	AMOE: information security policy, ac AMOE: information security policy, ac AMOE: information security policy, ac AMOE: information security policy, ac
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	ProvisioningPolicyCheckQ2	OPS-02.2H	AMOE: cloud service documentation AMOE: cloud service documentation AMOE: cloud service documentation AMOE: cloud service documentation
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	MalwareProtectionCheckQ4	OPS-04.1H	AMOE: malware, protection, antivirus AMOE: malware, protection, antivirus AMOE: malware, protection, antivirus AMOE: malware, protection, antivirus
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	MalwareProtectionOutput	OPS-05.3H	
□	Assign Metric Owner	> Assign Metric Owner > Open Properties	BackupEncryptionEnabled	OPS-21.1H OPS-06.1S	
		> Assign Metric Owner			AMOE: backup, access, restore

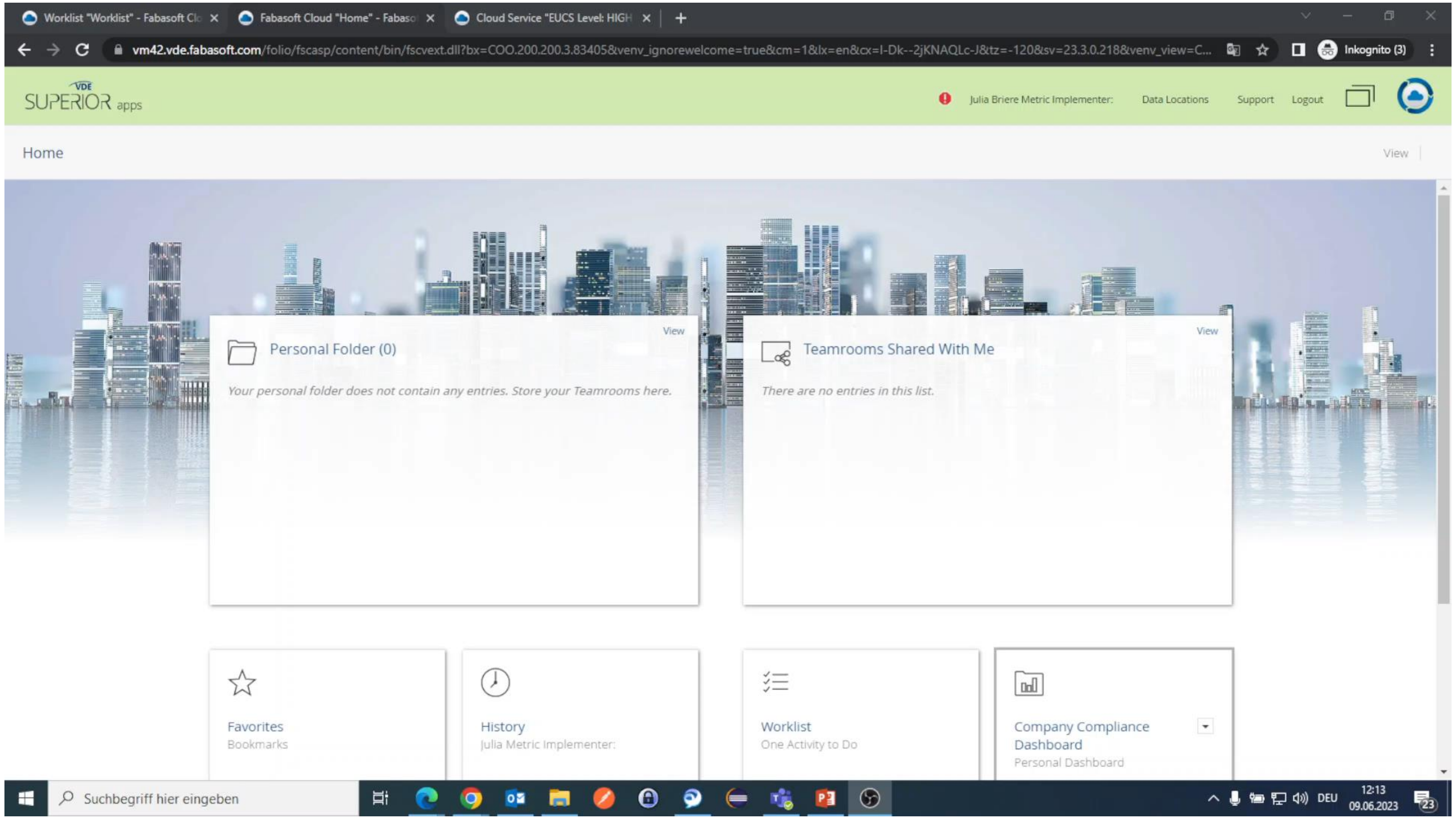
MEDINA

METRIC IMPLEMENTER

IMPLEMENTS METRICS


Cloud Service
to certify (TOE)
CSP
CAB
NCCA
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Accept implementation

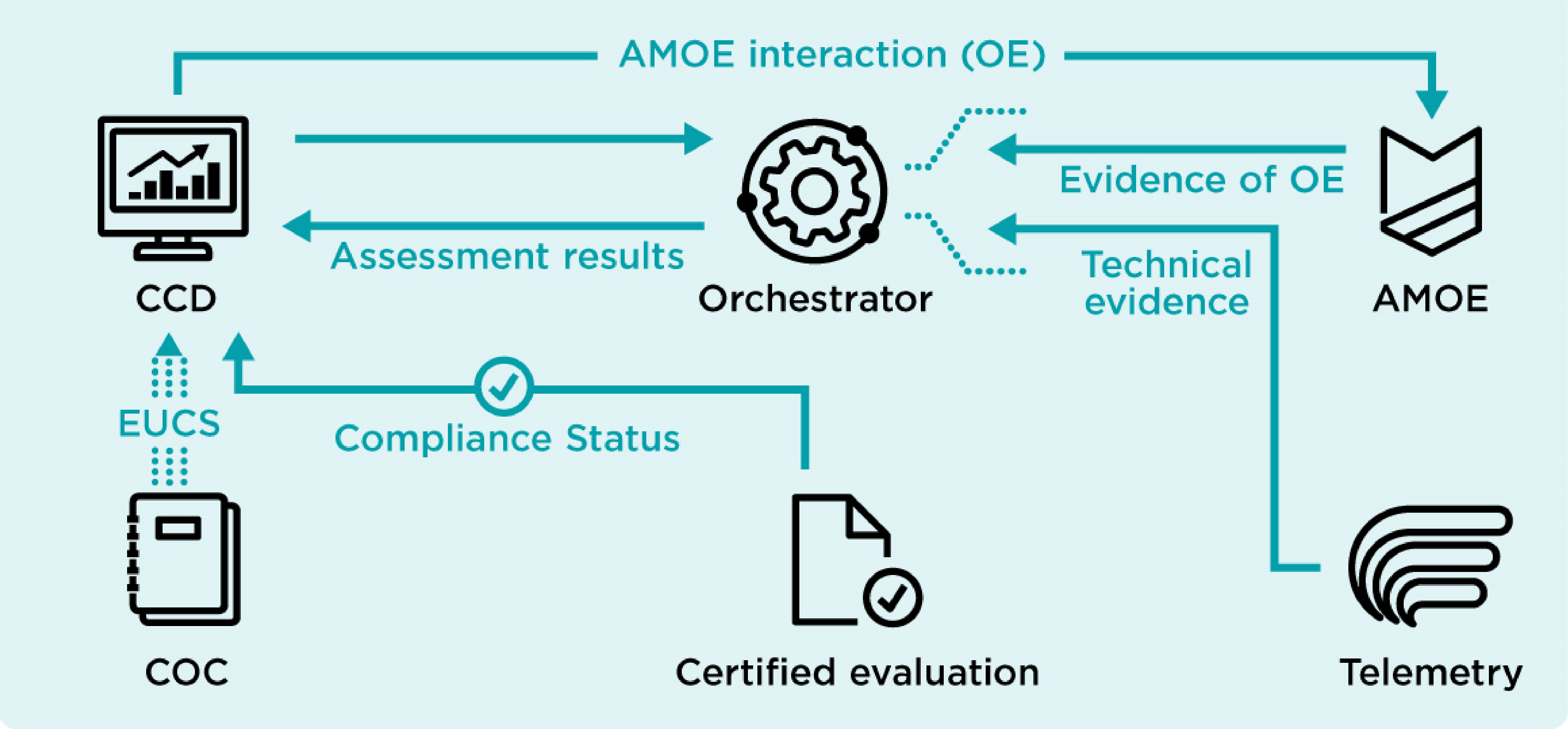


Worklist "Worklist" - Fabasoft Clo
Fabasoft Cloud "Home" - Fabaso
Cloud Service "EUCS Level: HIGH
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.3.83405&venv_ignorewelcome=true&cm=1&lx=en&cx=I-Dk--2jKNAQLc-J&tz=-120&sv=23.3.0.218&venv_view=C...
Inkognito (3)
VDE SUPERIOR apps
Julia Briere Metric Implementer:
Data Locations
Support
Logout
Home
View
Personal Folder (0)
View
Teamrooms Shared With Me
View
Favorites
Bookmarks
History
Julia Metric Implementer:
Worklist
One Activity to Do
Company Compliance Dashboard
Personal Dashboard
Suchbegriff hier eingeben
DEU
12:13
09.06.2023

Your personal folder does not contain any entries. Store your Teamrooms here.

There are no entries in this list.

3 STANDARDIZED AUDIT



AMOE interaction (OE)

Evidence of OE

Assessment results

Technical evidence

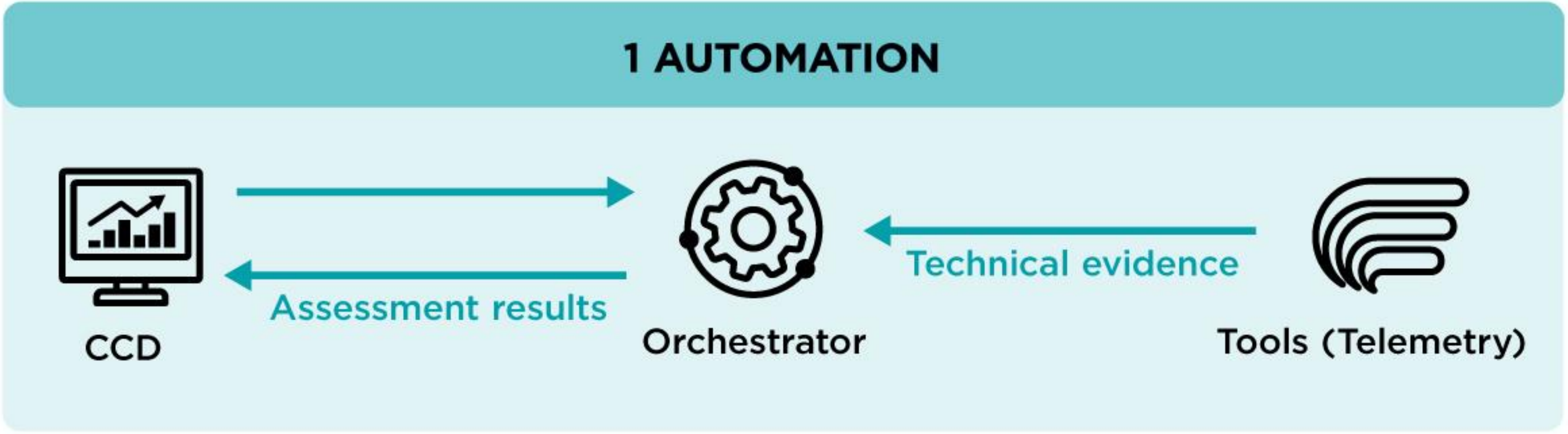
Compliance Status

EUCS

CCD	Company Compliance Dashboard
OE	Organizational Evidence
TE	Technical Evidence
CoC	Catalogue of Controls
ToE	Target of Evaluation

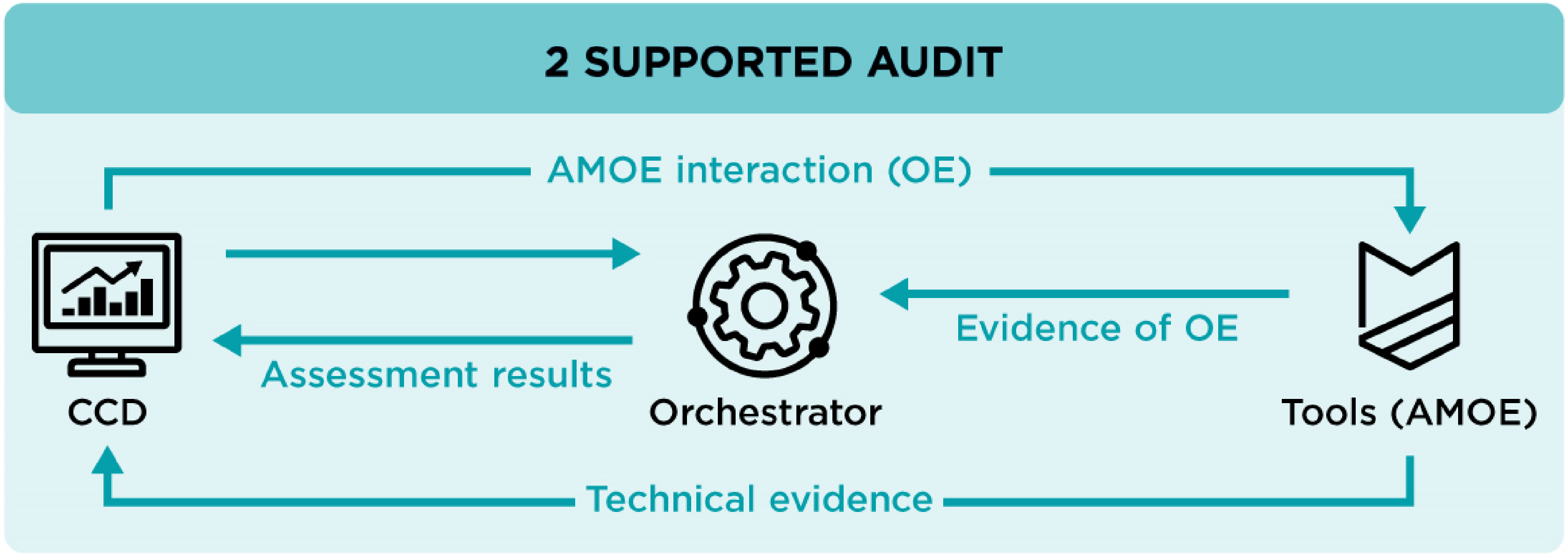
AMOE	Tool to Automatically Extract and Assess Organizational Evidence for Continuous Cloud Audit
⋮	One Pipeline for OE and TE
⠿	Fixed structure for each Catalogue
✓	Compliance Information based on whole ToE context

Audit Automation



CCD Company Compliance Dashboard

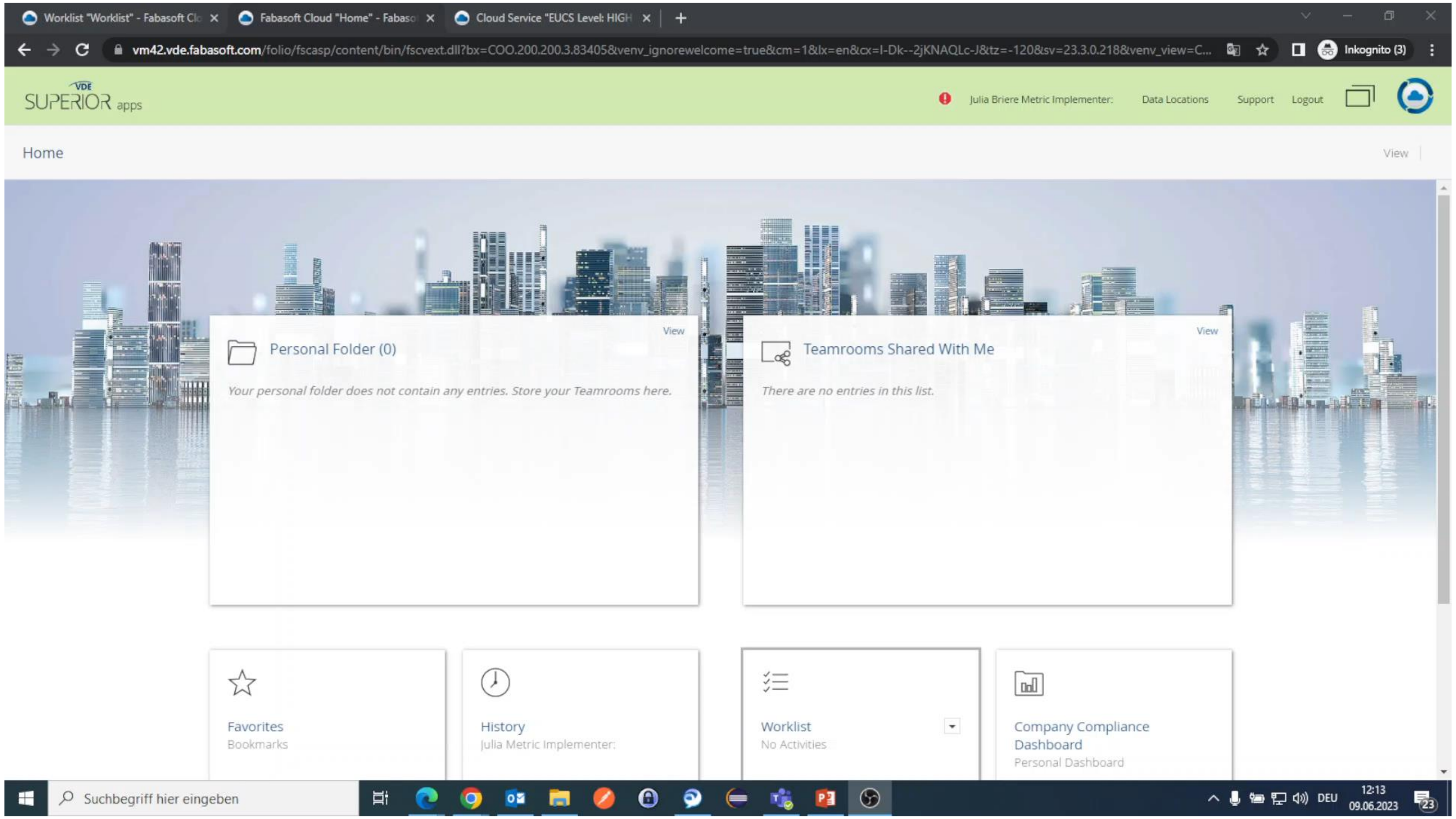
Supported Audit



CCD Company Compliance Dashboard

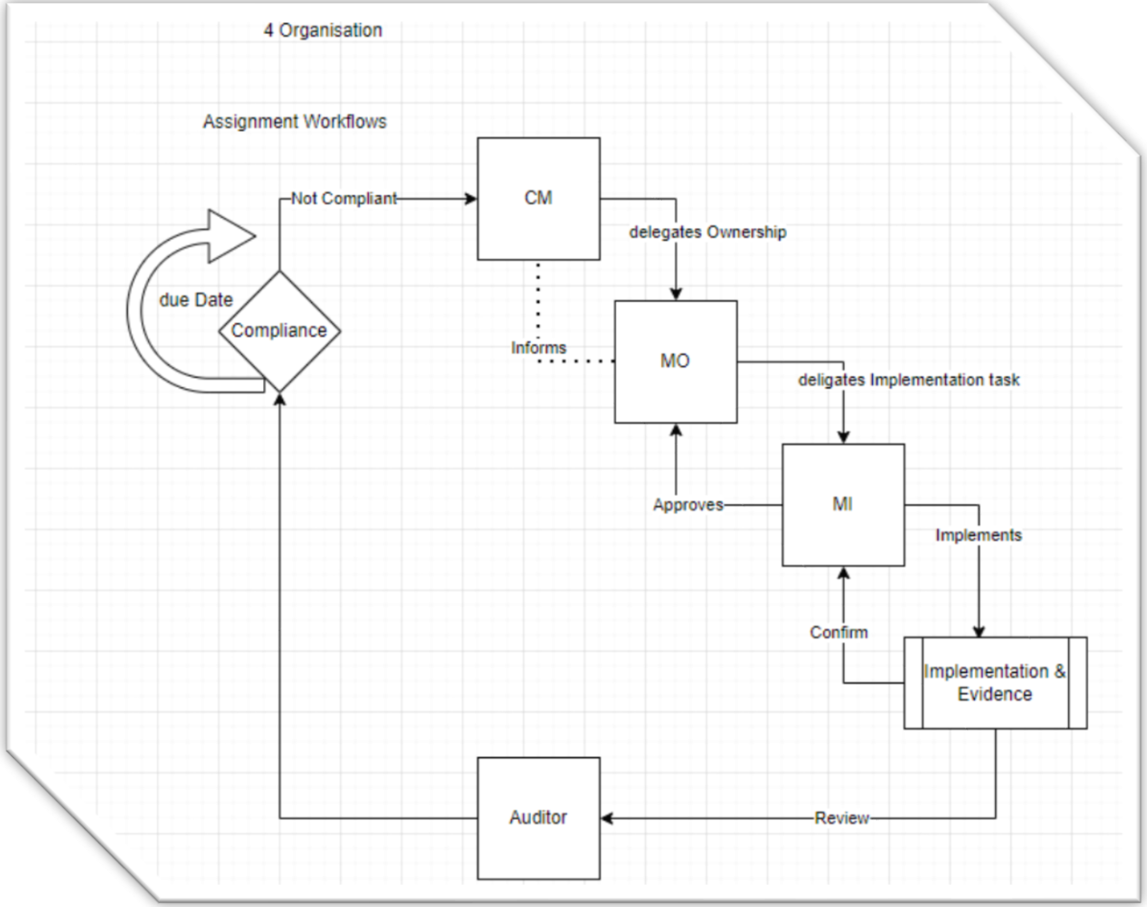
AMOE Tool to Automatically Extract and Assess Organizational Evidence for Continuous Cloud Audit

Implement metric

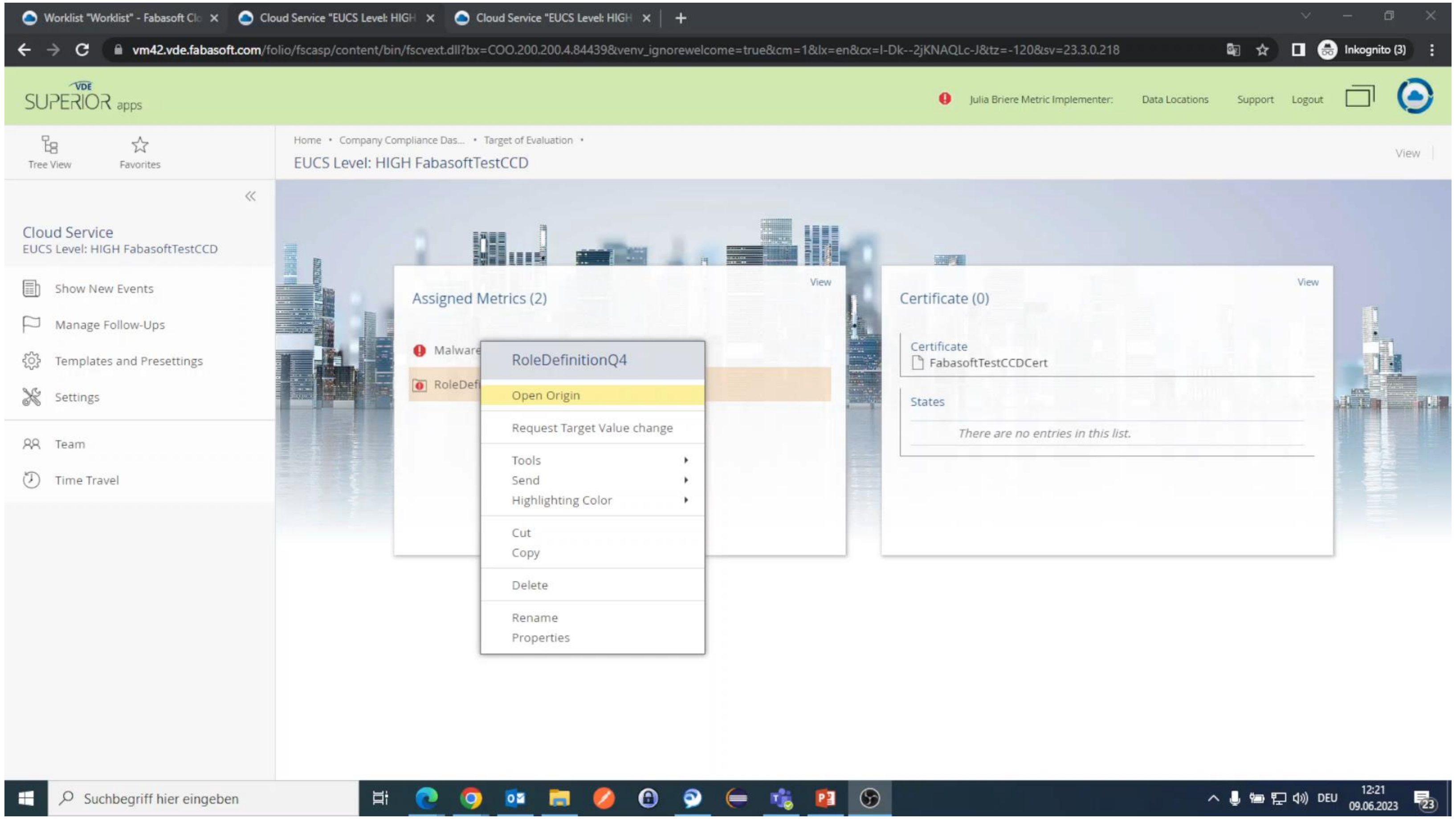

Worklist "Worklist" - Fabasoft Cl
Fabasoft Cloud "Home" - Fabaso
Cloud Service "EUCS Level: HIGH
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.3.83405&venv_ignorewelcome=true&cm=1&lx=en&cx=l-Dk--2jKNAQLc-J&tz=-120&sv=23.3.0.218&venv_view=C...
Inkognito (3)
VDE SUPERIOR apps
Julia Briere Metric Implementer:
Data Locations
Support
Logout
Home
View
Personal Folder (0)
View
Your personal folder does not contain any entries. Store your Teamrooms here.
Teamrooms Shared With Me
View
There are no entries in this list.
Favorites
Bookmarks
History
Julia Metric Implementer:
Worklist
No Activities
Company Compliance Dashboard
Personal Dashboard
Suchbegriff hier eingeben
DEU
12:13
09.06.2023

Inspect Implementation

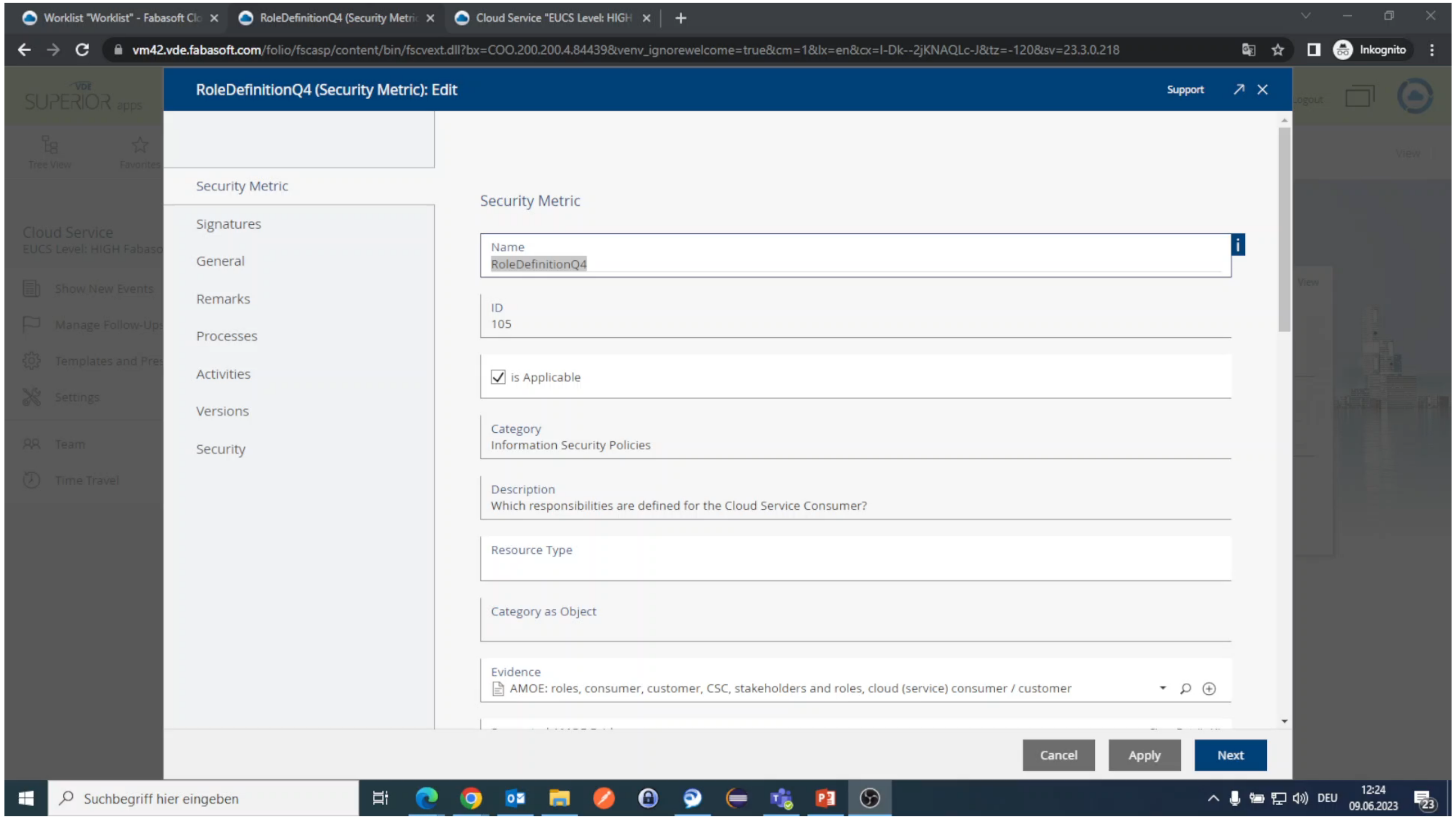
- Review and Release Metric Implementation



Release by Metric Owner


Worklist "Worklist" - Fabasoft Clo
Cloud Service "EUCS Level: HIGH
Cloud Service "EUCS Level: HIGH
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.84439&venv_ignorewelcome=true&cm=1&lx=en&cx=I-Dk--2jKNAQLc-J&tz=-120&sv=23.3.0.218
Inkognito (3)
VDE SUPERIOR apps
Julia Briere Metric Implementer:
Data Locations
Support
Logout
Tree View
Favorites
Home • Company Compliance Das... • Target of Evaluation •
EUCS Level: HIGH FabasoftTestCCD
View
Cloud Service
EUCS Level: HIGH FabasoftTestCCD
Show New Events
Manage Follow-Ups
Templates and Presettings
Settings
Team
Time Travel
Assigned Metrics (2)
View
Malware
RoleDef
RoleDefinitionQ4
Open Origin
Request Target Value change
Tools
Send
Highlighting Color
Cut
Copy
Delete
Rename
Properties
Certificate (0)
View
Certificate
FabasoftTestCCDCert
States
There are no entries in this list.
Suchbegriff hier eingeben
DEU
12:21
09.06.2023

Confirm by Compliance Manager



vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.4.84439&venv_ignorewelcome=true&cm=1&lx=en&cx=I-Dk--2jKNAQLc-J&tz=-120&sv=23.3.0.218

RoleDefinitionQ4 (Security Metric): Edit

Security Metric

Name
RoleDefinitionQ4

ID
105

☑ is Applicable

Category
Information Security Policies

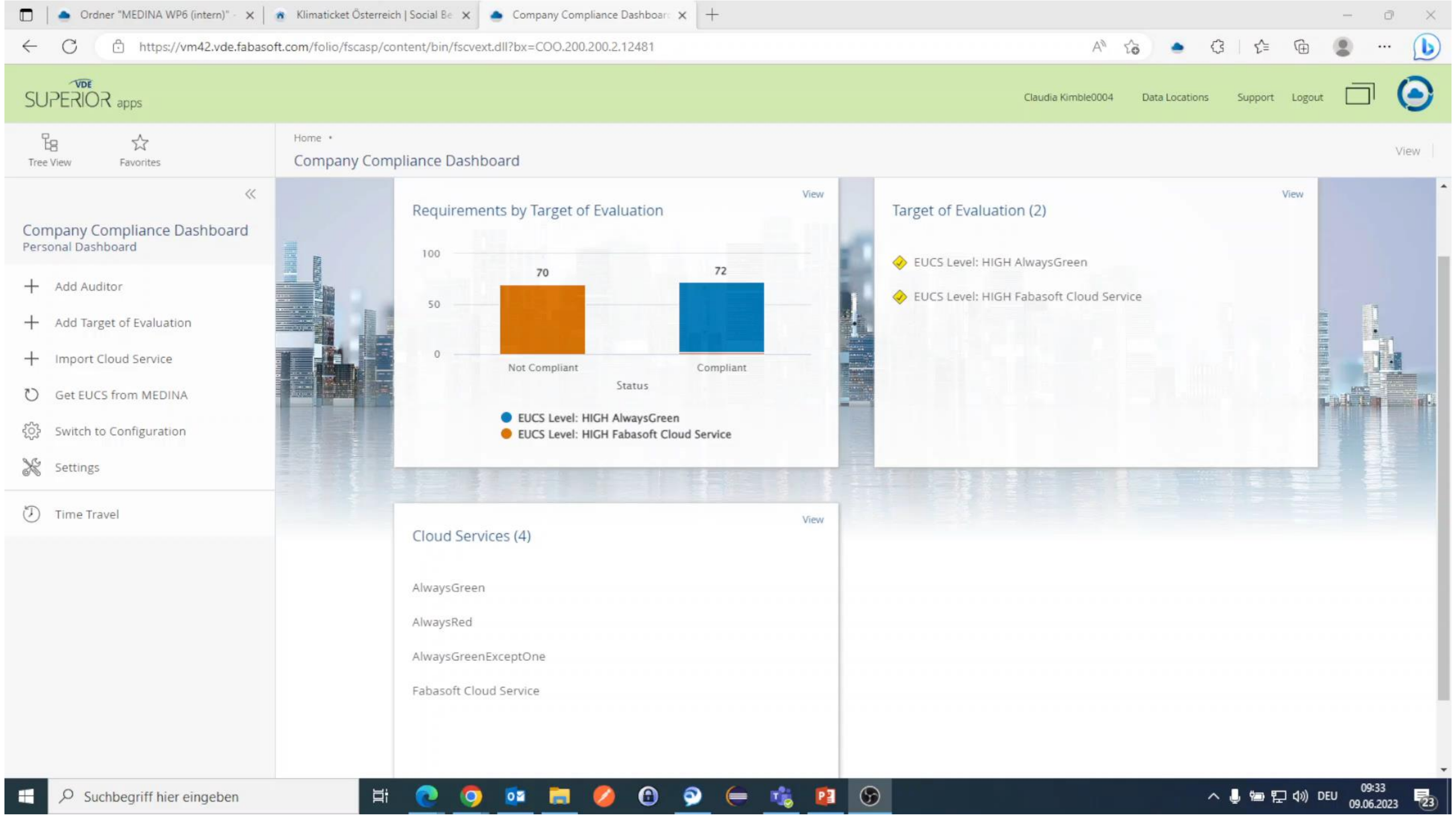
Description
Which responsibilities are defined for the Cloud Service Consumer?

Resource Type

Category as Object

Evidence
AMOE: roles, consumer, customer, CSC, stakeholders and roles, cloud (service) consumer / customer

Statusicons



Company Compliance Dashboard

Company Compliance Dashboard
Personal Dashboard

Requirements by Target of Evaluation

- ● EUCS Level: HIGH AlwaysGreen
- ● EUCS Level: HIGH Fabasoft Cloud Service

Target of Evaluation (2)

- EUCS Level: HIGH AlwaysGreen
- EUCS Level: HIGH Fabasoft Cloud Service

Cloud Services (4)

AlwaysGreen

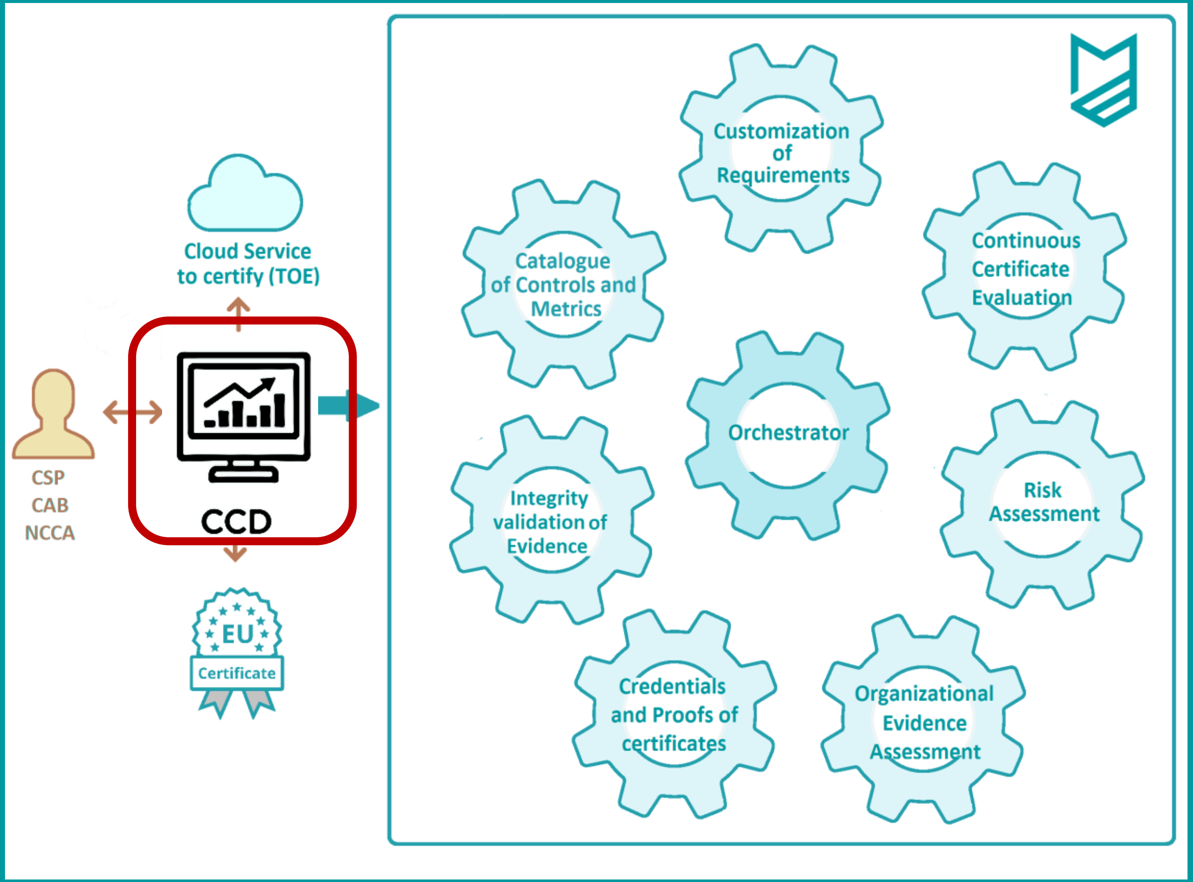
AlwaysRed

AlwaysGreenExceptOne

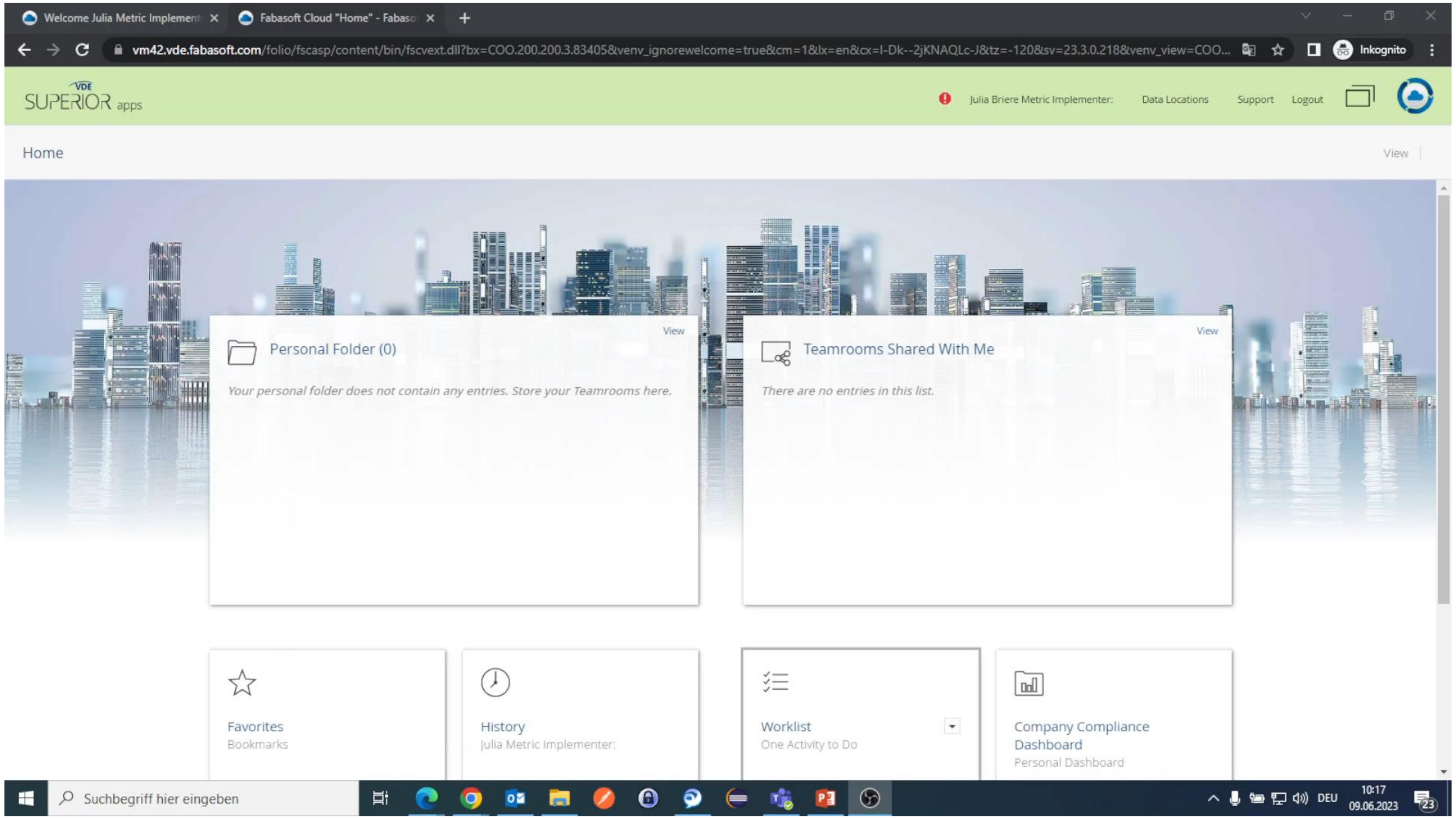
Fabasoft Cloud Service

Re-Assignments

Reject and Redirect Tasks


Cloud Service to certify (TOE)
CSP
CAB
NCCA
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Decline ownership

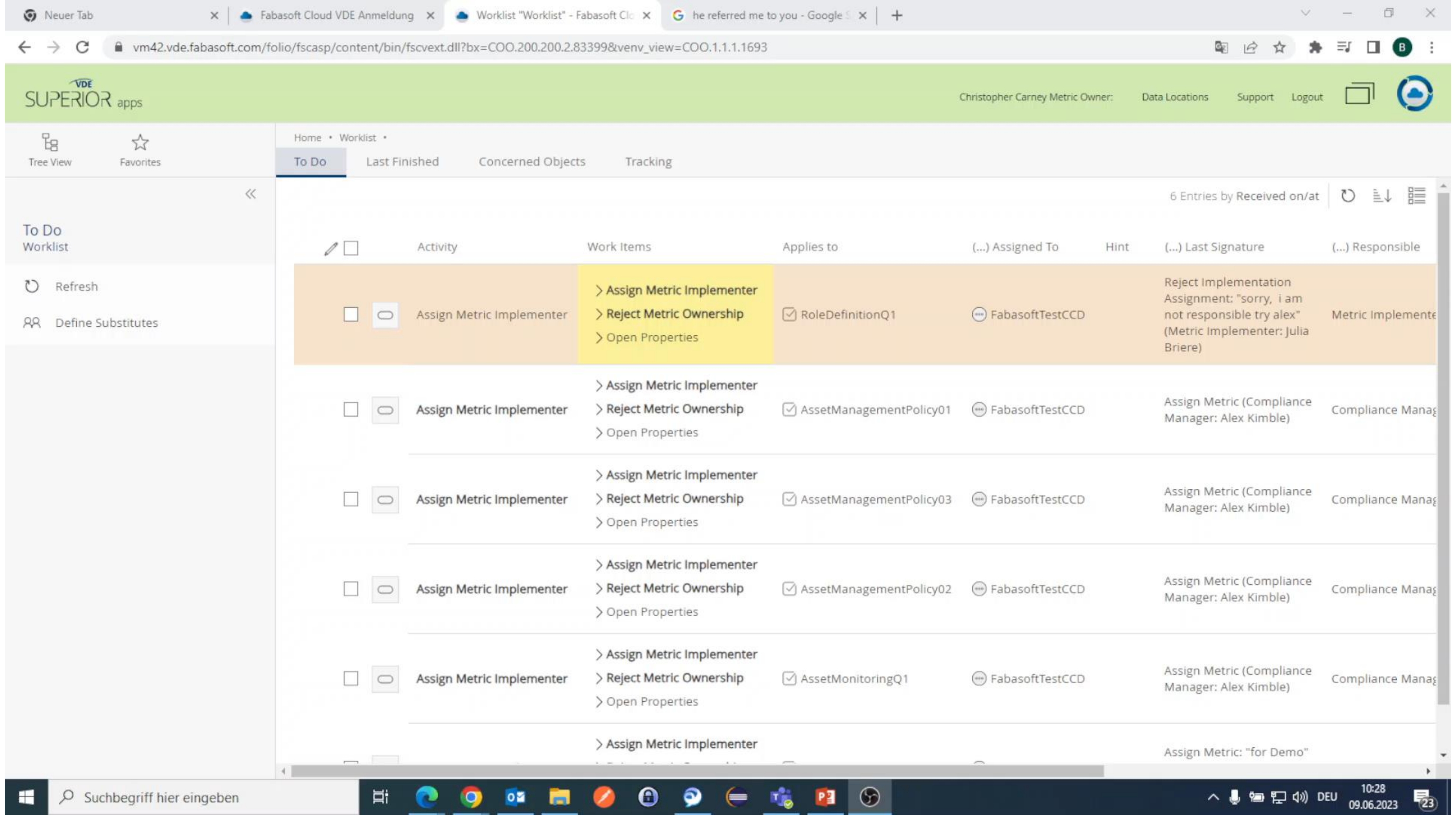


vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.3.83405&venv_ignorewelcome=true&cm=1&lx=en&cx=l-Dk--2jKNAQLc-J&tz=-120&sv=23.3.0.218&venv_view=COO...

Your personal folder does not contain any entries. Store your Teamrooms here.

There are no entries in this list.

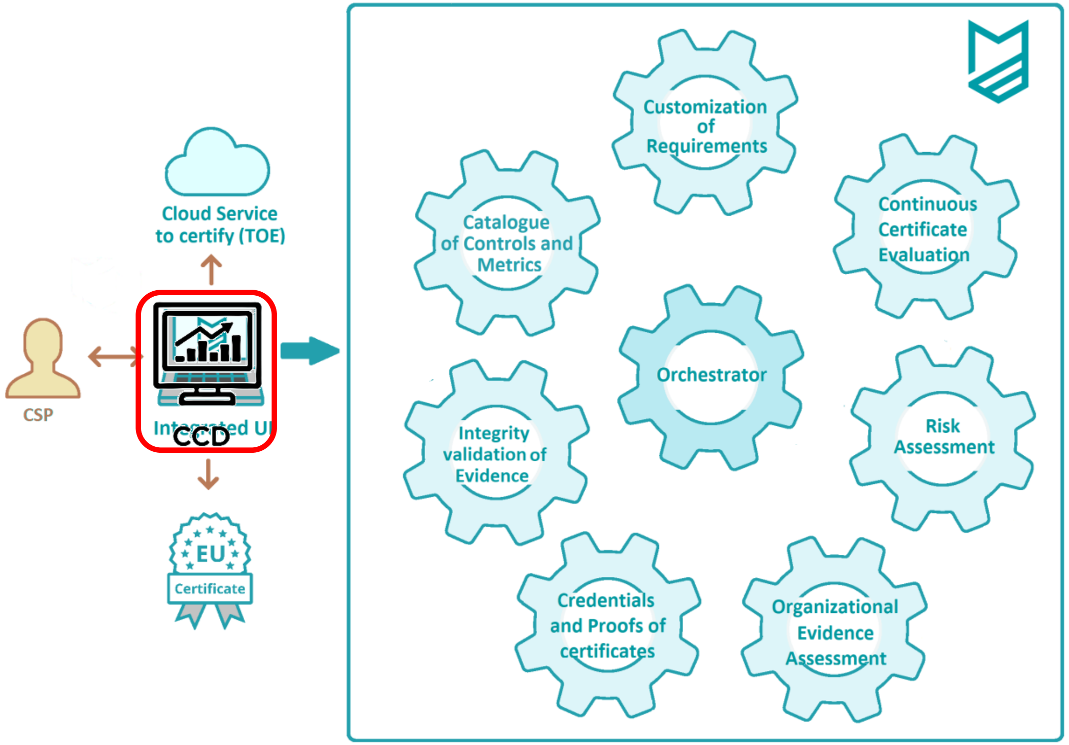
Redirect implementation


Neuer Tab
Fabasoft Cloud VDE Anmeldung
Worklist "Worklist" - Fabasoft Cl
he referred me to you - Google
vm42.vde.fabasoft.com/folio/fscasp/content/bin/fscvext.dll?bx=COO.200.200.2.83399&venv_view=COO.1.1.1.1693
VDE SUPERIOR apps
Christopher Carney Metric Owner:
Data Locations
Support
Logout
Tree View
Favorites
To Do
Worklist
Refresh
Define Substitutes
Home • Worklist •
To Do
Last Finished
Concerned Objects
Tracking
6 Entries by Received on/at
Suchbegriff hier eingeben
DEU
10:28
09.06.2023

□	Activity	Work Items	Applies to	(...) Assigned To	Hint	(...) Last Signature	(...) Responsible
□	Assign Metric Implementer	> Assign Metric Implementer > Reject Metric Ownership > Open Properties	☑ RoleDefinitionQ1	FabasoftTestCCD		Reject Implementation Assignment: "sorry, i am not responsible try alex" (Metric Implementer: Julia Briere)	Metric Implemente
□	Assign Metric Implementer	> Assign Metric Implementer > Reject Metric Ownership > Open Properties	☑ AssetManagementPolicy01	FabasoftTestCCD		Assign Metric (Compliance Manager: Alex Kimble)	Compliance Manag
□	Assign Metric Implementer	> Assign Metric Implementer > Reject Metric Ownership > Open Properties	☑ AssetManagementPolicy03	FabasoftTestCCD		Assign Metric (Compliance Manager: Alex Kimble)	Compliance Manag
□	Assign Metric Implementer	> Assign Metric Implementer > Reject Metric Ownership > Open Properties	☑ AssetManagementPolicy02	FabasoftTestCCD		Assign Metric (Compliance Manager: Alex Kimble)	Compliance Manag
□	Assign Metric Implementer	> Assign Metric Implementer > Reject Metric Ownership > Open Properties	☑ AssetMonitoringQ1	FabasoftTestCCD		Assign Metric (Compliance Manager: Alex Kimble)	Compliance Manag
		> Assign Metric Implementer				Assign Metric: "for Demo"	

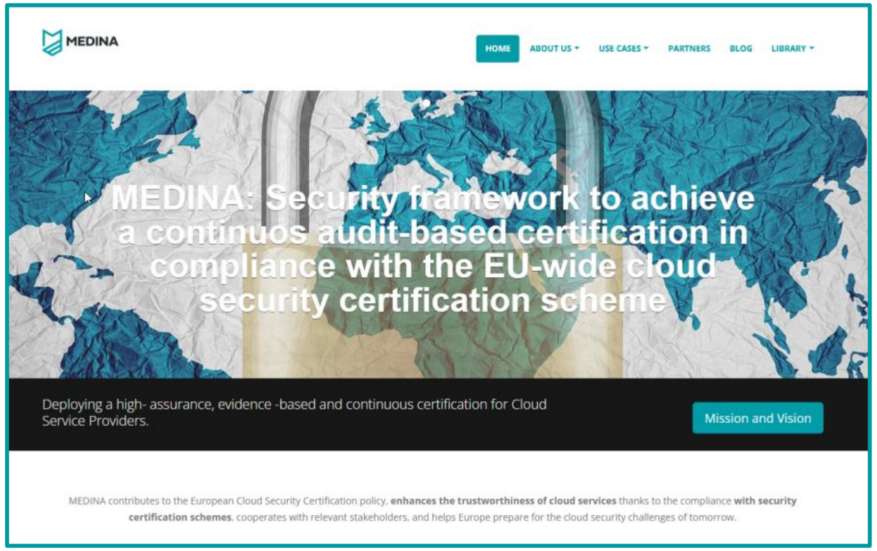
Company Compliance Dashboard

- Further information


Cloud Service to certify (TOE)
CSP
Integrated UI
CCD
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Fabasoft PROCECO Solutions
  - *Fabasoft app.ducx | Fabasoft - https://www.fabasoft.com/de/fabasoft-appducx*
  - *App.ducx help -https://help.developer.fabasoft.com/*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft

XLAB

nixu cybersecurity.

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

MEDINA

MEDINA architecture

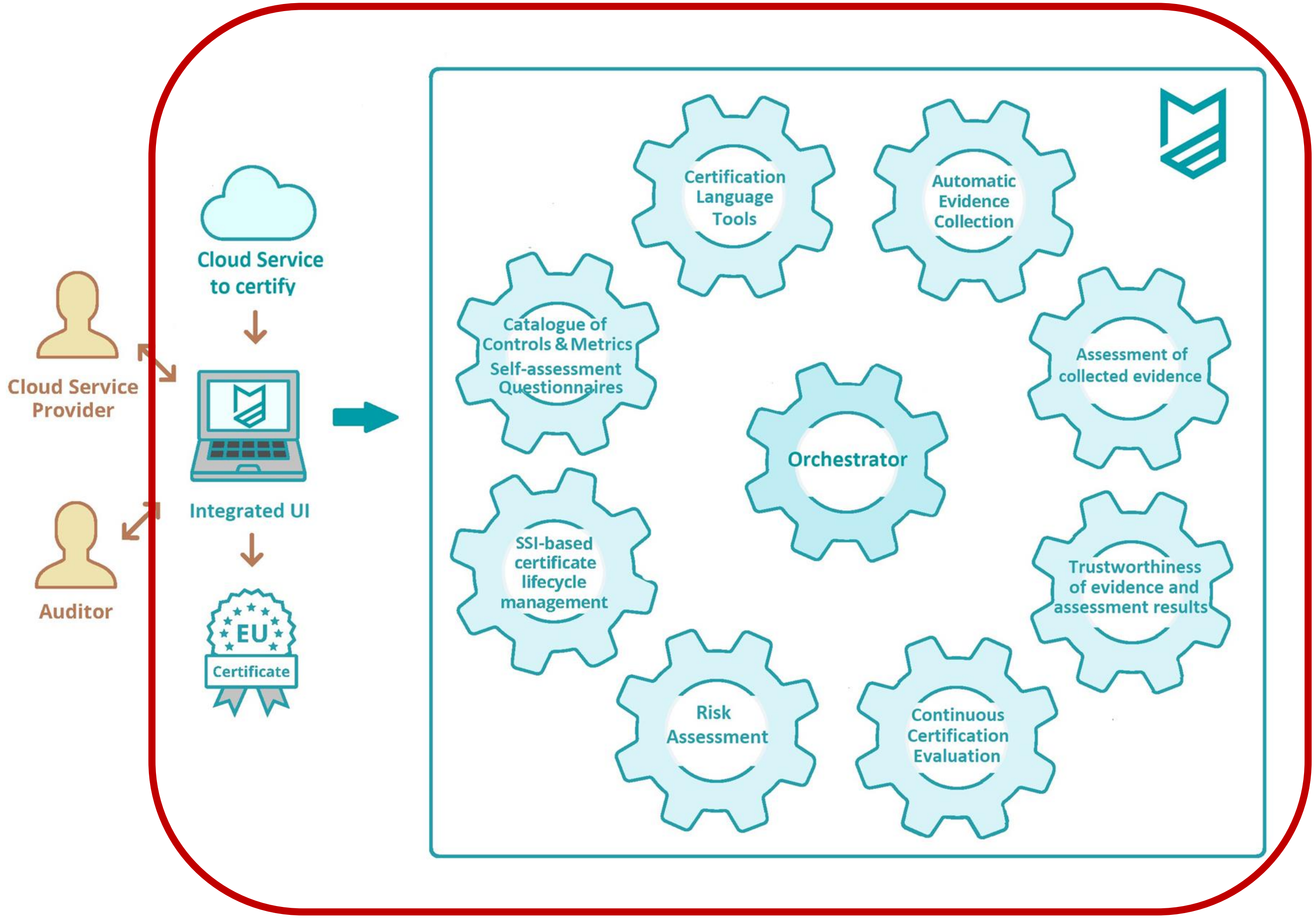
Iñaki Etxaniz, TECNALIA

October 2023

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

Chapters

- Diagram
- Data model
- User management
- Components
- Further information

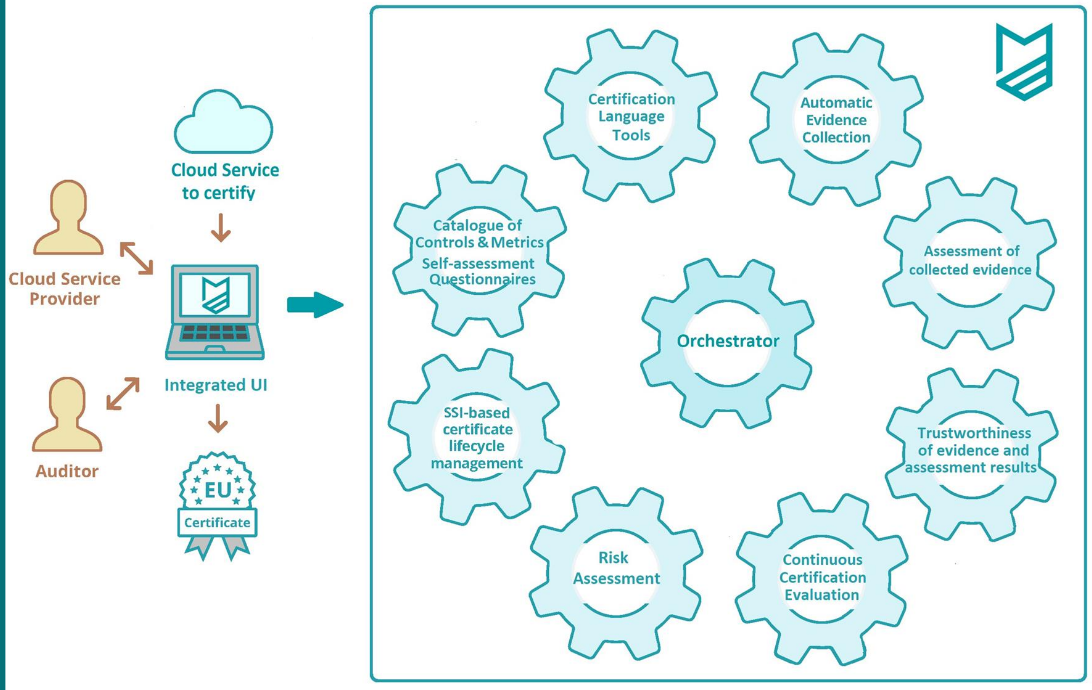


Cloud Service to certify
Cloud Service Provider
Integrated UI
Auditor
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

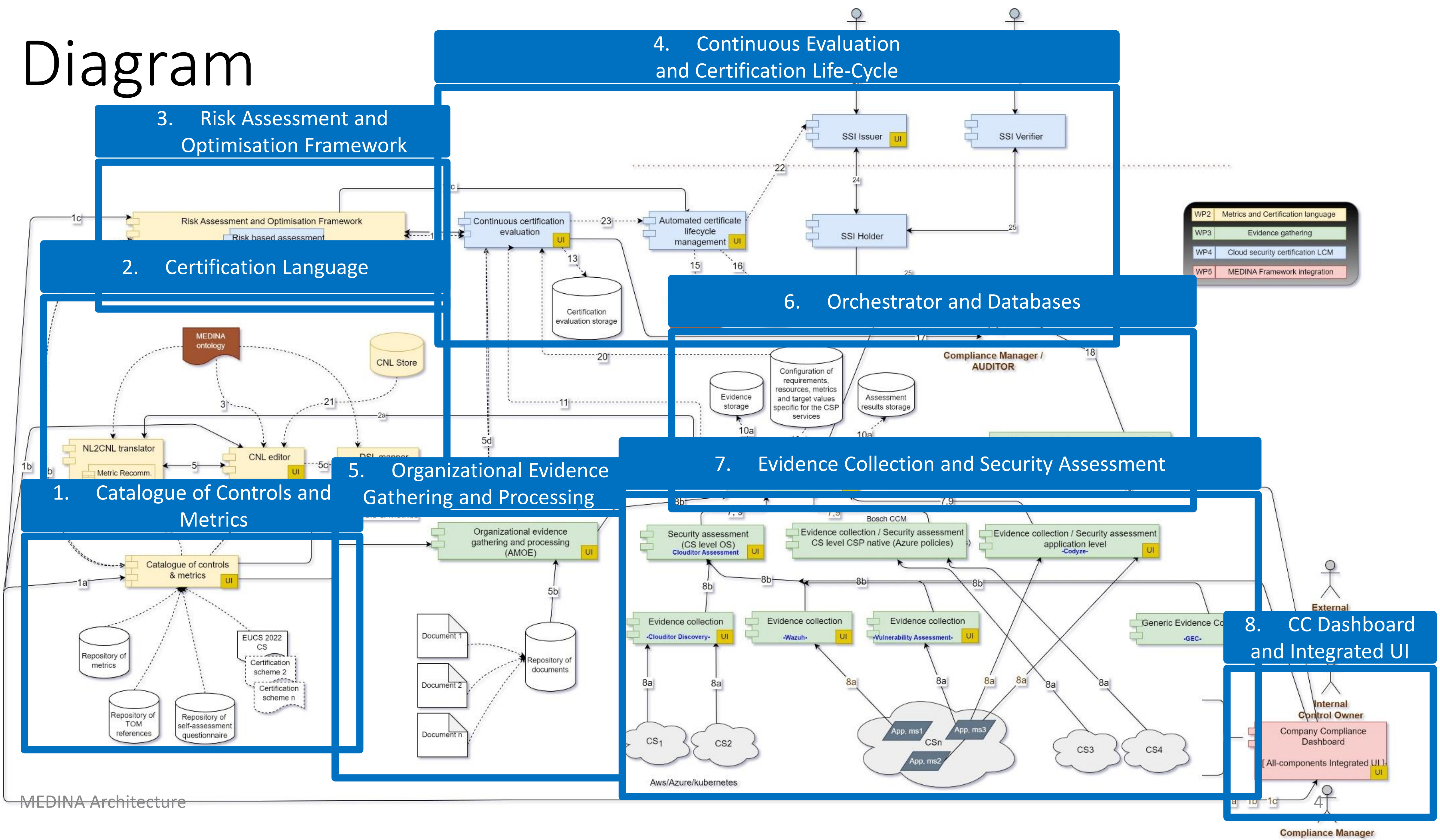
MEDINA Architecture

- Diagram
  - Component blocks
  - Data flow

MEDINA


Cloud Service to certify
Cloud Service Provider
Integrated UI
Auditor
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

Diagram



4. Continuous Evaluation and Certification Life-Cycle

3. Risk Assessment and Optimisation Framework

2. Certification Language

6. Orchestrator and Databases

5. Organizational Evidence Gathering and Processing

7. Evidence Collection and Security Assessment

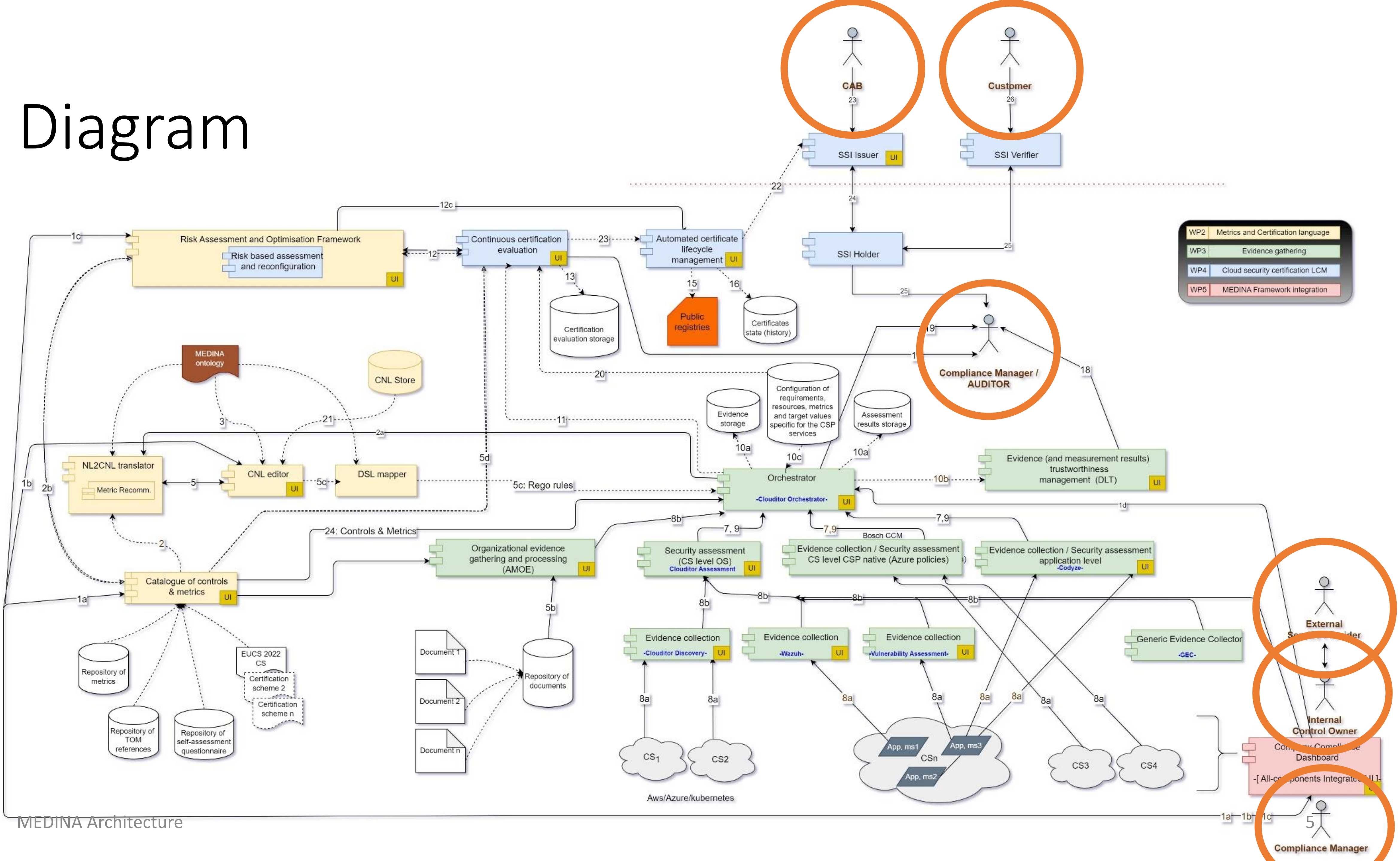
1. Catalogue of Controls and Metrics

8. CC Dashboard and Integrated UI

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

SSI Issuer
UI
SSI Verifier
22
24
25
SSI Holder
Risk Assessment and Optimisation Framework
Risk based assessment
1c
1
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
MEDINA ontology
CNL Store
20
17
18
Compliance Manager / AUDITOR
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
3
21
2a
11
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
1b
8b
7, 9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
Catalogue of controls & metrics
1a
5b
Evidence collection
-Clouditor Discovery-
-Wazuh-
-Vulnerability Assessment-
Generic Evidence Co
-GEC-
External
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Repository of TOM references
Repository of self-assessment questionnaire
8a
CS1
CS2
App, ms1
App, ms3
App, ms2
CSn
CS3
CS4
Aws/Azure/kubernetes
Internal Control Owner
Company Compliance Dashboard
[All-components Integrated UI]
Compliance Manager

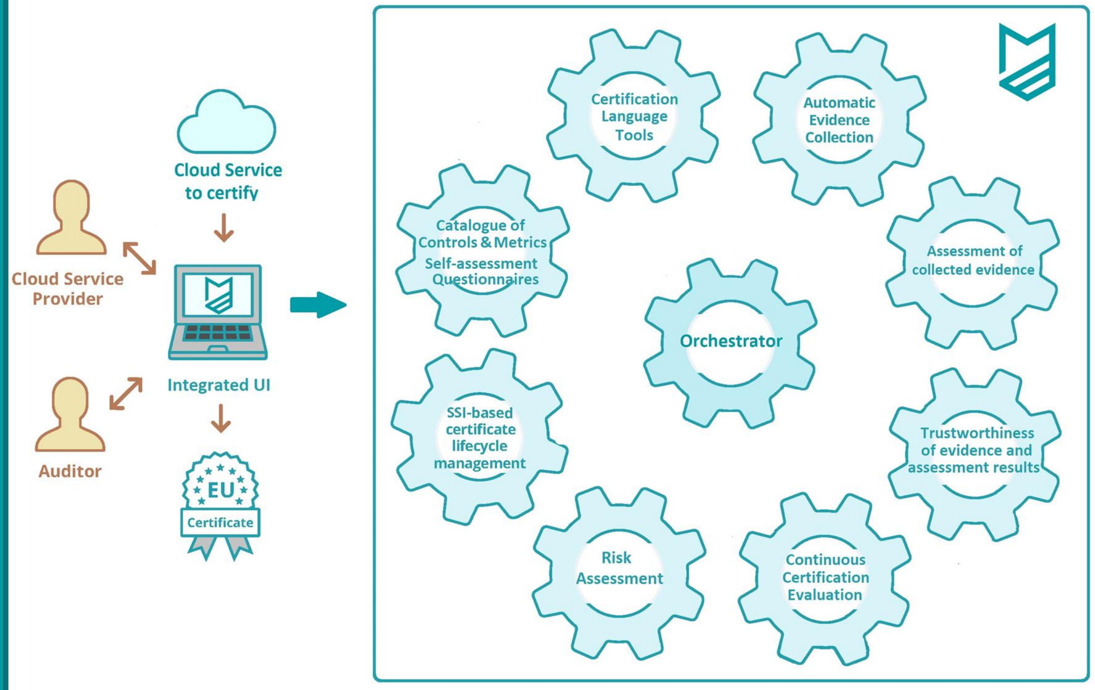
Diagram


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
25
SSI Holder
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
1
Compliance Manager / AUDITOR
18
MEDINA ontology
CNL Store
20
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
7, 9
7,9
7,9
Bosch CCM
24: Controls & Metrics
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
1a
1b
1c
5
Compliance Manager

MEDINA Architecture

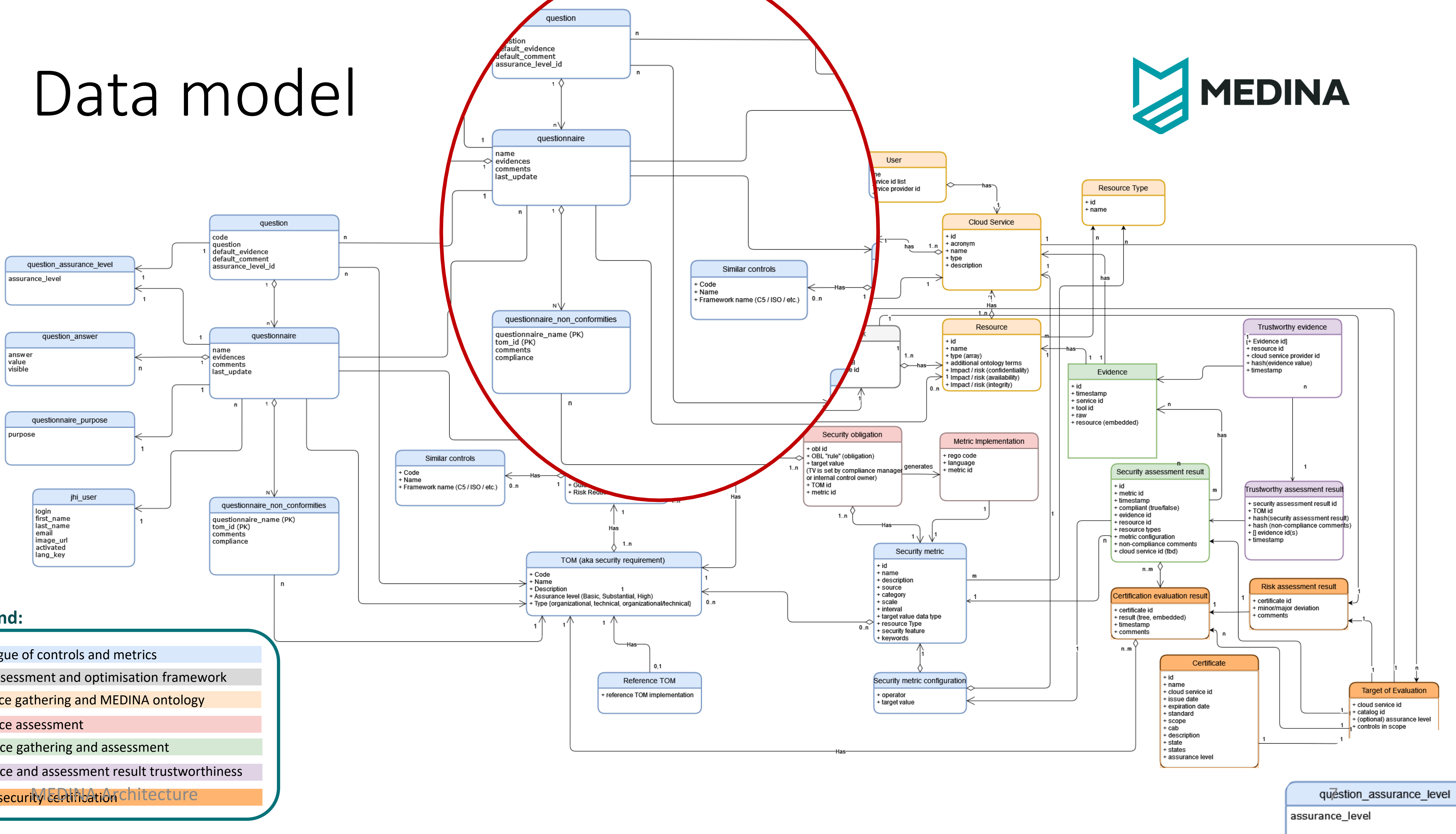
- Data Model

MEDINA


Cloud Service to certify
Cloud Service Provider
Integrated UI
Auditor
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

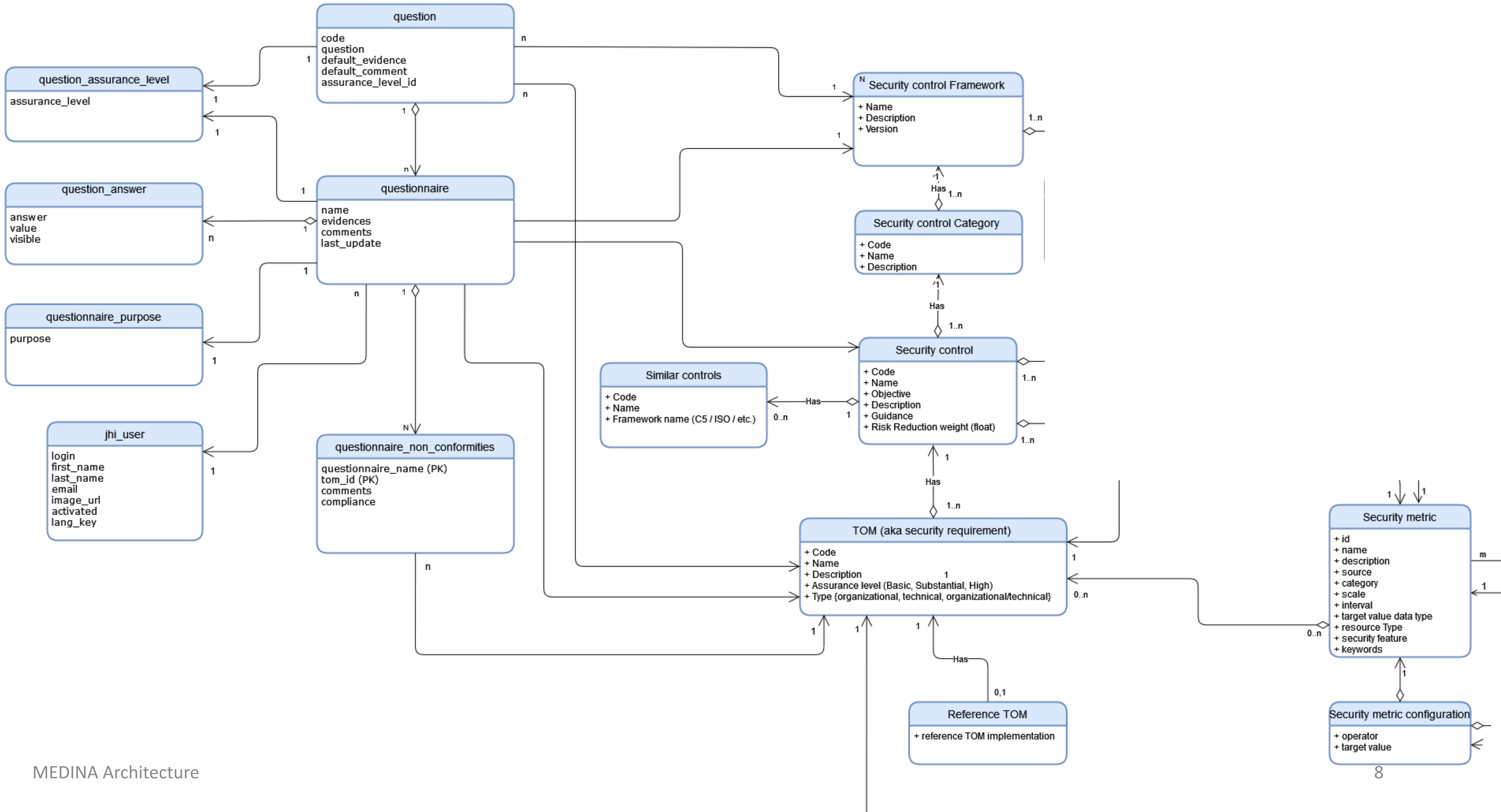
Data model

MEDINA



Legend:

- Catalogue of controls and metrics
- Risk Assessment and optimisation framework
- Evidence gathering and MEDINA ontology
- Evidence assessment
- Evidence gathering and assessment
- Evidence and assessment result trustworthiness
- Cloud security certification



question
code
question
default_evidence
default_comment
assurance_level_id

question_assurance_level
assurance_level

question_answer
answer
value
visible

questionnaire_purpose
purpose

jhi_user
login
first_name
last_name
email
image_url
activated
lang_key

questionnaire
name
evidences
comments
last_update

questionnaire_non_conformities
questionnaire_name (PK)
tom_id (PK)
comments
compliance

Security control Framework
+ Name
+ Description
+ Version

Security control Category
+ Code
+ Name
+ Description

Similar controls
+ Code
+ Name
+ Framework name (C5 / ISO / etc.)

Security control
+ Code
+ Name
+ Objective
+ Description
+ Guidance
+ Risk Reduction weight (float)

TOM (aka security requirement)
+ Code
+ Name
+ Description
+ Assurance level (Basic, Substantial, High)
+ Type {organizational, technical, organizational/technical}

Reference TOM
+ reference TOM implementation

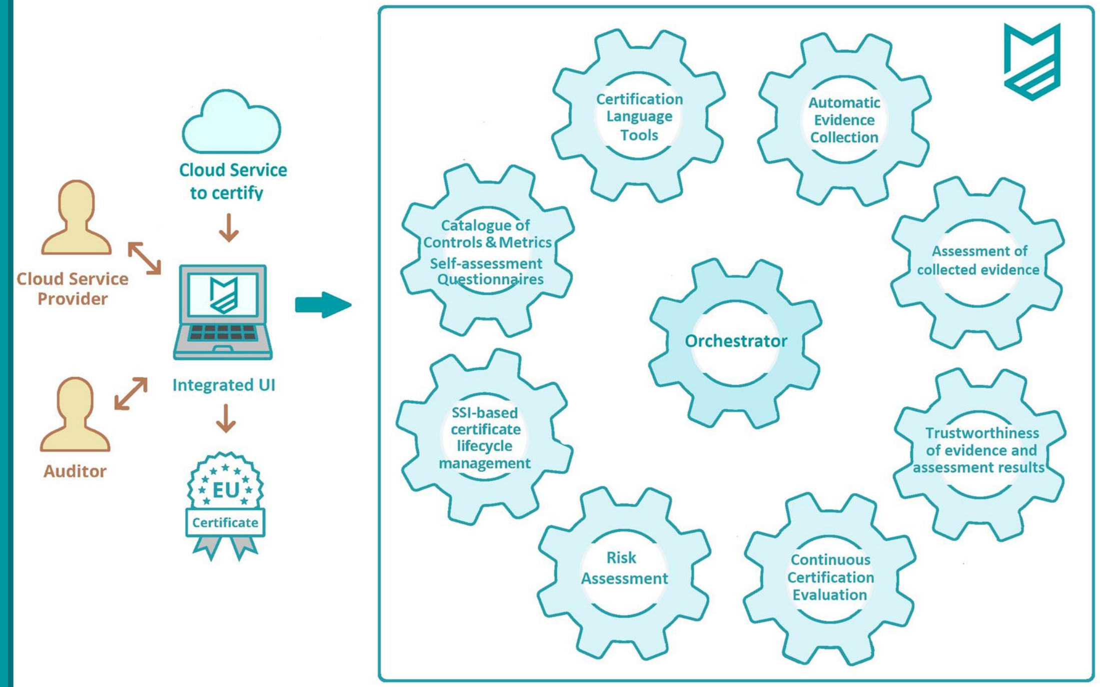
Security metric
+ id
+ name
+ description
+ source
+ category
+ scale
+ interval
+ target value data type
+ resource Type
+ security feature
+ keywords

Security metric configuration
+ operator
+ target value

MEDINA Architecture

- User Management
  - Keycloak
  - Roles
  - Authorization
  - Authentication

MEDINA

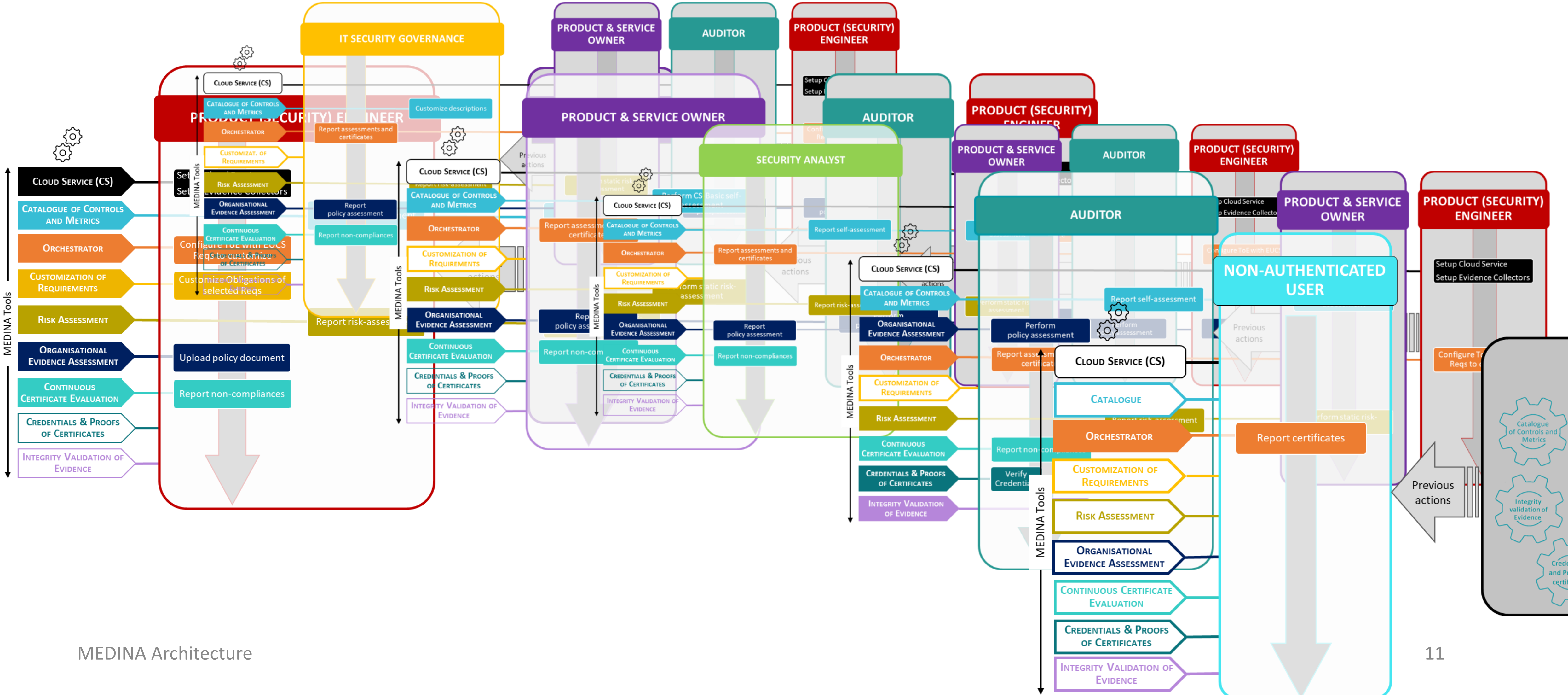


Cloud Service to certify
Cloud Service Provider
Integrated UI
Auditor
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

Roles

Role	Description	Level of Access
IT Security Governance	Its main objective is the protection of Bosch business models, products, services, and data.	Cloud Service Provider
Security Analyst	Responsible for ensuring that the Bosch Group's digital assets and sensitive information are protected as well as evaluating and reporting on the efficiency of the security policies in place.	Cloud Service Provider
Domain Governance	Acts as the core competence holder and responsible topic owner for product security.	One or more Cloud Services
Product and Service Owner	The Product & Service Owner is the central point of contact for all questions concerning a specific Bosch IT product or service.	Cloud Service
Product (Security) Engineer	Oversees the build, deploy, and run of a product and its system components.	Cloud Service
Chief Information Security Office (CISO)	The Chief Information Security Officer (CISO) is who the Compliance Manager has to report to.	Cloud Service Provider
Customer	The customer is either a company consuming cloud products or services (B2B, business-to-business context), or an individual (B2C, business-to-customer context).	Cloud Service
Auditor	The Conformity Assessment Body (CAB) is a body that performs conformity assessment services with the goal of demonstrating that specified requirements are fulfilled.	One or more Cloud Services

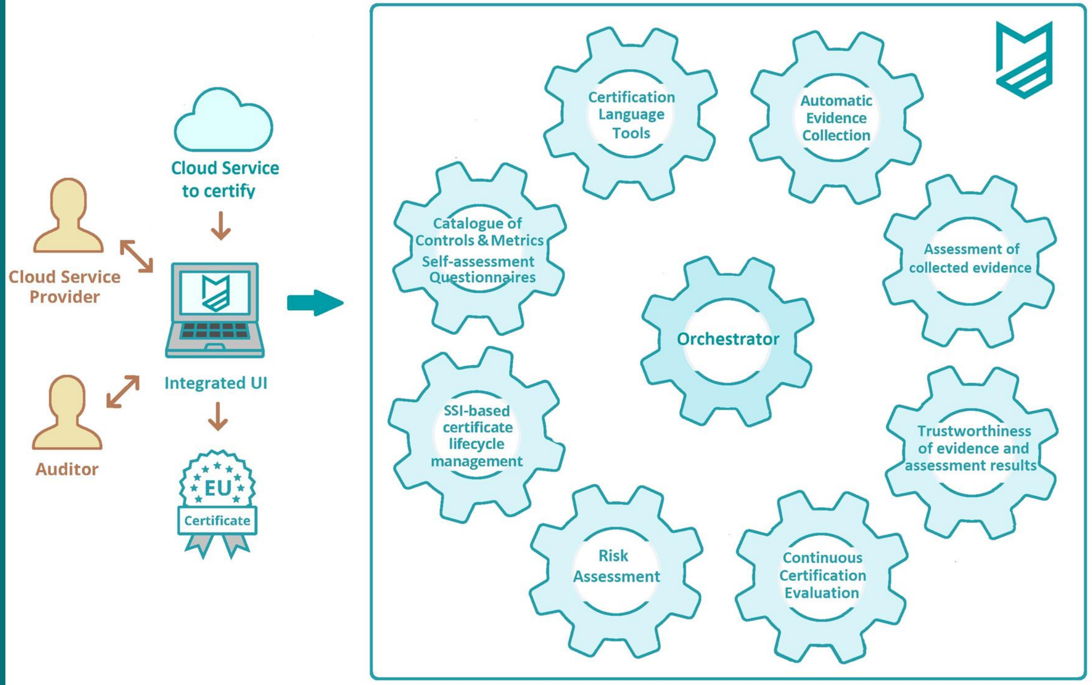
Authorization & Roles


MEDINA Tools
Cloud Service (CS)
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation
Credentials & Proofs of Certificates
Integrity Validation of Evidence
PRODUCT (SECURITY) ENGINEER
Configure ToE with EUCS Requirements
Customize Obligations of selected Reqs
Upload policy document
Report non-compliances
IT SECURITY GOVERNANCE
Customize descriptions
Report assessments and certificates
Report policy assessment
Report risk-assessment
Previous actions
PRODUCT & SERVICE OWNER
AUDITOR
SECURITY ANALYST
Perform CS Basic self-assessment
Report self-assessment
Perform static risk-assessment
Perform policy assessment
Verify Credentials
NON-AUTHENTICATED USER
Catalogue
Report certificates
Setup Cloud Service
Setup Evidence Collectors
Configure ToE with EUCS Reqs
Catalogue of Controls and Metrics
Integrity validation of Evidence

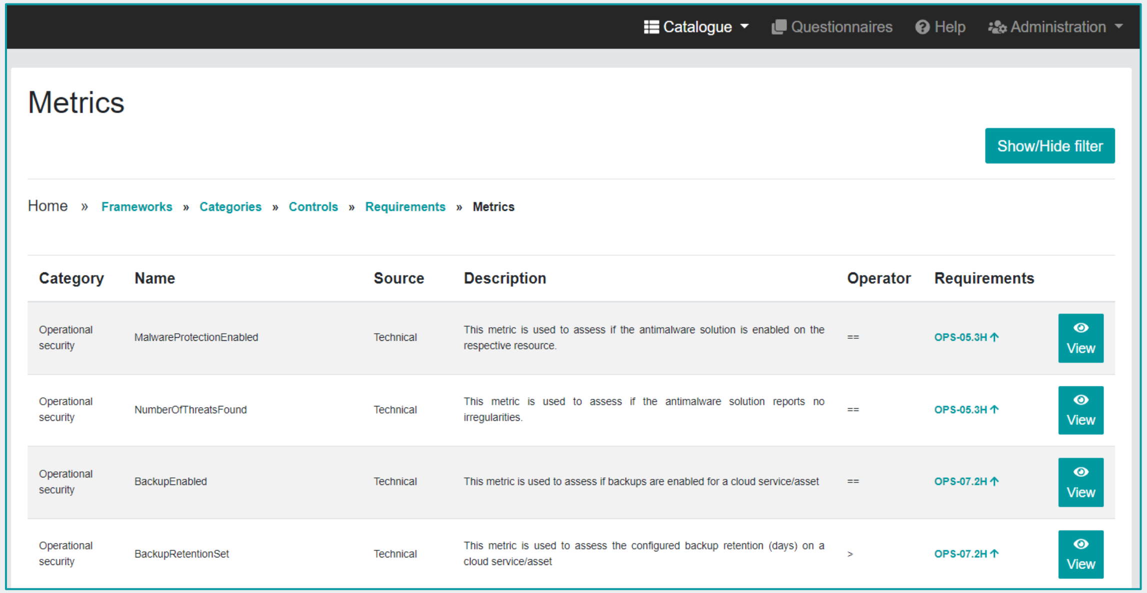
MEDINA Architecture

- Components

MEDINA


Cloud Service to certify
Cloud Service Provider
Auditor
Integrated UI
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

Catalogue of Controls and Metrics



Metrics

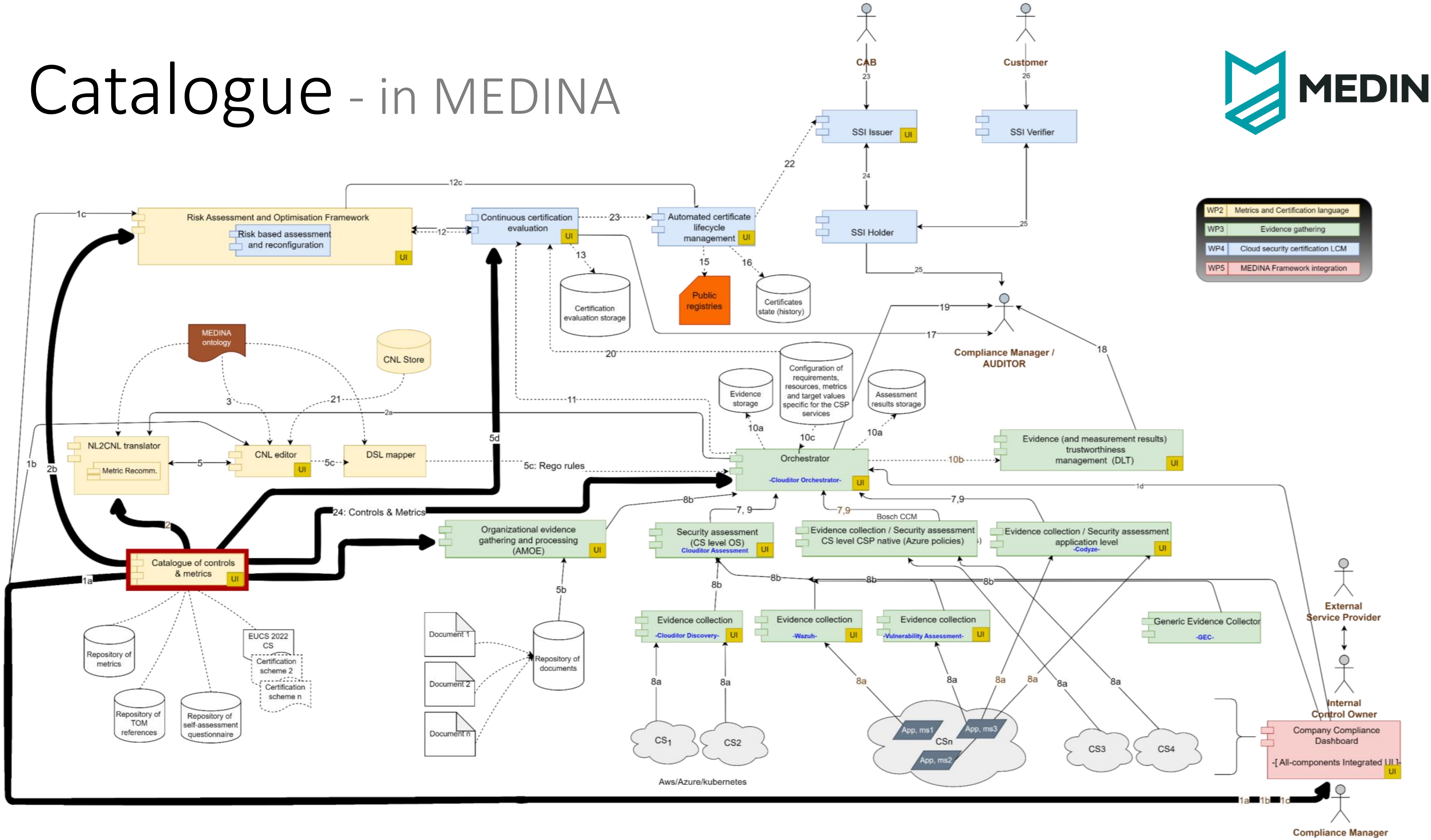
Home » Frameworks » Categories » Controls » Requirements » Metrics

Category	Name	Source	Description	Operator	Requirements	
Operational security	MalwareProtectionEnabled	Technical	This metric is used to assess if the antimalware solution is enabled on the respective resource.	==	OPS-05.3H ↑	View
Operational security	NumberOfThreatsFound	Technical	This metric is used to assess if the antimalware solution reports no irregularities.	==	OPS-05.3H ↑	View
Operational security	BackupEnabled	Technical	This metric is used to assess if backups are enabled for a cloud service/asset	==	OPS-07.2H ↑	View
Operational security	BackupRetentionSet	Technical	This metric is used to assess the configured backup retention (days) on a cloud service/asset	>	OPS-07.2H ↑	View

Catalogue - in a nutshell

- The Catalogue is the component that stores the **EUCS certification scheme** (draft version August-2022)
  - Stores as well the **metrics** defined in MEDINA
  - Defines **reference implementations** for “the 34” requirements
  - Provides **similar controls** in other schemas
  - Includes self-assessment **questionnaire** for CSPs
- Has a navigable **user interface** that allows the user to consult and check the standard
- Offers an **API** to the rest of MEDINA components to access the scheme information

Catalogue - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
Bosch CCM
7,9
Catalogue of controls & metrics
UI
1a
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
5b
8b
8b
8b
8b
Repository of metrics
Repository of TOM references
Repository of self-assessment questionnaire
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1d
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Catalogue - Interfaces

	Name	Description	Technology
INTERFACES	Catalogue UI	Web user interface of the Catalogue	Angular, Bootstrap
	Discovery API	Offers the EUCS set of controls, requirements, metrics with its attributes	Rest API

	Component	Interface description
INTERACTIONS WITH COMPONENTS	NL2CNL Translator	NL2CNL Translator **requests** the requirements and related information for a certain user
	Risk Assessment and Optimisation Framework/ Orchestrator/CCE/AMOE	RAOF **requests** to the Catalogue the requirements list and related information Catalogue **sends** to RAOF the answers of the questionnaire

Catalogue - More information

MEDINA

- Documentation:
  - *Catalogue User Manual* (https://zenodo.org/record/8425373)
  - *D2.2 Continuously certifiable technical and organizational measures and Catalogue of cloud security metrics-v2* (https://zenodo.org/record/7794478)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/catalogue-of-controls

- Training video:
  - https://youtu.be/Icuu1KeumXY

MEDINA

NL2CNL Translator

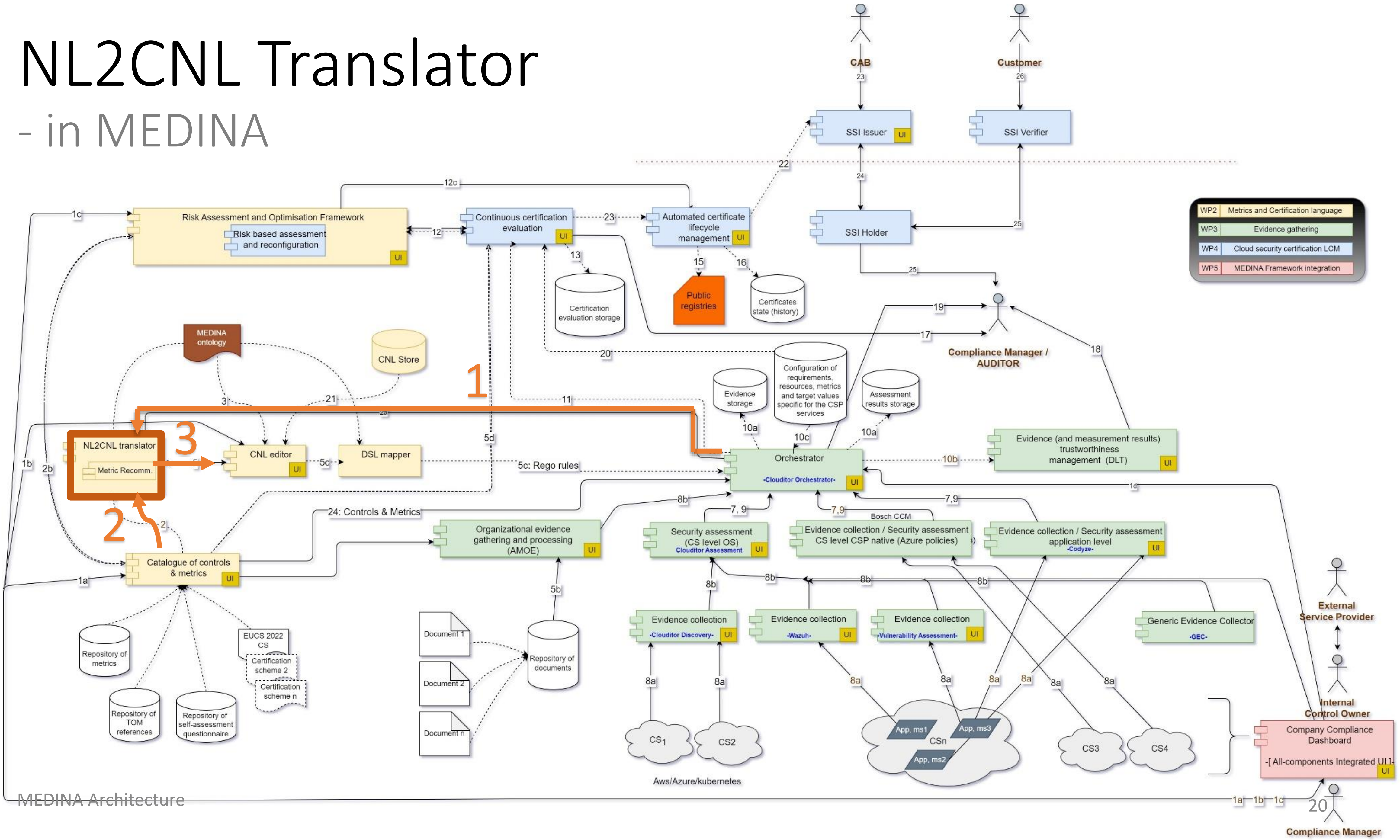
NL2CNL Translator – in a nutshell

- The goal of the Natural Language to Controlled Natural Language (NL2CNL) Translator is:
  - To associate a **Requirement** with a set of metrics
  - Translate the metrics into **Obligations**
  - Save both as a REO* object in the CNL Store
- Provides a **Metric Recommender** based on NLP techniques to automatically associate metrics to requirements.
- Communicates via a RESTful API

(*) REO: the association between the security Requirement and the policies (Obligations) a Cloud Service has to fulfil to be compliant, expressed in the MEDINA CNL.

NL2CNL Translator

- in MEDINA



CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
1
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
3
CNL editor
UI
DSL mapper
5c
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
Internal Control Owner
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

MEDINA Architecture

NL2CNL Translator - Interfaces

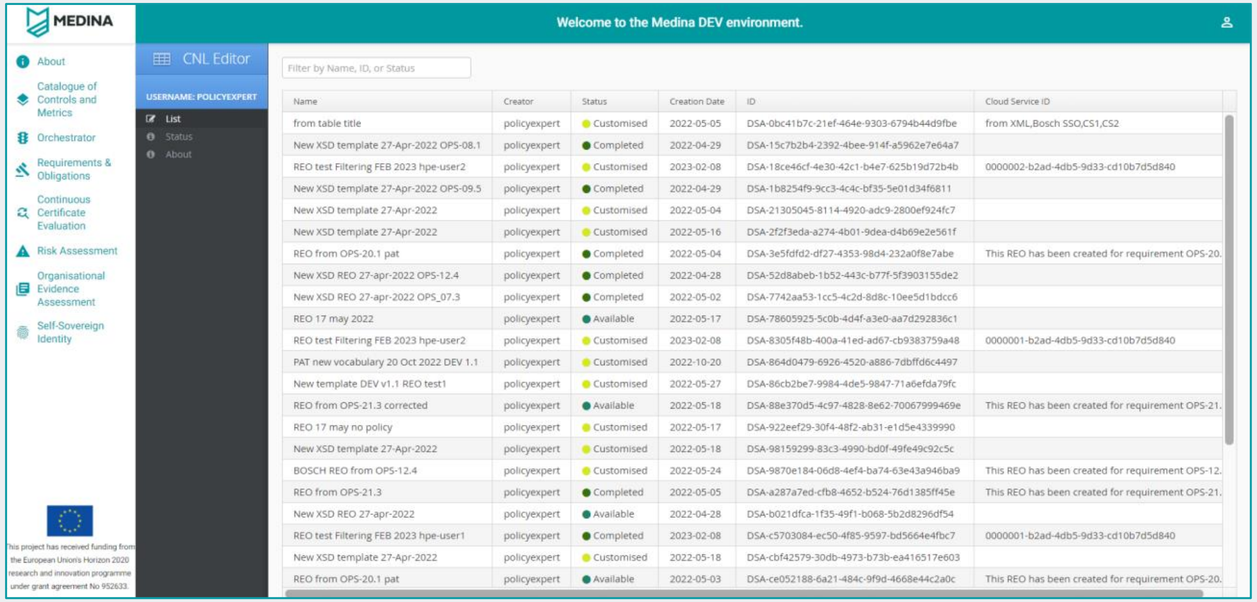
	Name	Description	Technology
INTERFACES	API Server	API to access NL2CNL functionalities	REST API

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Catalogue of controls and metrics	NL2CNL Translator **reads** requirements and metrics from it.
	Orchestrator	NL2CNL Translator receives from Orchestrator the link among the Cloud Services and requirements to be assessed.
	CNL Editor	NL2CNL Translator exploits CNL Editor API to **store** the requirements and obligations information in XML format.

NL2CNL Translator - More information

- Documentation:
  - *D2.5 Specification of the Cloud Security Certification Language – v3* (https://zenodo.org/record/7927213)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)
- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/nl2cnl-translator
- Training video:
  - https://youtu.be/cLISZR4yr1w

CNL Editor


MEDINA
Welcome to the Medina DEV environment.
About
Catalogue of Controls and Metrics
Orchestrator
Requirements & Obligations
Continuous Certificate Evaluation
Risk Assessment
Organisational Evidence Assessment
Self-Sovereign Identity
CNL Editor
USERNAME: POLICYEXPERT
List
Status
About
Filter by Name, ID, or Status

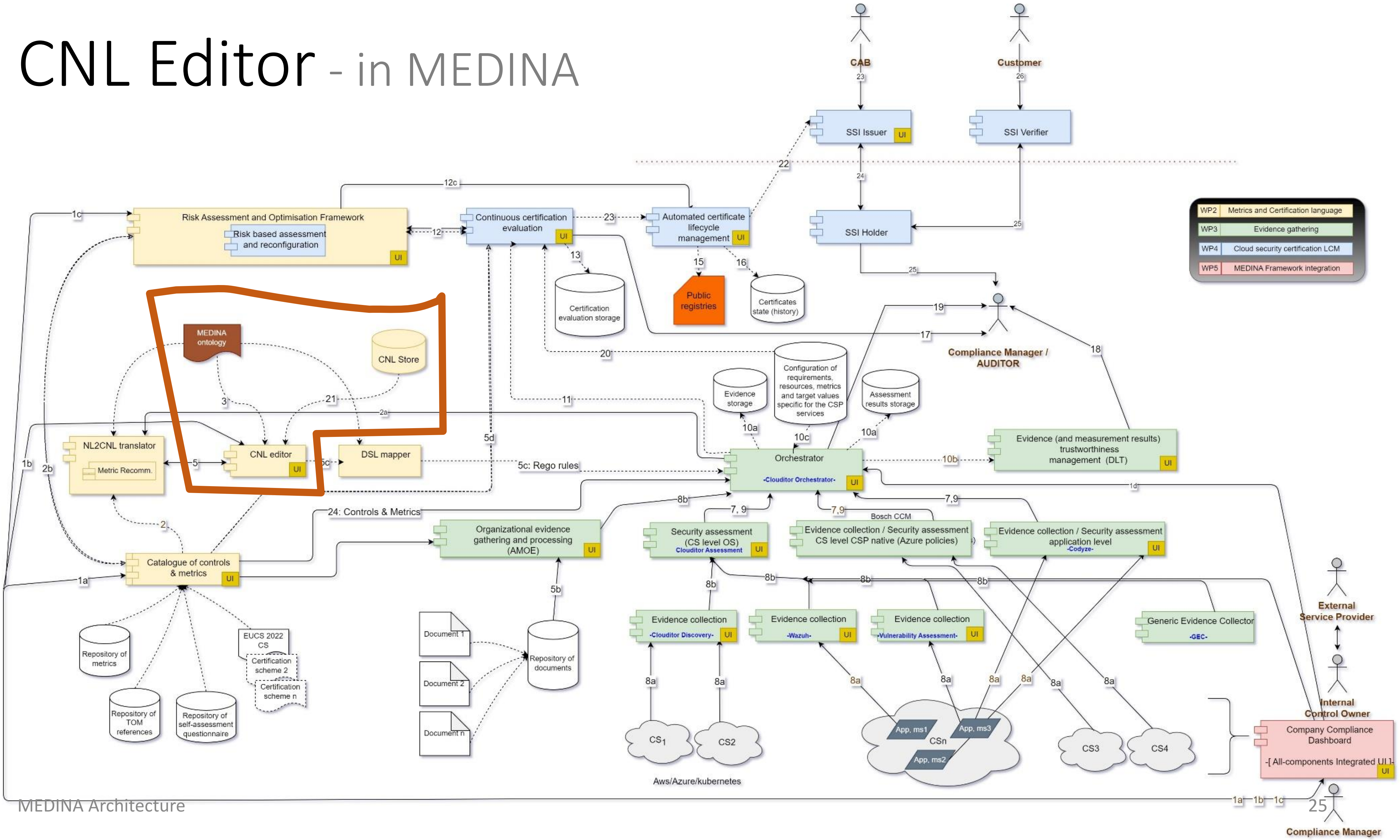
Name	Creator	Status	Creation Date	ID	Cloud Service ID
from table title	policyexpert	● Customised	2022-05-05	DSA-0bc41b7c-21ef-464e-9303-6794b44d9fbe	from XML,Bosch SSO,CS1,CS2
New XSD template 27-Apr-2022 OPS-08.1	policyexpert	● Completed	2022-04-29	DSA-15c7b2b4-2392-4bee-914f-a5962e7e64a7	
REO test Filtering FEB 2023 hpe-user2	policyexpert	● Customised	2023-02-08	DSA-18ce46cf-4e30-42c1-b4e7-625b19d72b4b	0000002-b2ad-4db5-9d33-cd10b7d5d840
New XSD template 27-Apr-2022 OPS-09.5	policyexpert	● Completed	2022-04-29	DSA-1b8254f9-9cc3-4c4c-bf35-5e01d34f6811	
New XSD template 27-Apr-2022	policyexpert	● Customised	2022-05-04	DSA-21305045-8114-4920-adc9-2800ef924fc7	
New XSD template 27-Apr-2022	policyexpert	● Customised	2022-05-16	DSA-2f2f3eda-a274-4b01-9dea-d4b69e2e561f	
REO from OPS-20.1 pat	policyexpert	● Completed	2022-05-04	DSA-3e5fdfd2-df27-4353-98d4-232a0f8e7abe	This REO has been created for requirement OPS-20.
New XSD REO 27-apr-2022 OPS-12.4	policyexpert	● Completed	2022-04-28	DSA-52d8abeb-1b52-443c-b77f-5f3903155de2	
New XSD REO 27-apr-2022 OPS_07.3	policyexpert	● Completed	2022-05-02	DSA-7742aa53-1cc5-4c2d-8d8c-10ee5d1bdcc6	
REO 17 may 2022	policyexpert	● Available	2022-05-17	DSA-78605925-5c0b-4d4f-a3e0-aa7d292836c1	
REO test Filtering FEB 2023 hpe-user2	policyexpert	● Customised	2023-02-08	DSA-8305f48b-400a-41ed-ad67-cb9383759a48	0000001-b2ad-4db5-9d33-cd10b7d5d840
PAT new vocabulary 20 Oct 2022 DEV 1.1	policyexpert	● Customised	2022-10-20	DSA-864d0479-6926-4520-a886-7dbffd6c4497	
New template DEV v1.1 REO test1	policyexpert	● Customised	2022-05-27	DSA-86cb2be7-9984-4de5-9847-71a6efda79fc	
REO from OPS-21.3 corrected	policyexpert	● Available	2022-05-18	DSA-88e370d5-4c97-4828-8e62-70067999469e	This REO has been created for requirement OPS-21.
REO 17 may no policy	policyexpert	● Customised	2022-05-17	DSA-922eef29-30f4-48f2-ab31-e1d5e4339990	
New XSD template 27-Apr-2022	policyexpert	● Customised	2022-05-18	DSA-98159299-83c3-4990-bd0f-49fe49c92c5c	
BOSCH REO from OPS-12.4	policyexpert	● Customised	2022-05-24	DSA-9870e184-06d8-4ef4-ba74-63e43a946ba9	This REO has been created for requirement OPS-12.
REO from OPS-21.3	policyexpert	● Completed	2022-05-05	DSA-a287a7ed-cfb8-4652-b524-76d1385ff45e	This REO has been created for requirement OPS-21.
New XSD REO 27-apr-2022	policyexpert	● Available	2022-04-28	DSA-b021dfca-1f35-49f1-b068-5b2d8296df54	
REO test Filtering FEB 2023 hpe-user1	policyexpert	● Completed	2023-02-08	DSA-c5703084-ec50-4f85-9597-bd5664e4fbc7	0000001-b2ad-4db5-9d33-cd10b7d5d840
New XSD template 27-Apr-2022	policyexpert	● Customised	2022-05-18	DSA-cbf42579-30db-4973-b73b-ea416517e603	
REO from OPS-20.1 pat	policyexpert	● Available	2022-05-03	DSA-ce052188-6a21-484c-9f9d-4668e44c2a0c	This REO has been created for requirement OPS-20.

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

CNL Editor – in a nutshell

- The Controlled Natural Language (CNL) Editor allows the **customization of Requirements and Obligations** (REO*)
  - Deleting Obligations
  - Changing the operator
  - Updating the TargetValue of the metric
- Uses a vocabulary (.owl file) based in an Obligations **Ontology**, as specified in the Catalogue
- Web user interface

CNL Editor - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
2a
11
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
1b
2b
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Catalogue of controls & metrics
UI
1a
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
8b
8b
8b
8b
5b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

CNL Editor - Interfaces

MEDINA

	Name	Description	Technology
INTERFACES	CNL Editor UI	CNL Editor Web GUI	HTTP (browser)
	Editor API	API to access CNL documents	REST API

	Component	Interface description
INTERACTIONS WITH COMPONENTS	CNL Translator	CNL Editor **reads** CNL documents in XML format as prepared by CNL Translator
	DSL Mapper	CNL Editor **provides** to DSL Mapper the finalised CNL documents to be mapped
	Catalogue of controls and metrics	CNL Editor **uses** a vocabulary whose entities are derived from the Catalogue and serves to bind the user's choices.

CNL Editor - More information

- Documentation:
  - *Customization of Requirements User manual* (https://zenodo.org/record/8425438)
  - *D2.5 Specification of the Cloud Security Certification Language – v3* (https://zenodo.org/record/7927213)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/cnl-editor

- Training video:
  - https://youtu.be/cLISZR4yr1w

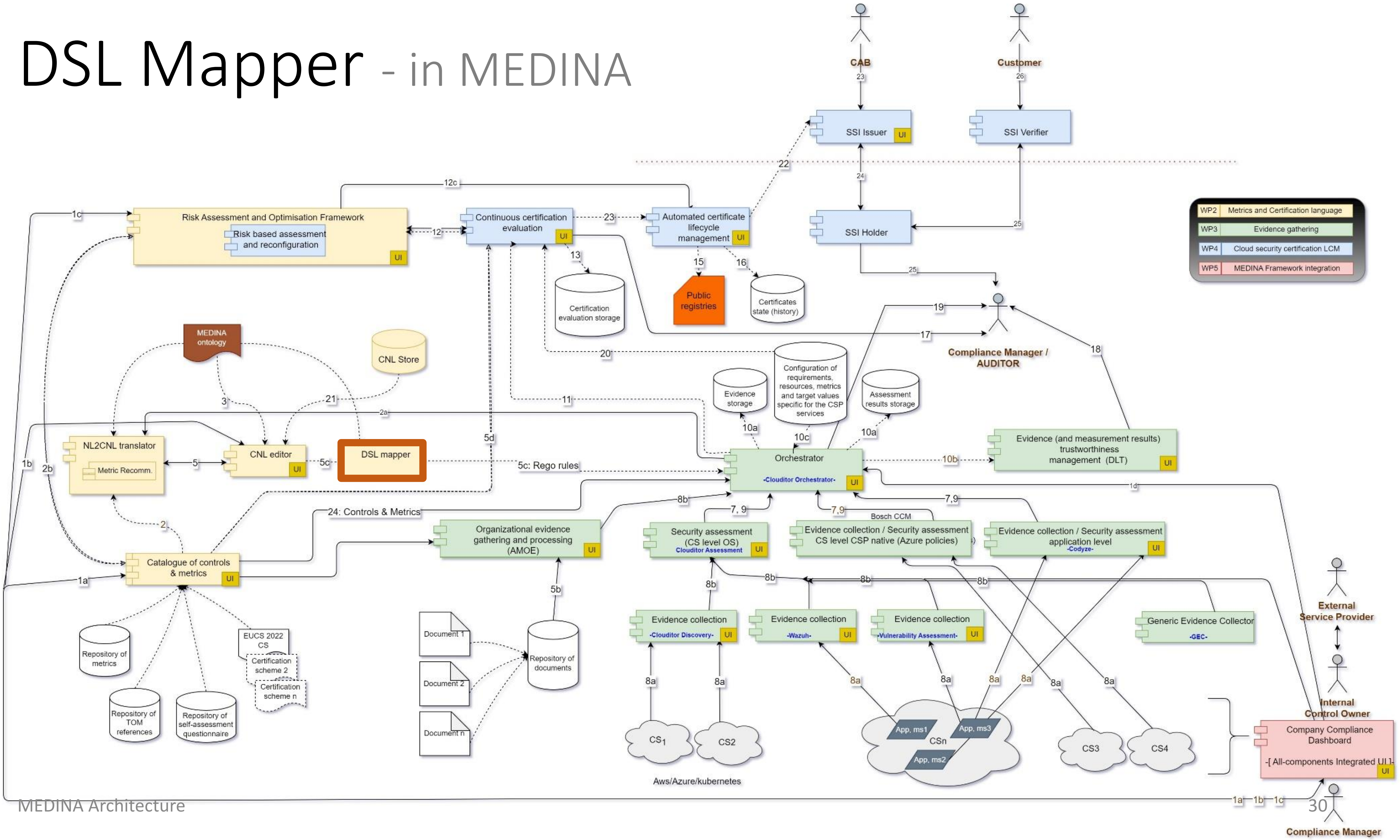
DSL Mapper

DSL Mapper – in a nutshell

- The Domain Specific Language (DSL) Mapper **maps the obligations into executable policies** expressed in DSL.
  - Obligations come expressed in CNL
  - DSL chosen in MEDINA: Rego language

- Provides a **translation** from a non-executable language (CNL) to an **executable** one (DSL).
  - Output Rego code is used by MEDINA Evidence Management Tools

DSL Mapper - in MEDINA


CAB
Customer
23
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
MEDINA ontology
CNL Store
20
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
24: Controls &amp; Metrics
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls &amp; metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
Internal Control Owner
Repository of TOM references
Repository of self-assessment questionnaire
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
Aws/Azure/kubernetes
1a
1b
1c
Compliance Manager

DSL Mapper - Interfaces

INTERFACES	Name	Description	Technology
	API Server	API to access DSL Mapper functionalities	REST API

INTERACTIONS WITH COMPONENTS	Component	Interface description
	CNL Editor	The DSL Mapper is **called** from the CNL Editor, which passes, as a parameter, an object in XML format, including all the necessary requirement metadata, metrics information, CNL obligations
	Orchestrator	The DSL Mapper **pushes** the selected obligations + metadata mapped into a DSL (Rego) to the Orchestrator

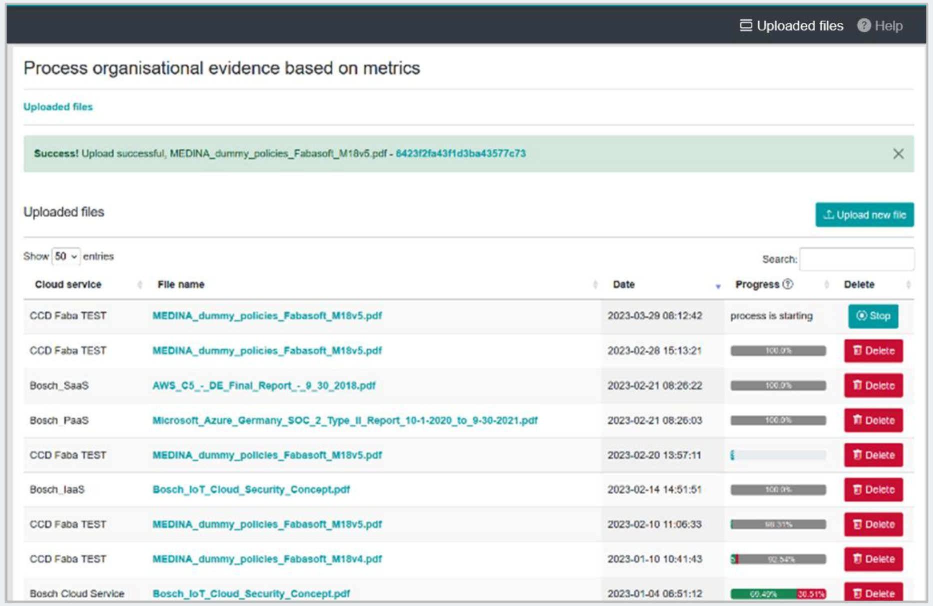
DSL Mapper - More information

- Documentation:
  - *D2.5 Specification of the Cloud Security Certification Language – v3* (https://zenodo.org/record/7927213)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/dsl-mapper

- Training video:
  - https://youtu.be/cLISZR4yr1w

AMOE – Assessment and Management of Organizational Evidence



Process organisational evidence based on metrics

Success! Upload successful, MEDINA_dummy_policies_Fabasoft_M18v5.pdf - 6423f2fa43f1d3ba43577c73

Uploaded files

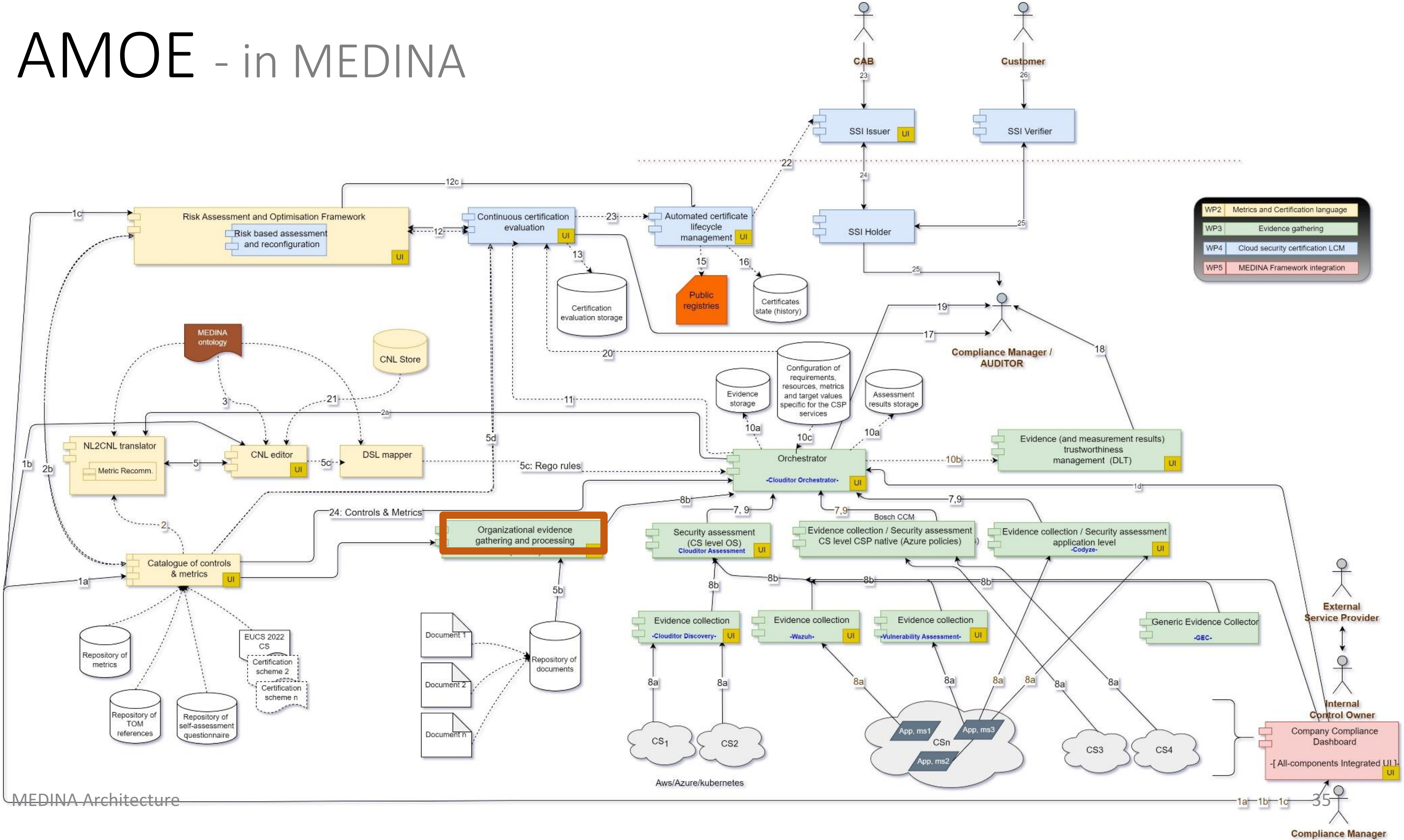
Cloud service	File name	Date	Progress	Delete
CCD Faba TEST	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-03-29 08:12:42	process is starting	Stop
CCD Faba TEST	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-02-28 15:13:21	100.0%	Delete
Bosch_SaaS	AWS_C5_-_DE_Final_Report_-_9_30_2018.pdf	2023-02-21 08:26:22	100.0%	Delete
Bosch_PaaS	Microsoft_Azure_Germany_SOC_2_Type_II_Report_10-1-2020_to_9-30-2021.pdf	2023-02-21 08:26:03	100.0%	Delete
CCD Faba TEST	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-02-20 13:57:11		Delete
Bosch_IaaS	Bosch_IoT_Cloud_Security_Concept.pdf	2023-02-14 14:51:51	100.0%	Delete
CCD Faba TEST	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-02-10 11:06:33	98.31%	Delete
CCD Faba TEST	MEDINA_dummy_policies_Fabasoft_M18v4.pdf	2023-01-10 10:41:43	92.54%	Delete
Bosch Cloud Service	Bosch_IoT_Cloud_Security_Concept.pdf	2023-01-04 06:51:12	69.49% 30.51%	Delete

AMOE – in a nutshell

- The Assessment and Management of Organizational Evidence (AMOE) **examines policy documents from which extracts evidences** to pre-assess metrics.
  - Allows to **upload** policy documents
  - Computes assessment **“hints”** (pre-assessments)

- The user decides the **assessment result**, and forwards it to the Orchestrator

AMOE - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls &amp; Metrics
Organizational evidence gathering and processing
8b
7, 9
7,9
Bosch CCM
7,9
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls &amp; metrics
UI
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Repository of TOM references
Repository of self-assessment questionnaire
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

AMOE- Interfaces

	Name	Description	Technology
INTERFACES	UI	GUI to upload documents, retrieve evidence, set assessment results and submit/forward assessment results	webservice
	API	Upload documents, retrieve evidence, set assessment results and submit/forward assessment results	REST

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Orchestrator	Send collected evidences + assessment results Retrieve metric configurations
	Catalogue of Controls and Metrics	Retrieve metrics and requirements as needed

AMOE - More information

MEDINA

- Documentation:
  - *Organisational Evidence Assessment User Manual* (https://zenodo.org/record/8425222)
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/amoe

- Training video:
  - https://youtu.be/QNdlzfNT4zM

MEDINA

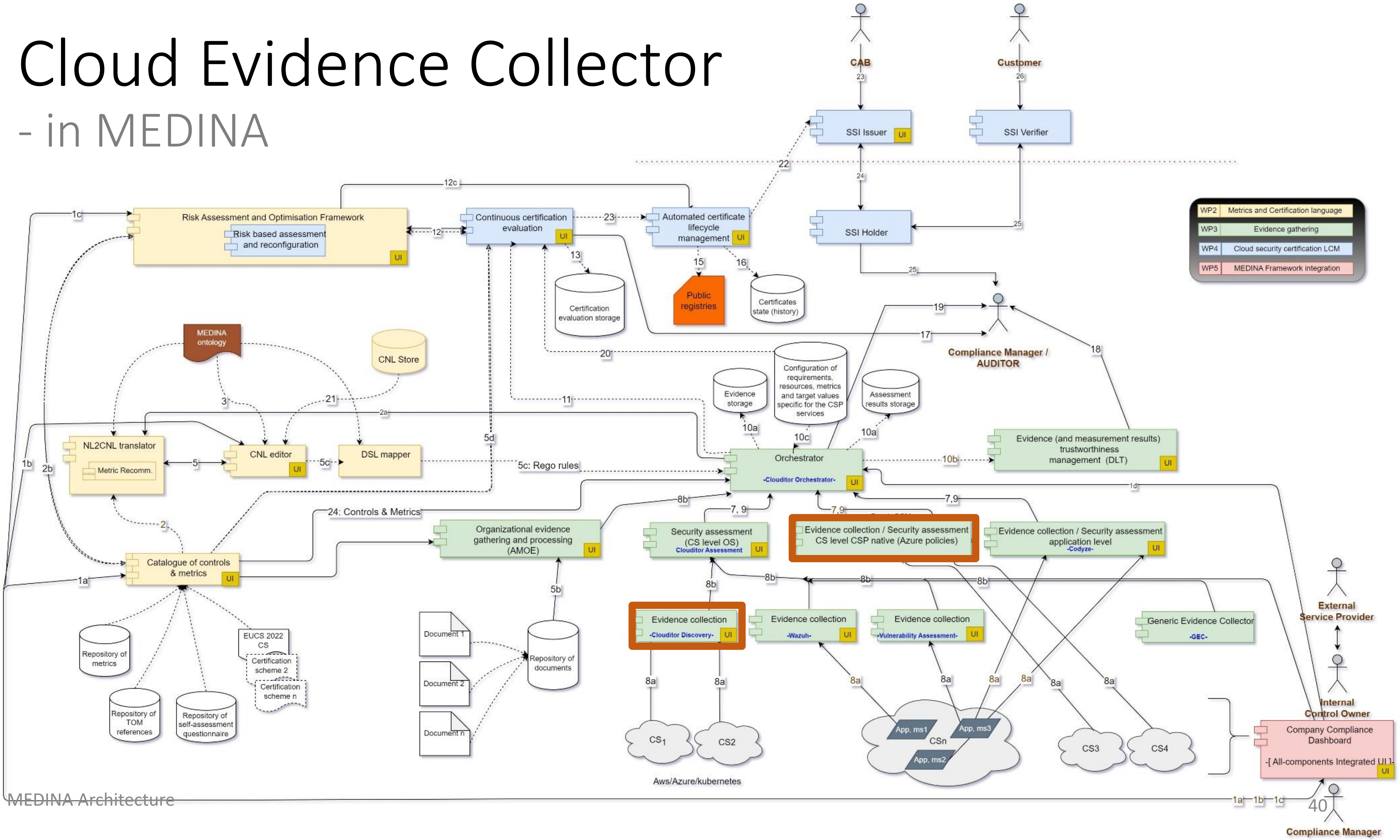
Cloud Evidence Collector

Cloud Evidence Collector – in a nutshell

- The Cloud Evidence Collector **collects data from Cloud resources** (e.g. Azure, AWS…) **and translates them to MEDINA evidences**
  - **Forwards** the data to the Orchestrator

Cloud Evidence Collector

- in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
Internal Control Owner
Repository of TOM references
Repository of self-assessment questionnaire
8a
8a
8a
8a
8a
8a
8a
8a
App, ms1
App, ms3
CSn
App, ms2
CS1
CS2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

Cloud Evidence Collector - Interfaces

	Name	Description	Technology
INTERFACES	Assessment API	An interface for providing evidence to be assessed against suitable metrics	gRPC

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Orchestrator	Send assessment results

Cloud Evidence Collector- More information

MEDINA

- Documentation:
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/cloud-evidence-collector

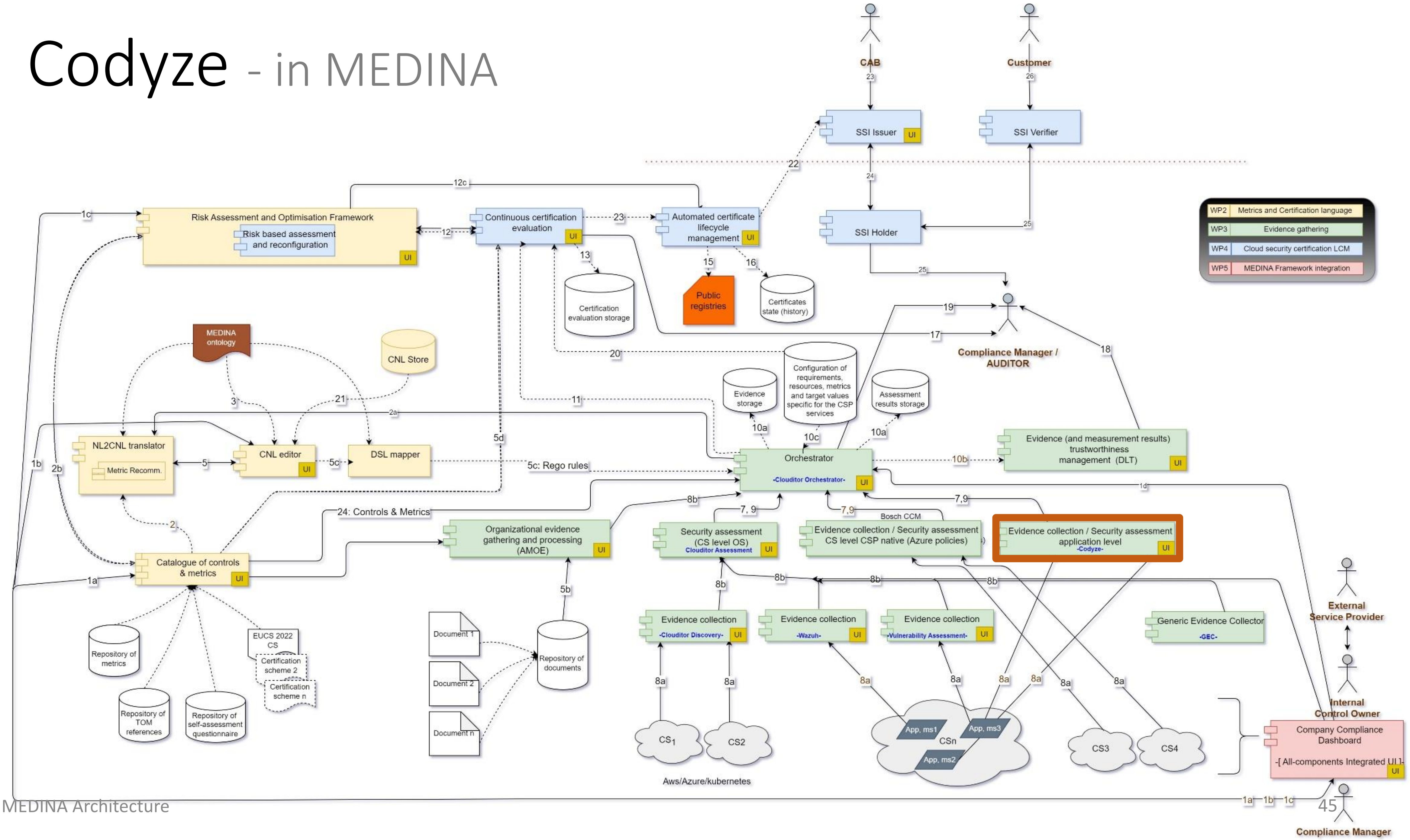
- Training video:
  - https://youtu.be/Sl-7zfn5eK4

Codyze

Codyze – in a nutshell

- Codyze goal is to **collect data from source code** and **assess it** according to MEDINA metrics
  - **Forwards** the data to the Orchestrator

Codyze - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Codyze - Interfaces

	Name	Description	Technology
INTERFACES	CLI	*Codyze* provides a command line interface. It can be used to call *Codyze* to analyse a set of files and produce results. It is suitable for example for a CI/CD pipeline.	stdin/stdout
	MARK	MARK depends on Eclipse Xtext and reuses the UI elements of Eclipse and Xtext. Writing MARK requires an Eclipse IDE.	UI of Eclipse

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Orchestrator	Send assessment results

Codyze - More information

- Documentation:
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)
- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/codyze
- Training video:
  - https://youtu.be/f63Ba8QvChA

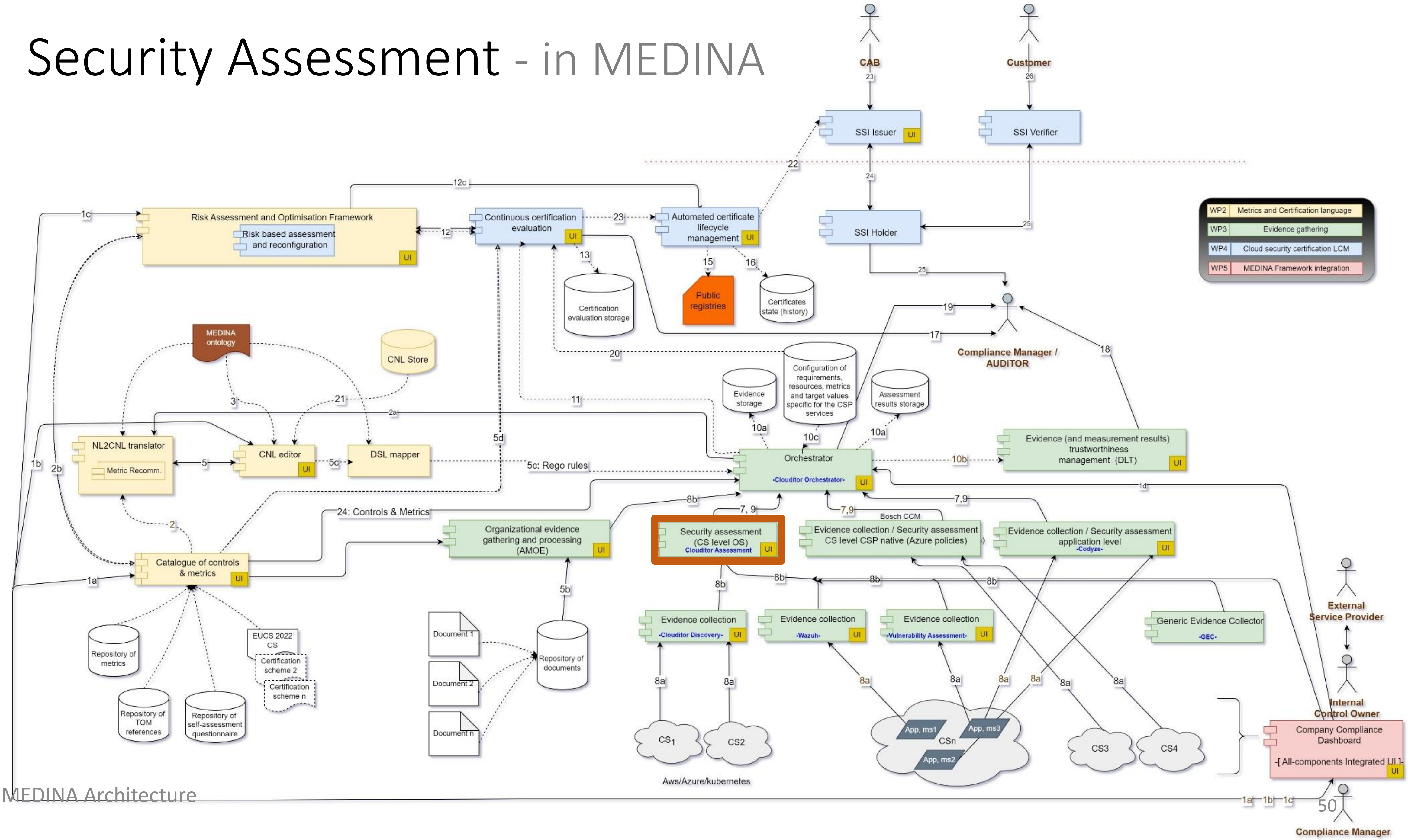
MEDINA

Security Assessment

Security Assessment – in a nutshell

- Security Assessment tool **assess evidences** according to MEDINA metrics stored in the Orchestrator
  - **Forwards** the results to the Orchestrator

Security Assessment - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
24: Controls & Metrics
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Security Assessment - Interfaces

	Name	Description	Technology
INTERFACES	Assessment interface	An interface for providing evidence to be assessed against suitable metrics	gRPC

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Orchestrator	Send assessment results

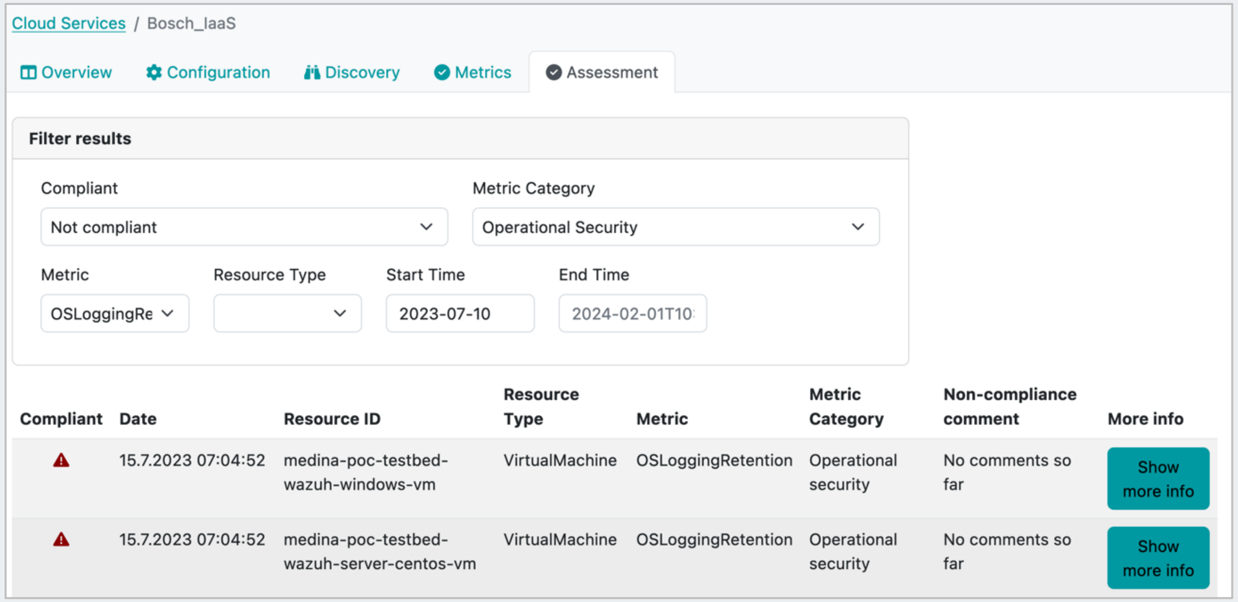
Security Assessment - More information

- Documentation:
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/security-assessment

- Training video:
  - https://youtu.be/Sl-7zfn5eK4

Orchestrator



Cloud Services / Bosch_IaaS

Filter results

Compliant: Not compliant

Metric Category: Operational Security

Metric: OSLoggingRe

Resource Type:

Start Time: 2023-07-10

End Time: 2024-02-01T10:

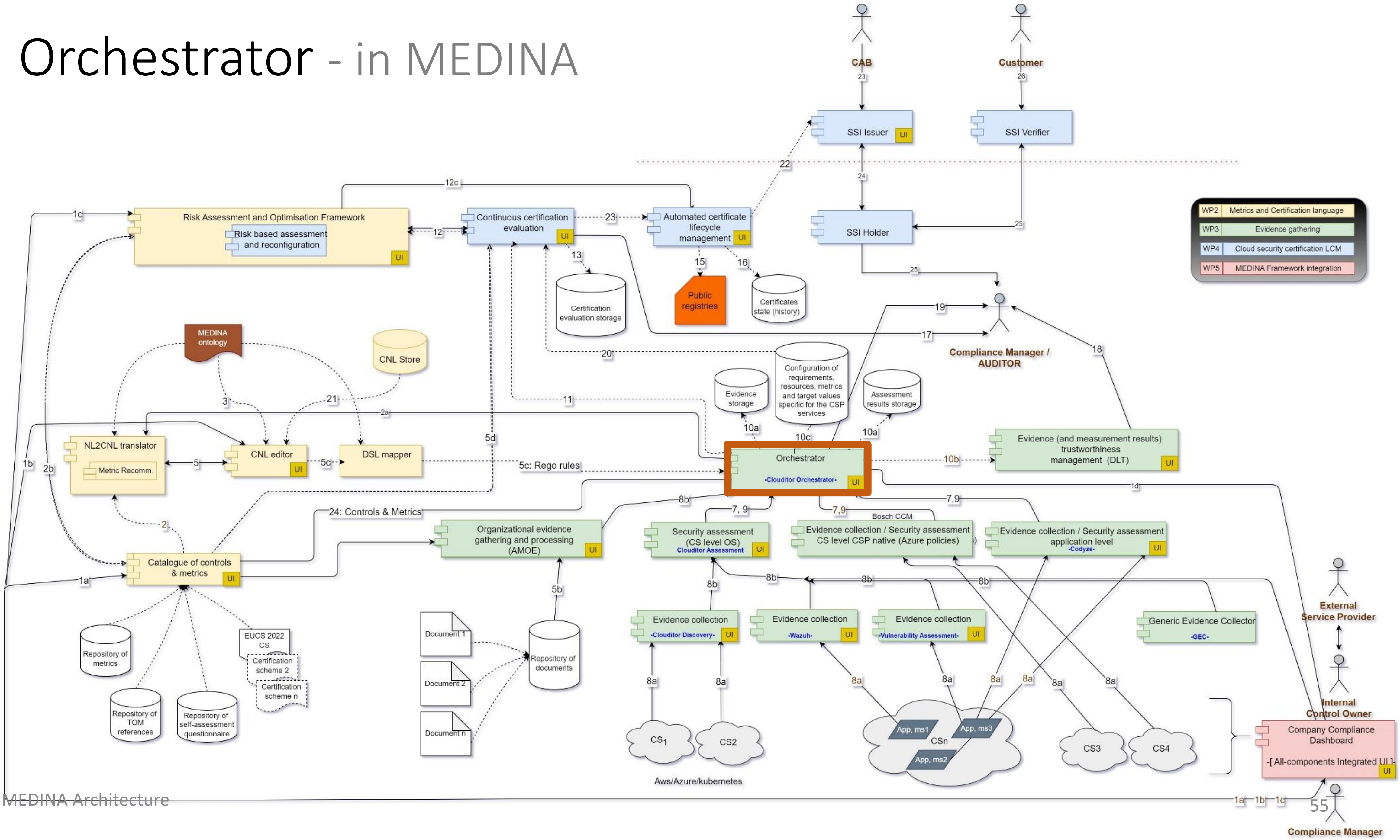
Compliant	Date	Resource ID	Resource Type	Metric	Metric Category	Non-compliance comment	More info
⚠	15.7.2023 07:04:52	medina-poc-testbed-wazuh-windows-vm	VirtualMachine	OSLoggingRetention	Operational security	No comments so far	Show more info
⚠	15.7.2023 07:04:52	medina-poc-testbed-wazuh-server-centos-vm	VirtualMachine	OSLoggingRetention	Operational security	No comments so far	Show more info

Orchestrator – in a nutshell

- Orchestrator is the central component of the framework which **processes evidence and assessment results**.
  - Receives data from the security assessment tools
  - Stores evidence, assessment results and other data.

- Allows users to **create new Cloud Services** and **Targets of Evaluation**

Orchestrator - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
MEDINA ontology
CNL Store
20
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
1b
2b
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
2
8b
24: Controls & Metrics
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
Internal Control Owner
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

Orchestrator - Interfaces

	Name	Description	Technology
INTERFACES	Assessment results storage	Provide assessment results which are then stored in the relevant database, and forwarded to the relevant components	REST / gRPC
	Database access	Provides access to stored evidence and assessment results, to the configuration of cloud services and targets of evaluation, etc.	REST / gRPC
	DLT storage	Interface to the DLT through which evidence and assessment result checksums are stored to the trustworthiness system.	REST
	Configure metrics and target values	Provides access to metrics and target values	REST / gRPC
	Graphical UI	GUI that allows to view stored data, configure cloud services and targets of evaluation, etc.	JavaScript

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Assessment tools	Receives assessment results from assessment tools
	Databases	Stores and retrieves evidence/assessment results from the relevant databases
	Trustworthiness system	Sends assessment result hashes to the trustworthiness system
	Metrics and target values repository	Retrieves metrics and target values for the assessment components and offers an API to modify them

Orchestrator- More information

- Documentation:
  - *Orchestrator User Manual* (https://zenodo.org/record/8425460)
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/orchestrator

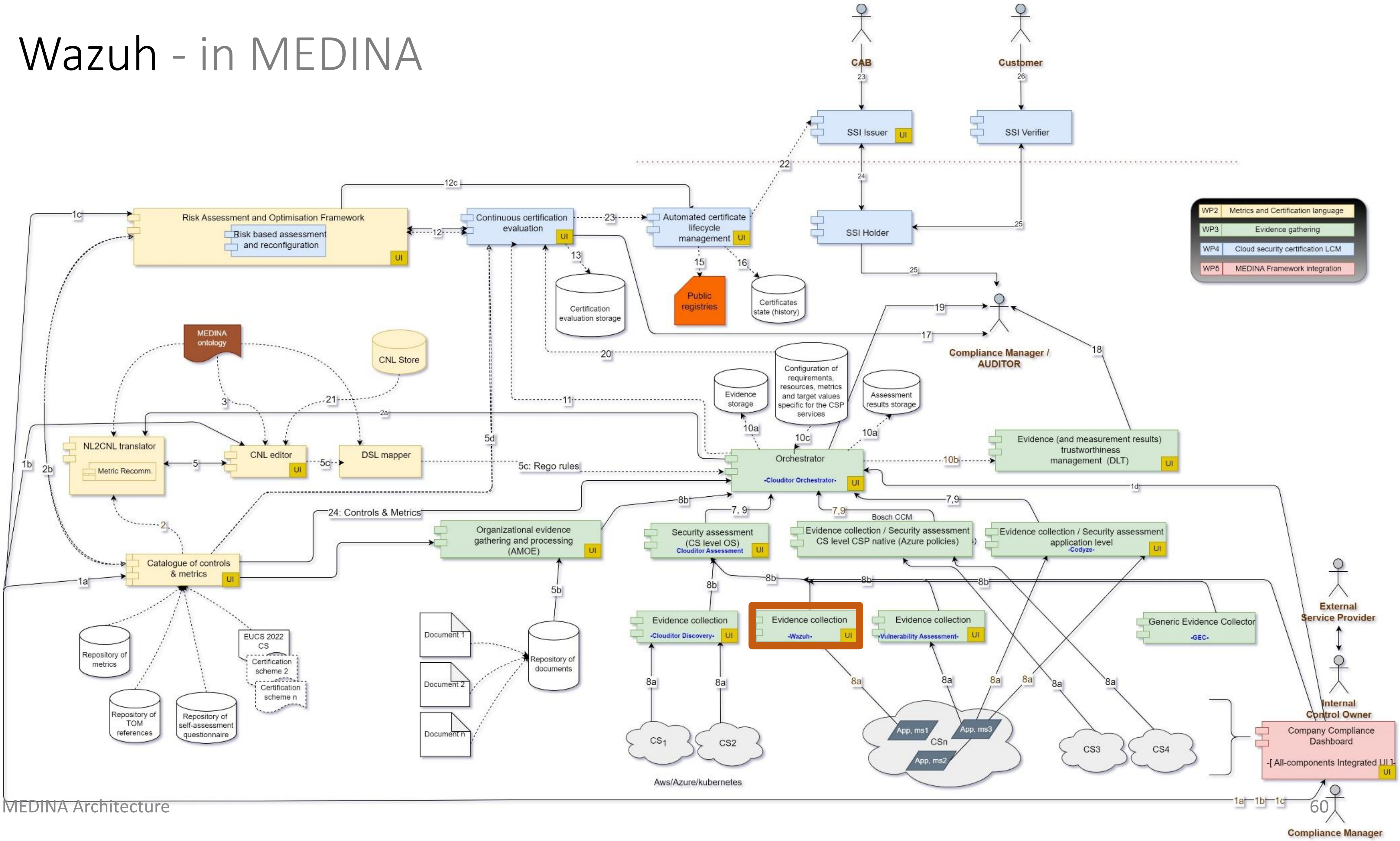
- Training video:
  - https://youtu.be/Sl-7zfn5eK4

Wazuh

Wazuh – in a nutshell

- Wazuh provides capabilities for **threat detection** to MEDINA users (CSPs)
  - Agents are installed directly on the (virtual) machines of the monitored infrastructure
  - Based in rules that include internal metrics and thresholds to trigger events or alerts
  - Controls malware protection, logging, threat analytics, and automatic monitoring (alerting)

Wazuh - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12c
1c
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
7, 9
7,9
7,9
24: Controls & Metrics
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Wazuh - Interfaces

	Name	Description	Technology
INTERFACES	Wazuh WUI	Main web UI	Web, based on Kibana
	ElasticSearch	ElasticSearch	HTTP API (REST)

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Wazuh and VAT Evidence Collector	Wazuh and VAT Evidence Collector pulls information from the Wazuh server (custom integration sub-component). Interface technology is HTTP REST API.

Wazuh - More information

- Documentation:
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)
- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/wazuh-vat-evidence-collector
- Training video:
  - https://youtu.be/9Y7Q9sclrsA

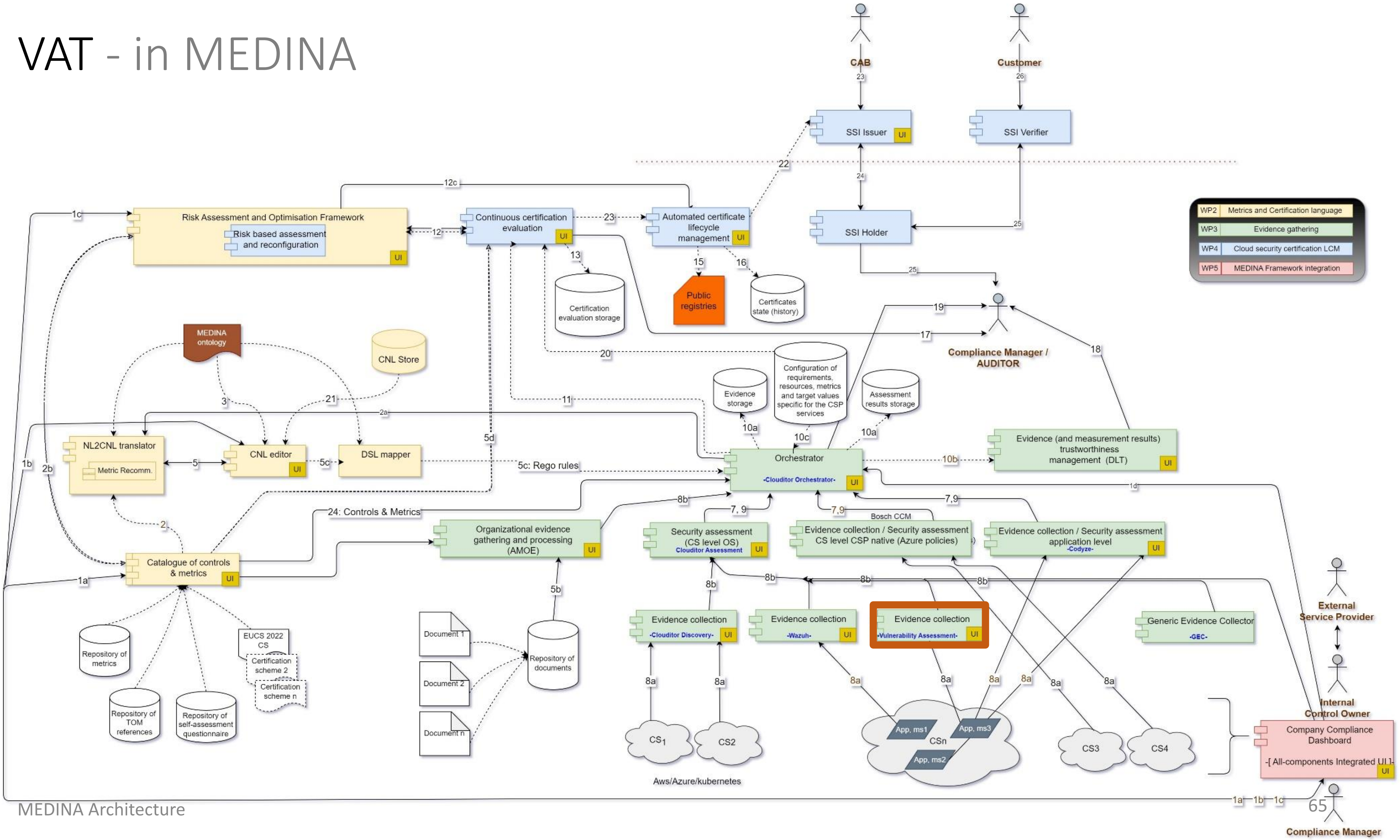
MEDINA

VAT - Vulnerability Assessment Tools

VAT – in a nutshell

- VAT comprises several tools to cover **vulnerability detection** and the **usage of encrypted communication protocols**
  - Is deployed in the CSP's infrastructure
  - Periodically scans the machines and servers on the monitored network
  - Tools comprise two web vulnerability scanners, a network discovery and auditing tool

VAT - in MEDINA



CAB
Customer
23
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
12
Continuous certification evaluation
23
Automated certificate lifecycle management
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
MEDINA ontology
CNL Store
20
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
10b
Evidence (and measurement results) trustworthiness management (DLT)
1d
1b
2b
2
8b
24: Controls & Metrics
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
Catalogue of controls & metrics
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
1a
1b
1c
Compliance Manager

VAT - Interfaces

	Name	Description	Technology
INTERFACES	Scan reports output	Pushing the results of scan tasks (vulnerability reports)	RabbitMQ (AMQP), JSON
	Management UI	Web UI to manage the scanning tasks and review their results	Web

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Wazuh and VAT Evidence Collector	Wazuh and VAT EC pulls information from the Wazuh server (sub-component). Interface technology is HTTP REST API.
		Wazuh and VAT EC pulls reports from VAT. Interface technology is HTTP REST API.

VAT - More information

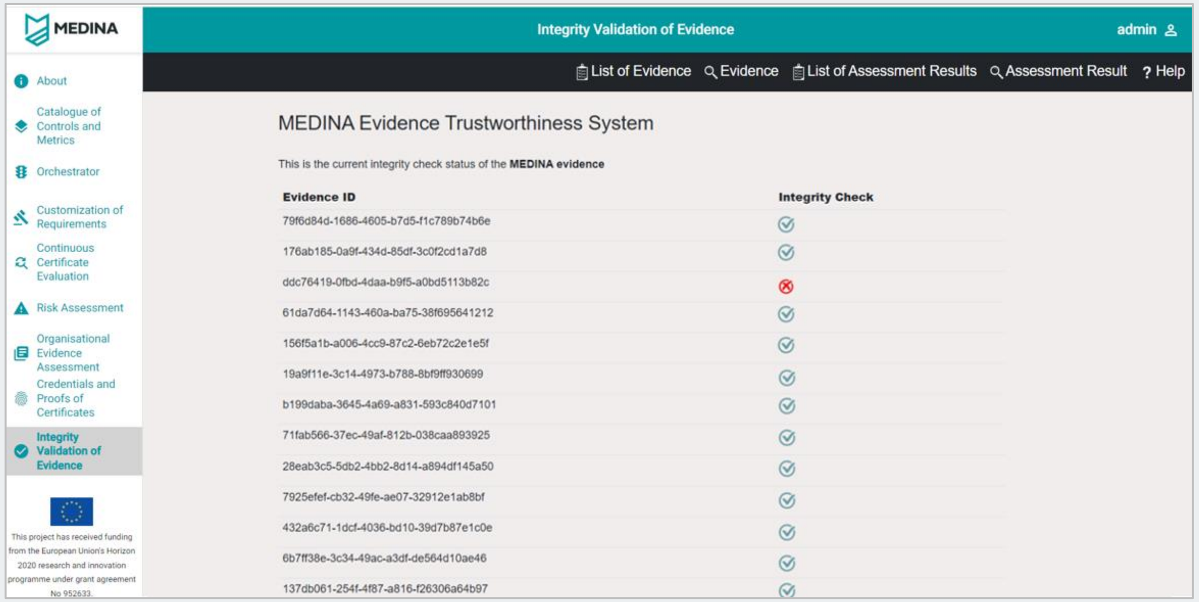
MEDINA

- Documentation:
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/wazuh-vat-evidence-collector

- Training video:
  - https://youtu.be/9Y7Q9sclrsA

Trustworthiness System


MEDINA
Integrity Validation of Evidence
admin
List of Evidence
Evidence
List of Assessment Results
Assessment Result
? Help
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Continuous Certificate Evaluation
Risk Assessment
Organisational Evidence Assessment
Credentials and Proofs of Certificates
Integrity Validation of Evidence

MEDINA Evidence Trustworthiness System

This is the current integrity check status of the **MEDINA evidence**

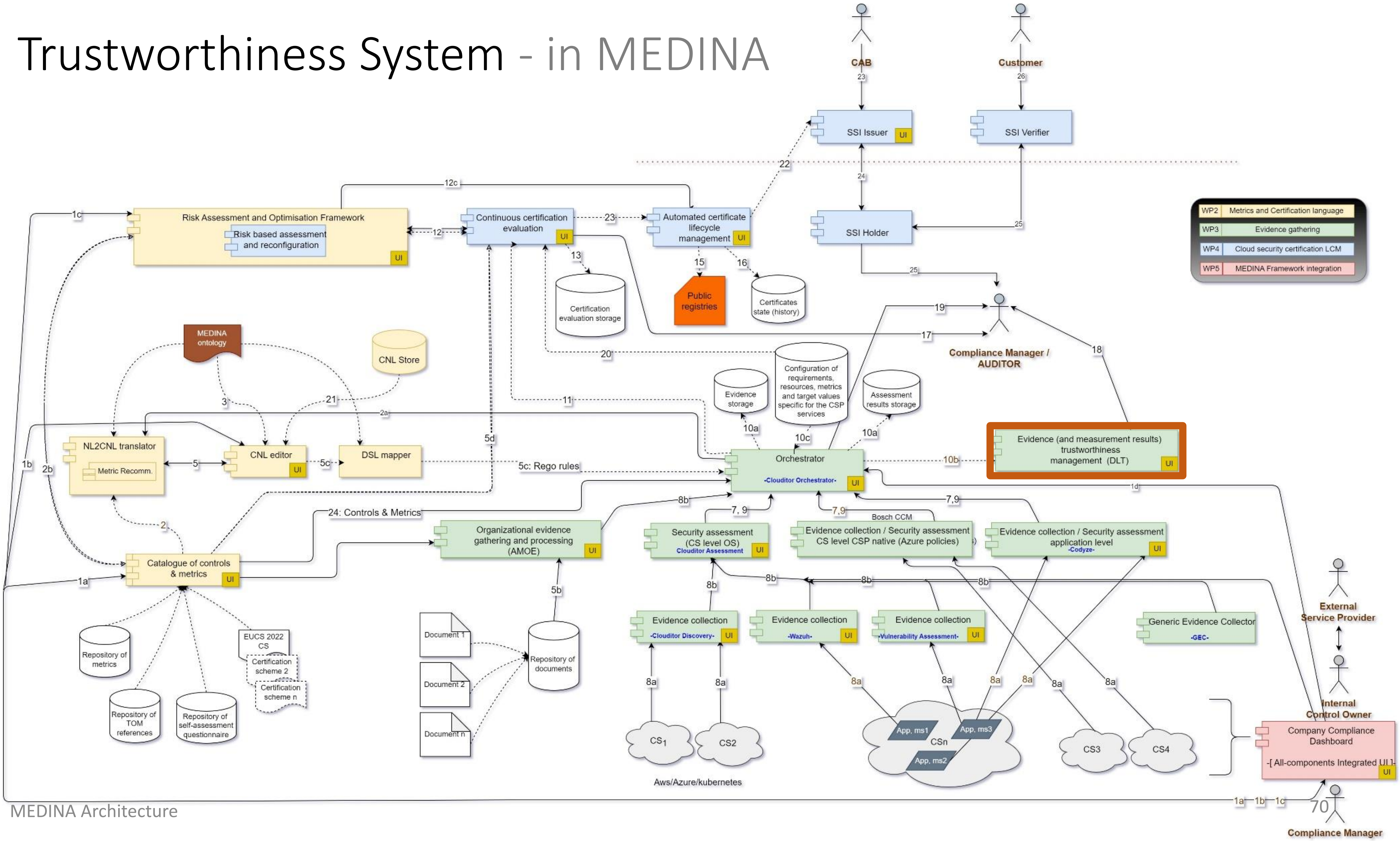
Evidence ID	Integrity Check
79f6d84d-1686-4605-b7d5-f1c789b74b6e	✓
176ab185-0a9f-434d-85df-3c0f2cd1a7d8	✓
ddc76419-0fbd-4daa-b9f5-a0bd5113b82c	⊗
61da7d64-1143-460a-ba75-38f695641212	✓
156f5a1b-a006-4cc9-87c2-6eb72c2e1e5f	✓
19a9f11e-3c14-4973-b788-8bf9ff930699	✓
b199daba-3645-4a69-a831-593c840d7101	✓
71fab566-37ec-49af-812b-038caa893925	✓
28eab3c5-5db2-4bb2-8d14-a894df145a50	✓
7925efef-cb32-49fe-ae07-32912e1ab8bf	✓
432a6c71-1dcf-4036-bd10-39d7b87e1c0e	✓
6b7ff38e-3c34-49ac-a3df-de564d10ae46	✓
137db061-254f-4f87-a816-f26306a64b97	✓

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

Trustworthiness System – in a nutshell

- Trustworthiness System provides a **secure mechanism** to maintain an **audit trail of evidence and assessment results**
  - Based in **Smart Contracts** backboned by a **Blockchain** network
  - Provides the **information to be audited** (about evidence and assessment results)
  - Provides **long-term information recording**
  - Provides a GUI to **access MEDINA's audited information**

Trustworthiness System - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
Internal Control Owner
CS_1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Trustworthiness System - Interfaces

INTERFACES	Name	Description	Technology
	Blockchain client	Saves in or obtains from the Blockchain the required evidence and assessment results.	REST API
	Graphical Viewer Client	GUI to manually check evidence and assessment results saved on the Blockchain.	WEB
	Automatic Verification Service	GUI for automatic verification of the integrity of evidence and assessment results.	WEB

INTERACTIONS WITH COMPONENTS	Component	Interface description
	Orchestrator	The orchestrator will provide (and check, if needed) the information (evidence/assessment results) to be saved on the Blockchain.
	Auditors	The auditors will check the information saved on the Blockchain manually (GUI) or automatically (via API)

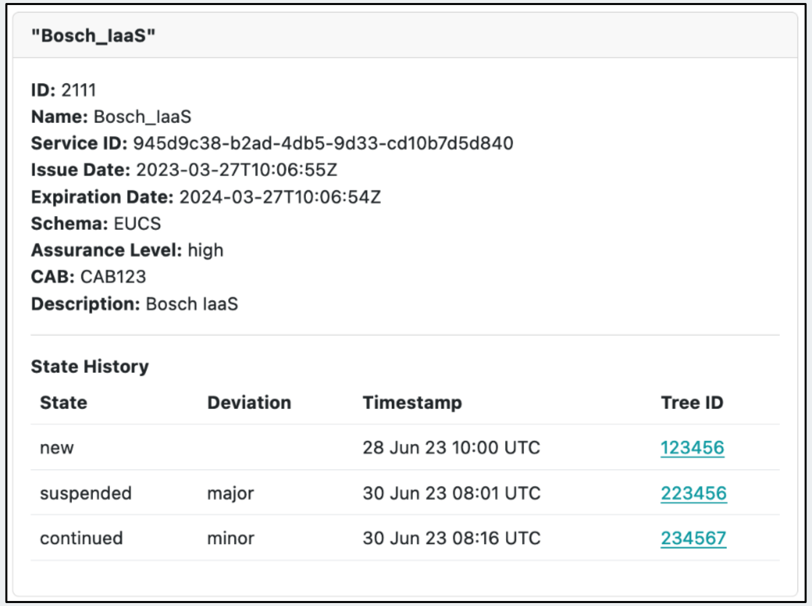
Trustworthiness System - More information

- Documentation:
  - *Integrity Validation of Evidence User manual* (https://zenodo.org/record/8425612)
  - *D3.3 – Tools and techniques for the management of trustworthy evidence-v3* (https://zenodo.org/record/7927220)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/blockchain-monitoring-tool

- Training video:
  - https://youtu.be/LO-gzX6LO0k

Lifecycle Manager



"Bosch_IaaS"

ID: 2111
Name: Bosch_IaaS
Service ID: 945d9c38-b2ad-4db5-9d33-cd10b7d5d840
Issue Date: 2023-03-27T10:06:55Z
Expiration Date: 2024-03-27T10:06:54Z
Schema: EUCS
Assurance Level: high
CAB: CAB123
Description: Bosch IaaS

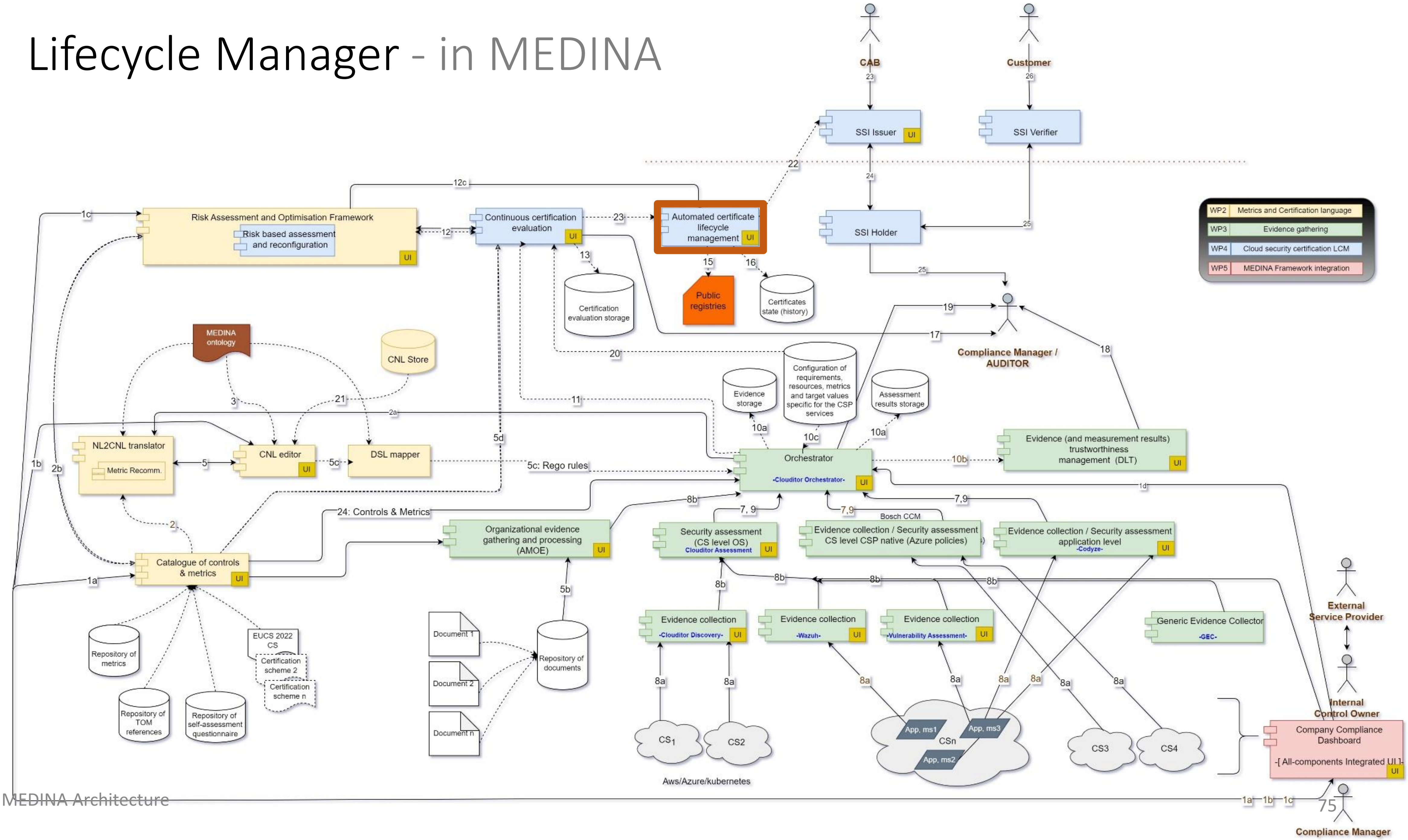
State History

State	Deviation	Timestamp	Tree ID
new		28 Jun 23 10:00 UTC	123456
suspended	major	30 Jun 23 08:01 UTC	223456
continued	minor	30 Jun 23 08:16 UTC	234567

Lifecycle Manager – in a nutshell

- Lifecycle Manager goal is to **aggregate relevant data** for the certification decision and automatically **derive a (preliminary) certificate state**
  - Receives data from RAOF (risk assessment deviation) and CCE (operational effectiveness)
  - Certificate state according to EUCS (new, suspended, withdrawn, etc.)

Lifecycle Manager - in MEDINA



CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

Lifecycle Manager - Interfaces

	Name	Description	Technology
INTERFACES	Certificate	Create, update, and delete certificates.	REST
	Evaluation	Provide results of the risk assessment	REST

	Component	Interface description
INTERACTIONS WITH COMPONENTS	CCE - Continuous Evaluation of Cloud Security Certification	**Obtain** data about operational effectiveness
	RAOF - Risk Assessment and Optimisation Framework	**Obtain** a risk assessment, including if a minor or major deviation has been identified.
	CAB / SSI Framework	**Forward** created certificates and updates to the SSI Framework.
	Orchestrator	**Store** certificate data in the *Orchestrator* database.

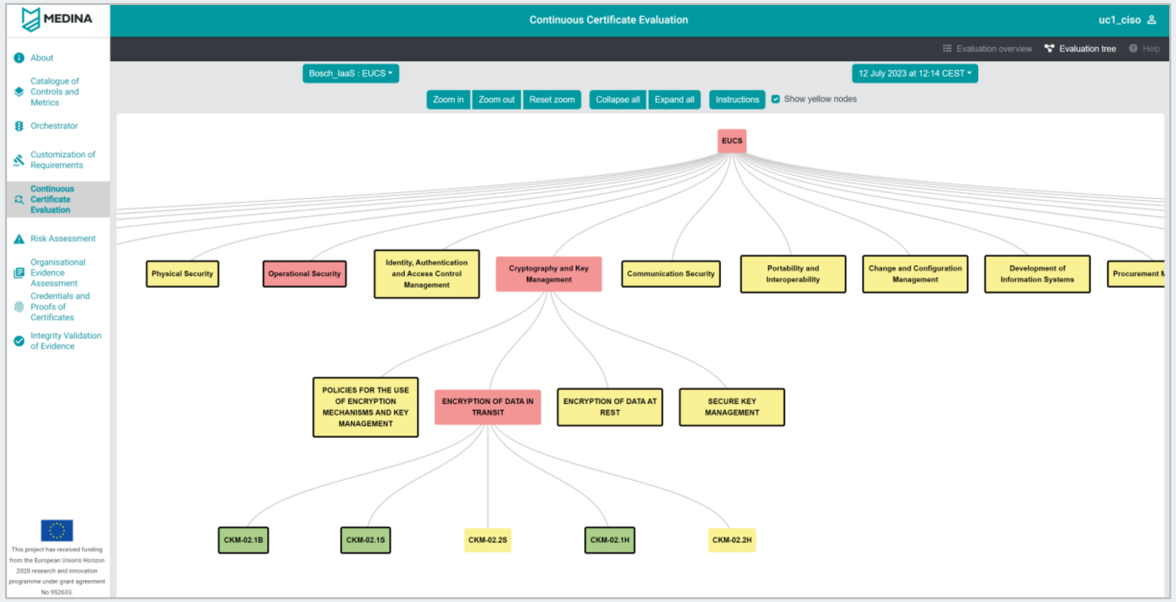
Lifecycle Manager - More information

- Documentation:
  - *D4.3 – Tools and Techniques for the Management and Evaluation of Cloud Security Certifications – v3* (https://zenodo.org/record/7927231)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/life-cycle-manager

- Training video:
  - https://youtu.be/R1z2-Q8Uh1Q

CCE - Continuous Certification Evaluation

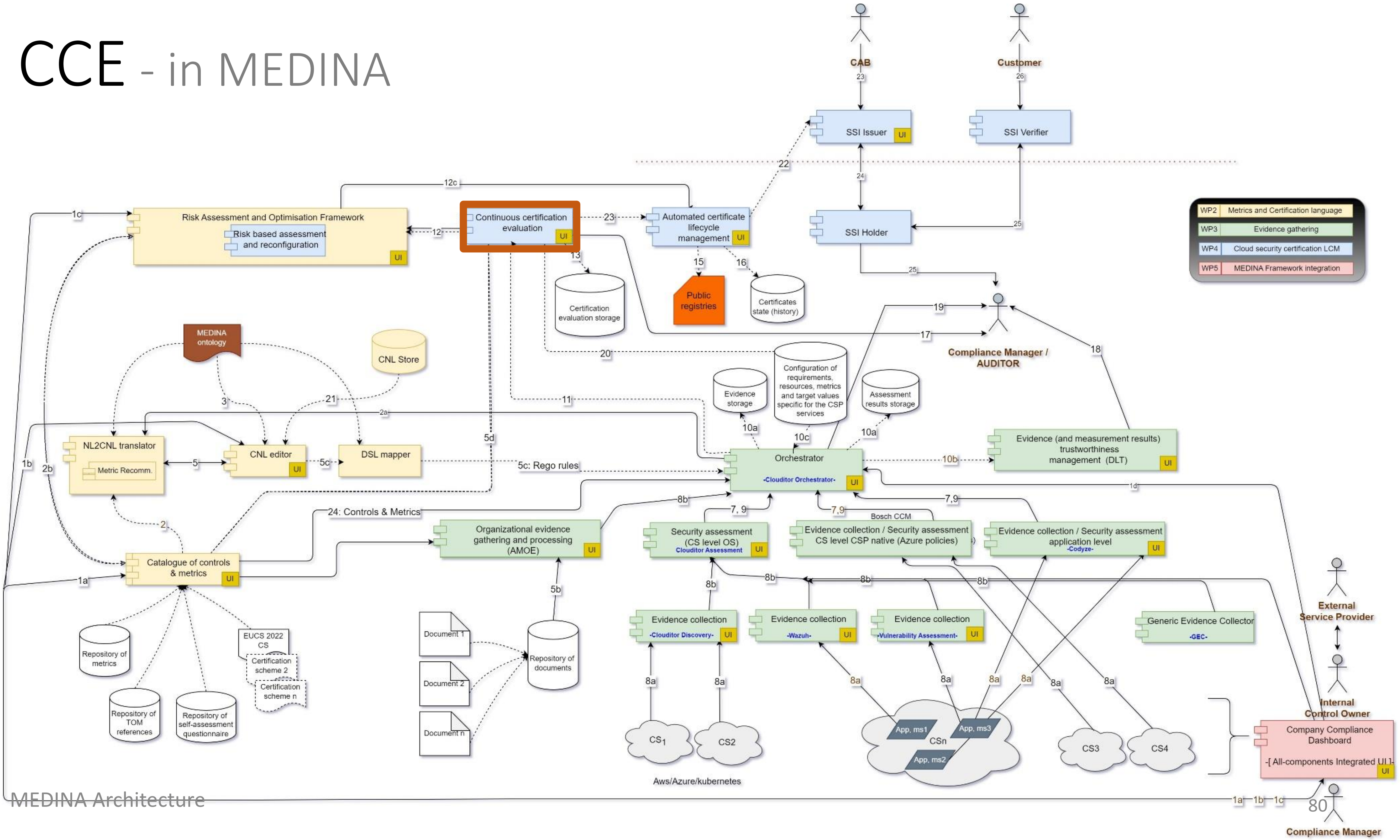

MEDINA
Continuous Certificate Evaluation
uc1_ciso
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Continuous Certificate Evaluation
Risk Assessment
Organisational Evidence Assessment
Credentials and Proofs of Certificates
Integrity Validation of Evidence
Evaluation overview
Evaluation tree
Help
Bosch_IaaS : EUCS
12 July 2023 at 12:14 CEST
Zoom in
Zoom out
Reset zoom
Collapse all
Expand all
Instructions
☑ Show yellow nodes
EUCS
Physical Security
Operational Security
Identity, Authentication and Access Control Management
Cryptography and Key Management
Communication Security
Portability and Interoperability
Change and Configuration Management
Development of Information Systems
Procurement M
POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT
ENCRYPTION OF DATA IN TRANSIT
ENCRYPTION OF DATA AT REST
SECURE KEY MANAGEMENT
CKM-02.1B
CKM-02.1S
CKM-02.2S
CKM-02.1H
CKM-02.2H

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

CCE – in a nutshell

- CCE **collects assessment results** and builds an **evaluation tree**, representing the assessment results on higher levels of the certification scheme
  - **Aggregates** single assessment values of a specific metric
  - Determines **compliance** with the different certification elements

CCE - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
External Service Provider
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration

MEDINA Architecture

CCE - Interfaces

	Name	Description	Technology
INTERFACES	Assessment Results	Receive assessment results from the *Orchestrator*.	REST / gRPC
	Certification evaluation	Send evaluation results to storage and the *RAOF*.	REST
	Statistics	Provide statistical data (*operational effectiveness data)* about the fulfilment of requirements over time.	REST
	Metric data	Obtain detailed metric data from the *CNL Editor*	REST
	Internal interfaces	Internal interfaces for the storage and retrieval of certification trees, as well as further communication between frontend, backend, and database	REST

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Orchestrator	Receive assessment results from the Orchestrator
	Risk Assessment and Optimisation Framework	Send certification trees to RAOF for risk assessment
	Life-Cycle Manager	Provide operational effectiveness data to be included in the certification decision
	CNL Editor	Obtain detailed metric data to be visualized in the frontend

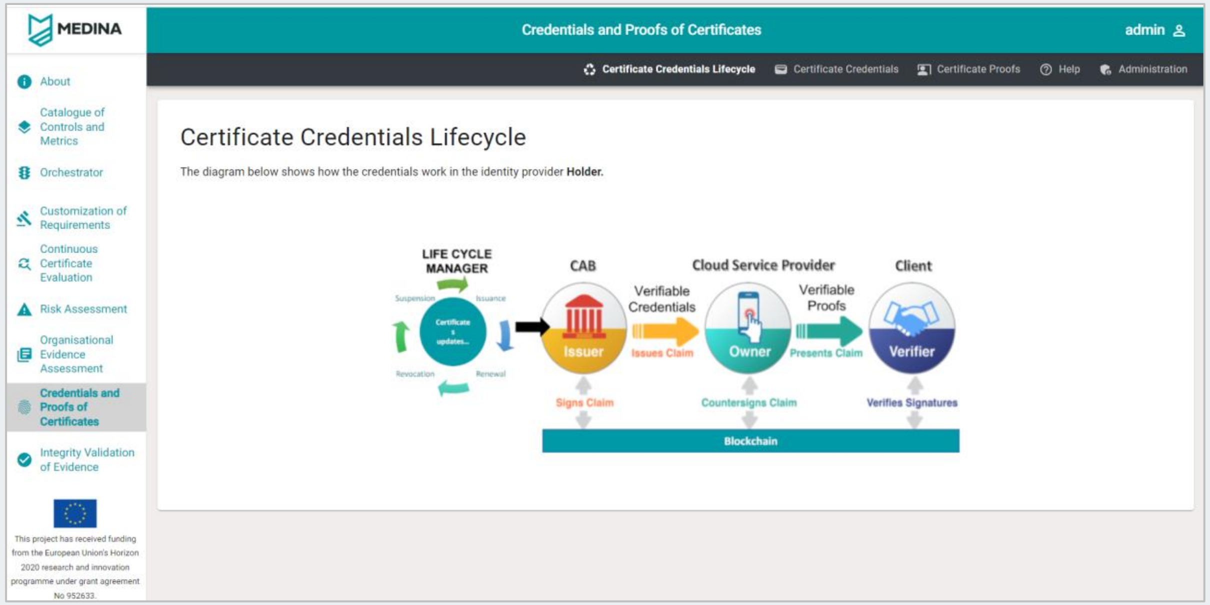
CCE - More information

- Documentation:
  - *CCE User Manual* (https://zenodo.org/record/8425414)
  - *D4.3 – Tools and Techniques for the Management and Evaluation of Cloud Security Certifications – v3* (https://zenodo.org/record/7927231)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/cce-frontend

- Training video:
  - https://youtu.be/R1z2-Q8Uh1Q

SSI - Self-Sovereign Identity Framework



Certificate Credentials Lifecycle

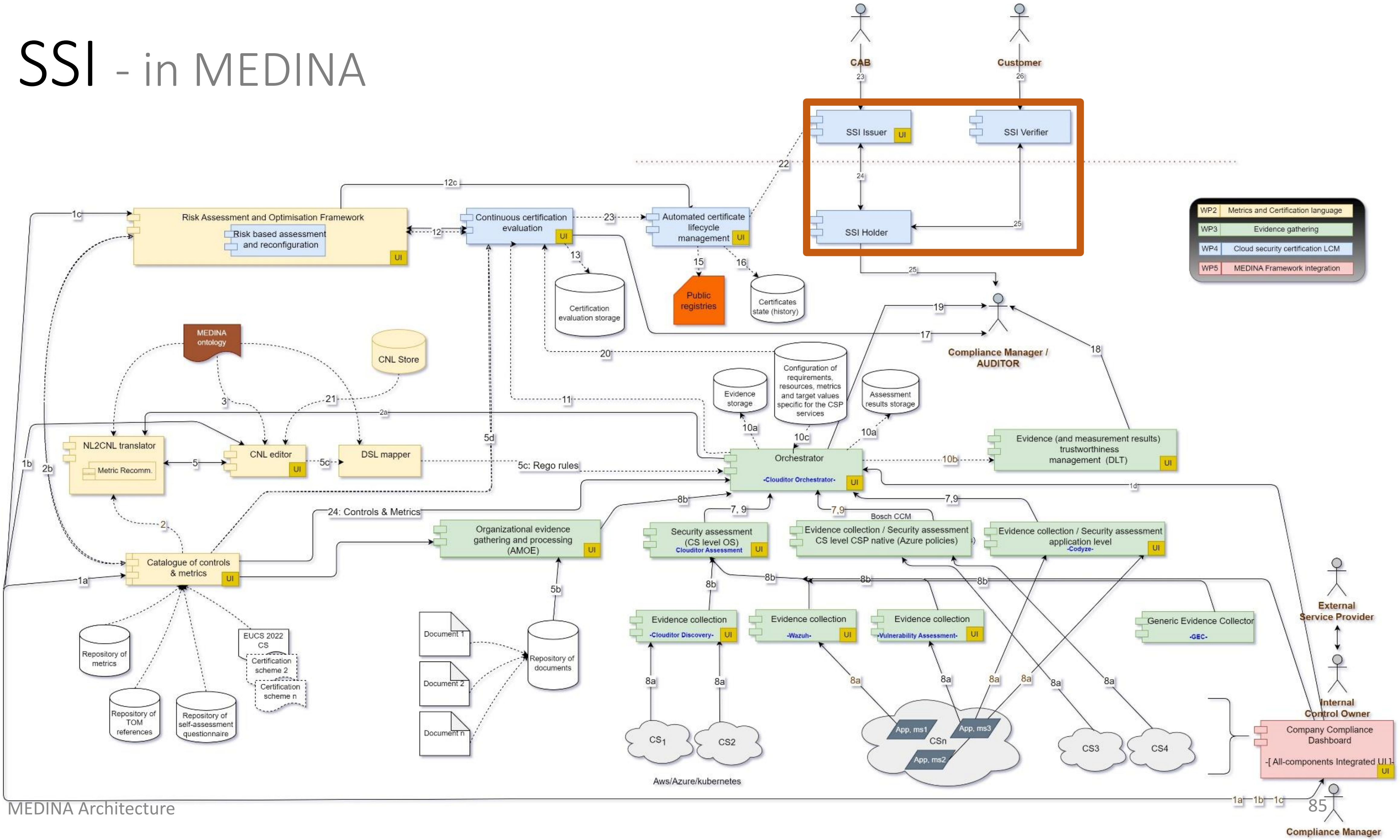
The diagram below shows how the credentials work in the identity provider **Holder.**

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

SSI – in a nutshell

- SSI provides CSPs the capability to **manage their own identity** through verifiable credentials
  - CSPs store identity on their own “user space”, without intervention of a third-party
  - Issues verifiable credentials about the certification status
  - Stores verifiable credentials about the certification status and provides verifiable proofs of them
  - Verifies verifiable proofs of the credentials

SSI - in MEDINA



CAB
Customer
23
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12c
1c
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
20
MEDINA ontology
CNL Store
3
21
2a
11
5d
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
7, 9
7,9
7,9
24: Controls & Metrics
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
Internal Control Owner
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

SSI - Interfaces

	Name	Description	Technology
INTERFACES	Life Cycle Manager (*LCM*)	Provides the security certificate state update.	REST API
	CAB	Sign and publicly publish security certifications	Web (aaS)
	CSP	List and proof generation of security certifications	Web (aaS)
	CSP client	Proof request and verification of security certifications.	Web (aaS)

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Life Cycle Manager (*LCM*)	It will provide the security certificate state update.

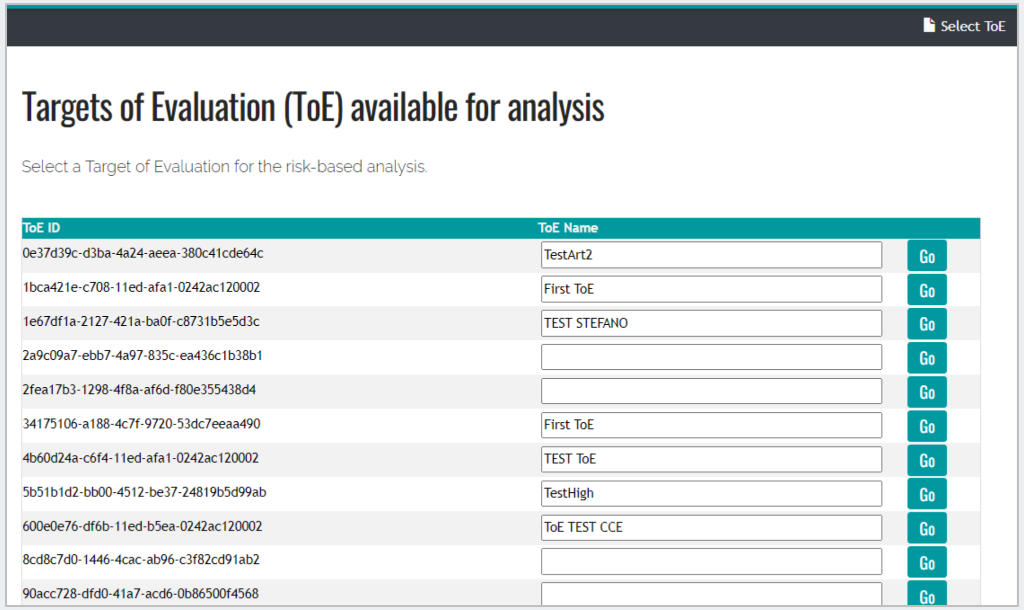
SSI - More information

- Documentation:
  - *Credentials and Proofs of Certificates User Manual* (https://zenodo.org/record/8425563)
  - *D4.3 – Tools and Techniques for the Management and Evaluation of Cloud Security Certifications – v3* (https://zenodo.org/record/7927231)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - Sorry, this repository is private

- Training video:
  - https://youtu.be/NKq4fWBAyXs

RAOF - Risk Assessment and Optimisation Framework



Targets of Evaluation (ToE) available for analysis

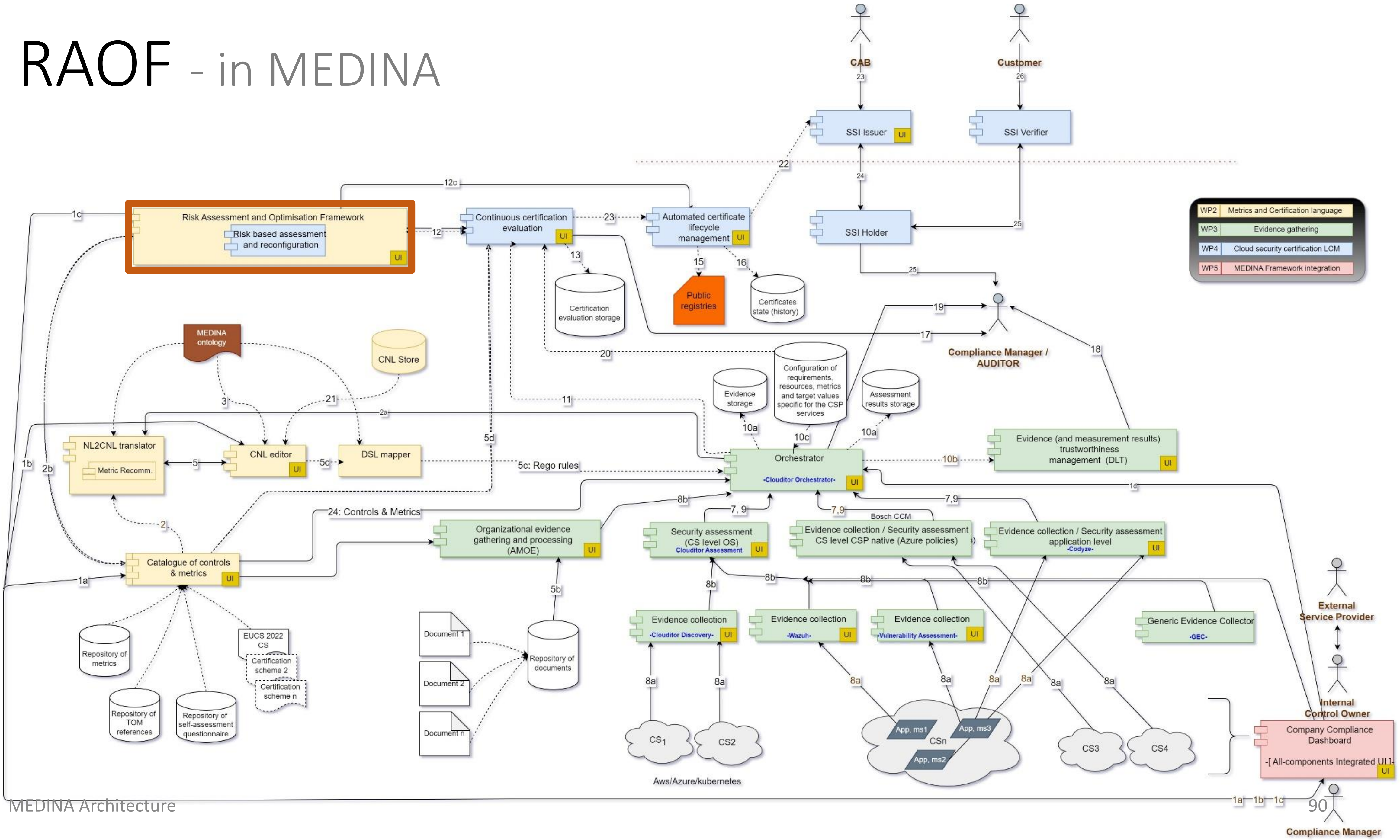
Select a Target of Evaluation for the risk-based analysis.

ToE ID	ToE Name	
0e37d39c-d3ba-4a24-aeea-380c41cde64c	TestArt2	Go
1bca421e-c708-11ed-afa1-0242ac120002	First ToE	Go
1e67df1a-2127-421a-ba0f-c8731b5e5d3c	TEST STEFANO	Go
2a9c09a7-ebb7-4a97-835c-ea436c1b38b1		Go
2fea17b3-1298-4f8a-af6d-f80e355438d4		Go
34175106-a188-4c7f-9720-53dc7eeaa490	First ToE	Go
4b60d24a-c6f4-11ed-afa1-0242ac120002	TEST ToE	Go
5b51b1d2-bb00-4512-be37-24819b5d99ab	TestHigh	Go
600e0e76-df6b-11ed-b5ea-0242ac120002	ToE TEST CCE	Go
8cd8c7d0-1446-4cac-ab96-c3f82cd91ab2		Go
90acc728-dfd0-41a7-acd6-0b86500f4568		Go

RAOF – in a nutshell

- RAOF goal is to **provide a risk-based analysis of non-conformities** to CSPs to perform risk assessment
  - Supports **manual analysis** by a *compliance manager*
    - Using the GUI (SATRA tool)
    - Providing information about addressed EUCS requirements
  - Supports **automatic (continuous) analysis**
    - Based on measured metrics, provided by monitoring tools
  - Provides **optimization** of the effort for ensuring compliance
    - Identifies the most cost-effective failed requirements

RAOF - in MEDINA



CAB
23
Customer
26
SSI Issuer UI
SSI Verifier
22
24
SSI Holder
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation UI
23
Automated certificate lifecycle management UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT) UI
1d
1b
2b
2
8b
7, 9
7,9
7,9
Bosch CCM
24: Controls & Metrics
Organizational evidence gathering and processing (AMOE) UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics UI
1a
5b
8b
8b
8b
8b
External Service Provider
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Repository of TOM references
Repository of self-assessment questionnaire
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

RAOF - Interfaces

	Name	Description	Technology
INTERFACES	Risk Assessment GUI	Graphical user interface of risk assessment	GUI
	Risk Assessment APIs	Set of machine-readable APIs for risk assessment	Rest API
	Non-conformity reporting API	API used for analysis and reporting a detected non-conformity.	Rest API

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Company Compliance Dashboard (CCD)	**Invokes** RAOF for the selection of suggested requirements to implement, analysis of security configuration, setting up resources and possible impact.
	Continuous Certification Evaluation (CCE)	**Invokes** RAOF for the evaluation of the detected non-conformity
	Life-Cycle -Manager (LCM)	**Consumes** the result of the risk-based non-conformity evaluation.
	Orchestrator	**Notifies** about creation/deletion of a Target of Evaluation.
	Catalogue	**Sends RAOF** the results (answers) of a questionnaire.

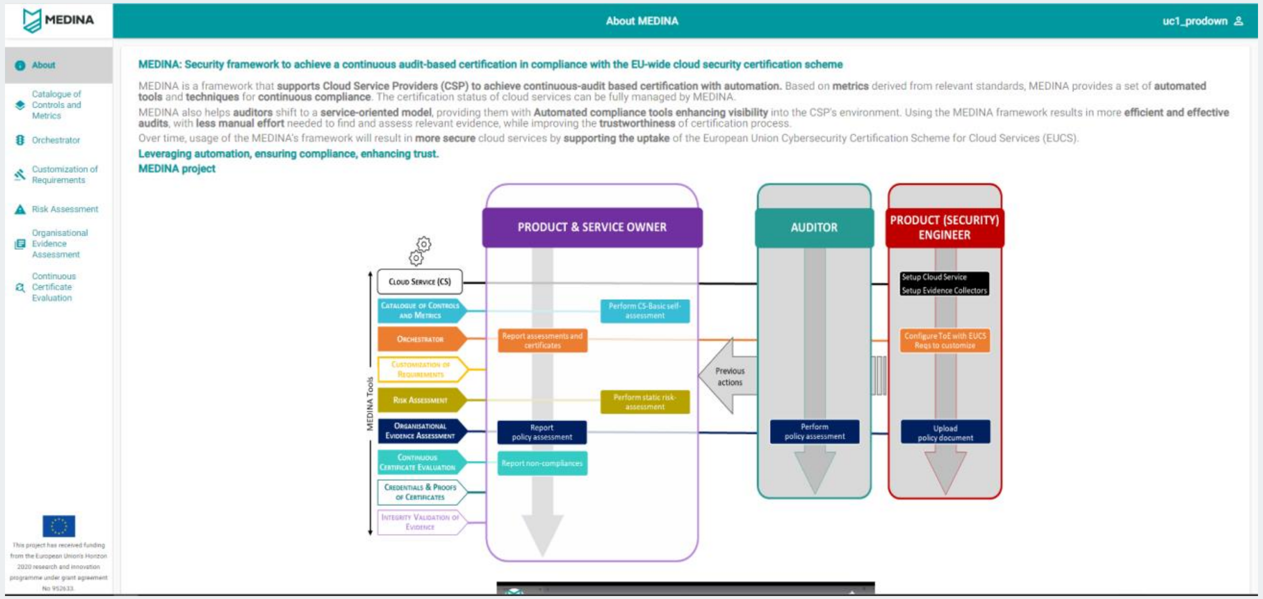
RAOF - More information

- Documentation:
  - *Risk Assessment User manual* (https://zenodo.org/record/8425537)
  - *D3.6 – Tools and techniques for collecting evidence of technical and organisational measures – v3* (https://zenodo.org/record/7927225)
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Git repository (source code, API):
  - https://git.code.tecnalia.com/medina/public/static-risk-assessment-and-optimization-framework

- Training video:
  - https://youtu.be/R1z2-Q8Uh1Q

IUI – Integrated User Interface



MEDINA
About MEDINA
uc1_prodown
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation

MEDINA: Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

MEDINA is a framework that **supports Cloud Service Providers (CSP) to achieve continuous-audit based certification with automation.** Based on **metrics** derived from relevant standards, MEDINA provides a set of **automated tools** and **techniques** for **continuous compliance**. The certification status of cloud services can be fully managed by MEDINA.

MEDINA also helps **auditors** shift to a **service-oriented model**, providing them with **Automated compliance tools enhancing visibility** into the CSP's environment. Using the MEDINA framework results in more **efficient and effective audits**, with **less manual effort** needed to find and assess relevant evidence, while improving the **trustworthiness** of certification process.

Over time, usage of the MEDINA's framework will result in **more secure** cloud services by **supporting the uptake** of the European Union Cybersecurity Certification Scheme for Cloud Services (EUCS).

Leveraging automation, ensuring compliance, enhancing trust.

MEDINA project

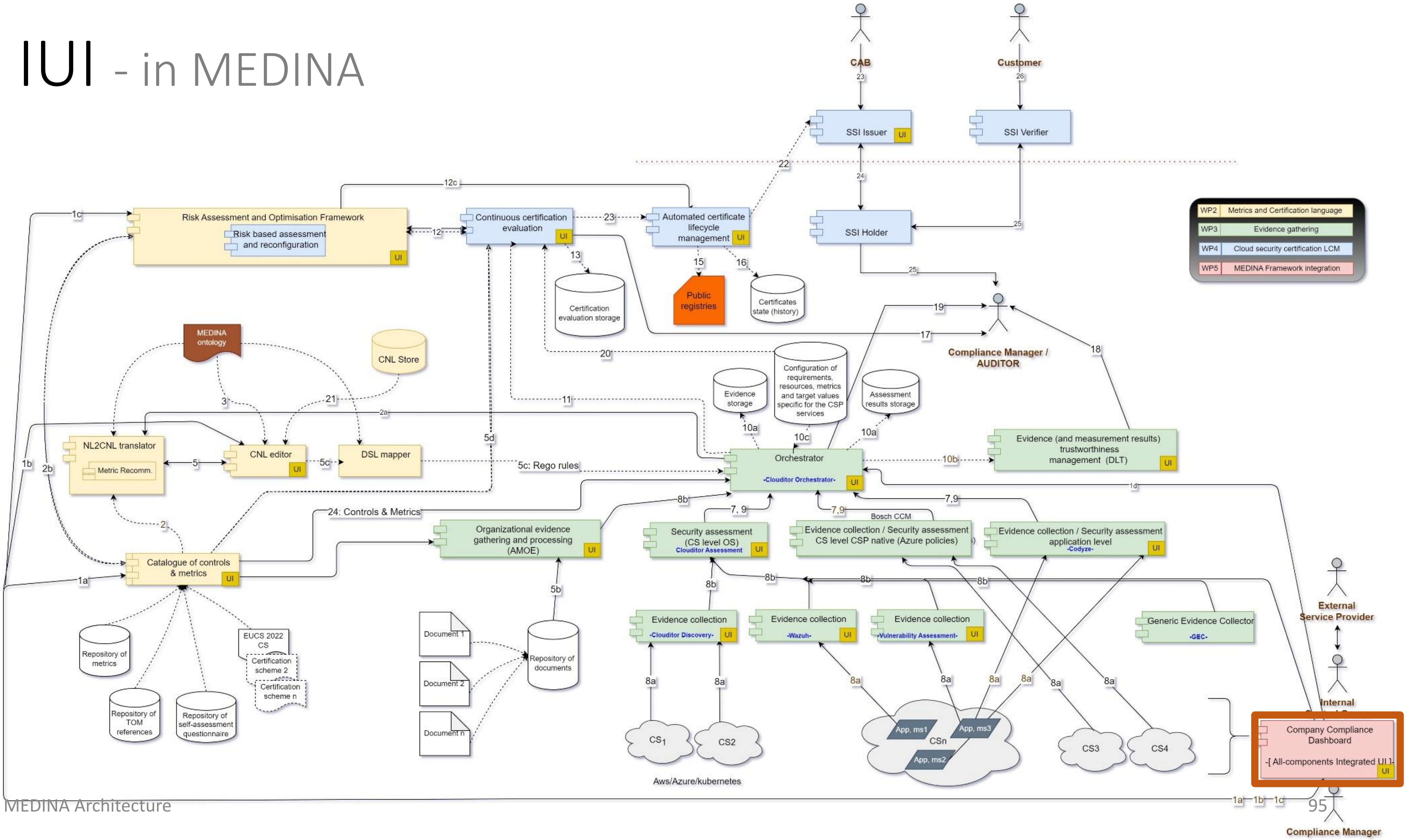
PRODUCT & SERVICE OWNER
AUDITOR
PRODUCT (SECURITY) ENGINEER
MEDINA Tools
Cloud Service (CS)
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation
Credentials & Proofs of Certificates
Integrity Validation of Evidence
Perform CS-Basic self-assessment
Report assessments and certificates
Perform static risk-assessment
Report policy assessment
Report non-compliances
Previous actions
Perform policy assessment
Setup Cloud Service
Setup Evidence Collectors
Configure ToE with EUCS Reqs to customize
Upload policy document

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

IUI – in a nutshell

- The IUI is the component that **encapsulates the graphical user interfaces** (GUI) of all MEDINA components.
  - Is the **landing page** of the MEDINA framework
  - Based in **micro-frontend** architecture
  - Common **look & feel** for all the tools: colors, toolbar, footer…
  - Interacts with Keycloak for the **authentication** and **authorization**

IUI - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
3
21
11
2a
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
8b
7, 9
7,9
7,9
Bosch CCM
24: Controls & Metrics
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
1a
Catalogue of controls & metrics
UI
5b
8b
8b
8b
8b
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

IUI - Interfaces

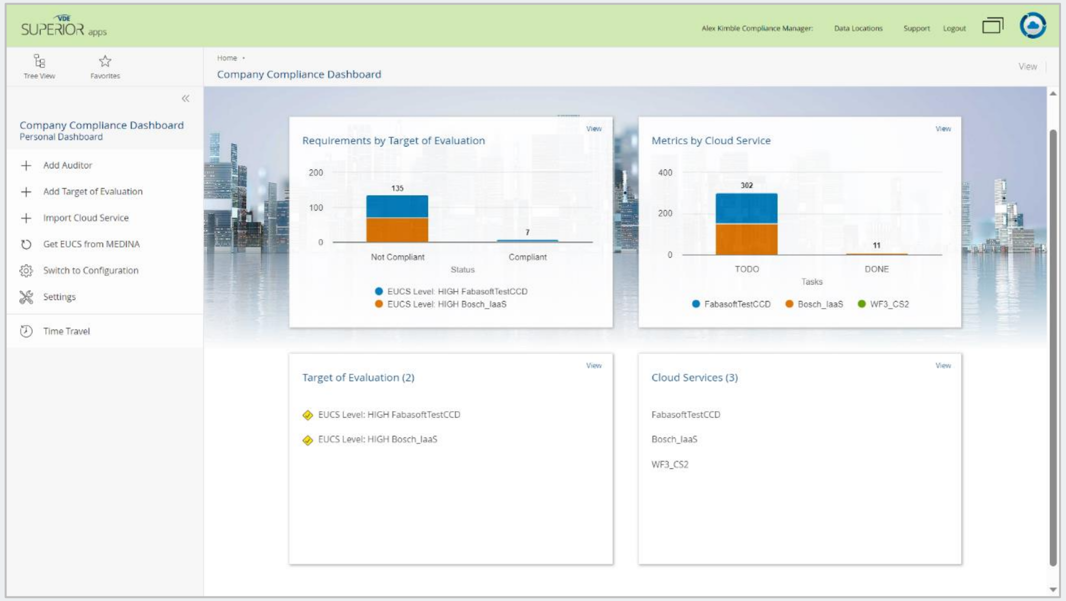
INTERFACES	Name	Description	Technology
	IUI	Main point of access to the framework, integrates all the other micro frontends	HTTPS (browser)

INTERACTIONS WITH COMPONENTS	Component	Interface description
	Catalogue	Integrates the Catalogue UI
	CNL Editor	Integrates the CNL Editor UI
	CCE	Integrates the CCE UI
	AMOE	Integrates the AMOE UI
	Orchestrator	Integrates the Orchestrator UI
	RAOF	Integrates the RAOF UI
	Trustworthiness System	Integrates the Trustworthiness System UI
	SSI Framework	Integrates the SSI Framework UI

IUI - More information

- Documentation:
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)
- Git repository:
  - Sorry, this repository is private
- Training video:
  - https://youtu.be/WwRdwi9lIZ4

CCD – Company Compliance Dashboard



Company Compliance Dashboard

Company Compliance Dashboard
Personal Dashboard

Requirements by Target of Evaluation

● EUCS Level: HIGH FabasoftTestCCD
● EUCS Level: HIGH Bosch_IaaS

Metrics by Cloud Service

● FabasoftTestCCD ● Bosch_IaaS ● WF3_CS2

Target of Evaluation (2)

EUCS Level: HIGH FabasoftTestCCD

EUCS Level: HIGH Bosch_IaaS

Cloud Services (3)

FabasoftTestCCD

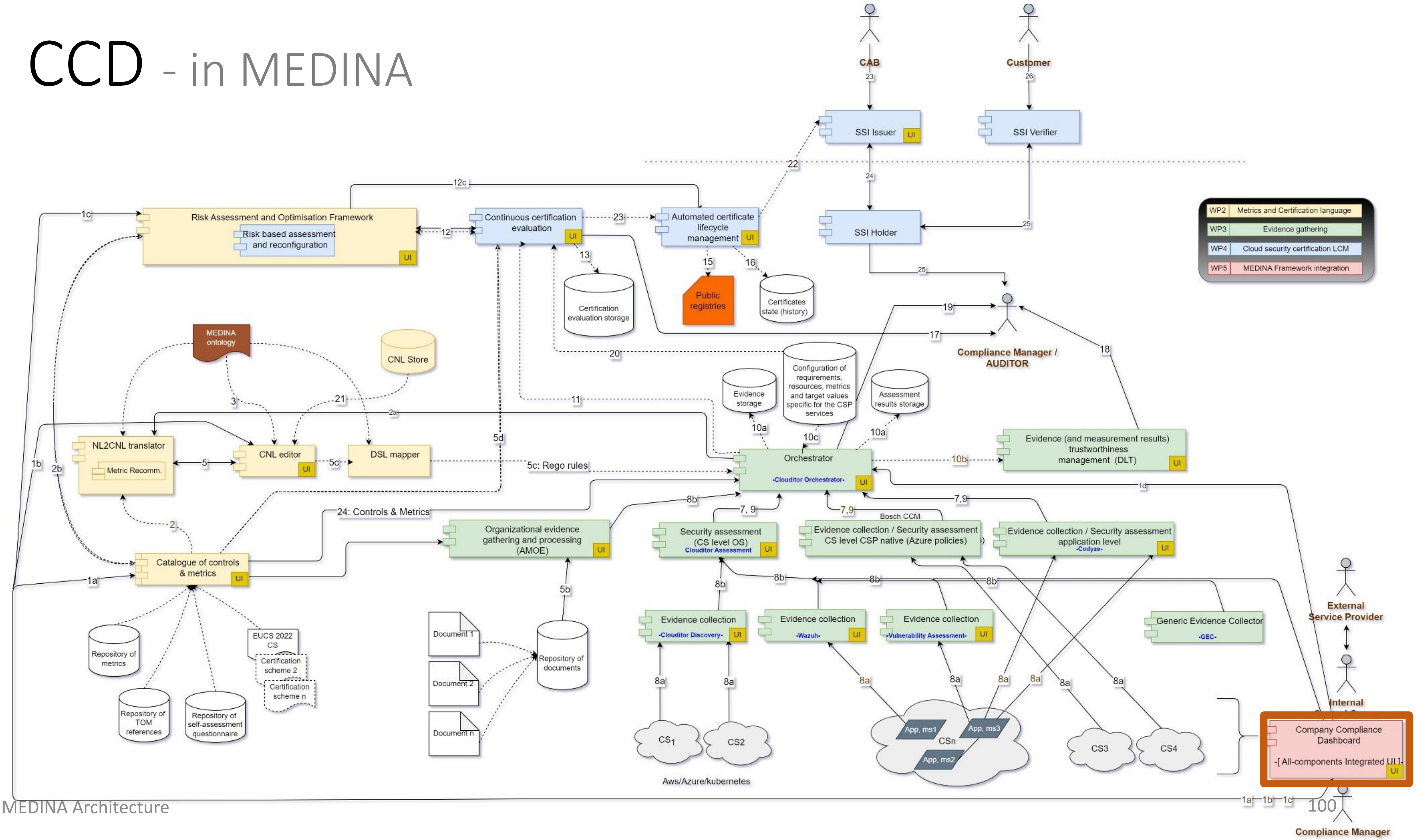
Bosch_IaaS

WF3_CS2

CCD – in a nutshell

- The CCD is the equivalent of the IUI, but **based in an already existing tool** that **connects to the MEDINA core APIs**
  - Company tool to manage all cloud-related certification processes
  - Uses the **Fabasoft Cloud UI** and high-charts functionalities
  - Demonstrates the **modularity** of the MEDINA framework, which customers can integrate seamlessly **into their own ecosystem**

CCD - in MEDINA


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
22
24
SSI Holder
25
25
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
Configuration of requirements, resources, metrics and target values specific for the CSP services
MEDINA ontology
CNL Store
3
21
11
2a
Evidence storage
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
Internal
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

CCD - Interfaces

	Name	Description	Technology
INTERFACES	CCD	Company-based dashboard to access the MEDINA framework components via APIs	HTTPS (browser), app.ducx.

	Component	Interface description
INTERACTIONS WITH COMPONENTS	Catalogue	Import the EUCS schema
	SATRA	The Risk-Assessment workflow
	AMOE	For organizational evidences
	Orchestrator	Receive and send audit relevant information, CCE and CNL results

CCD - More information

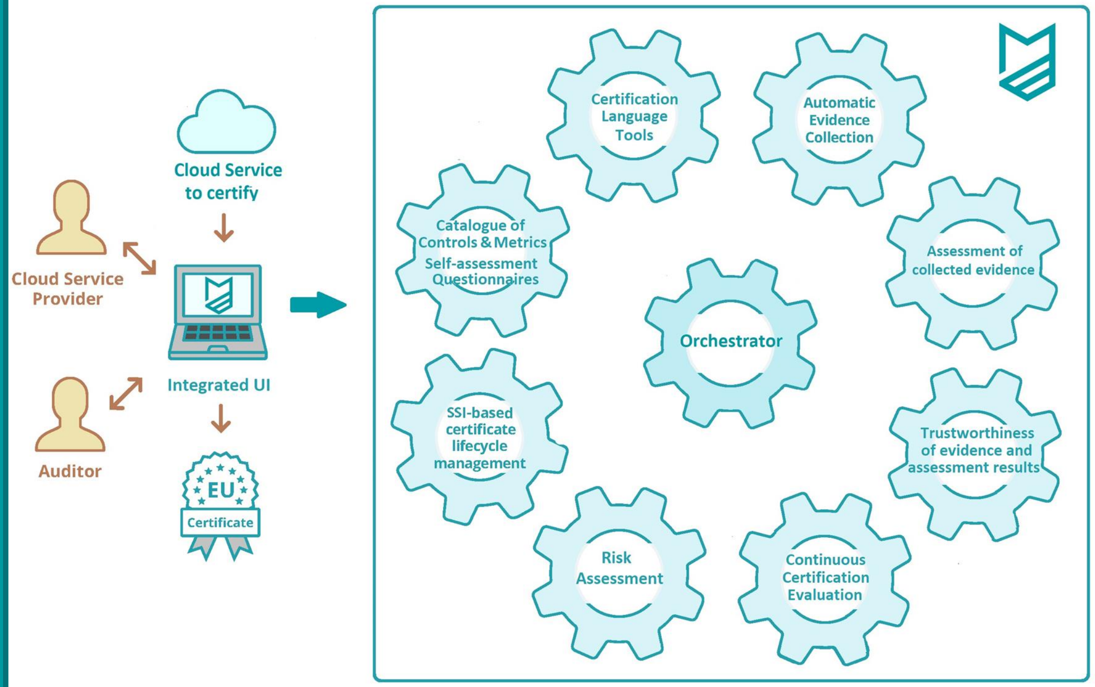
- Documentation:
  - *D5.5 MEDINA integrated solution-v3* (https://zenodo.org/record/8214685)

- Training video:
  - https://youtu.be/hgkisRsELr0

MEDINA Architecture

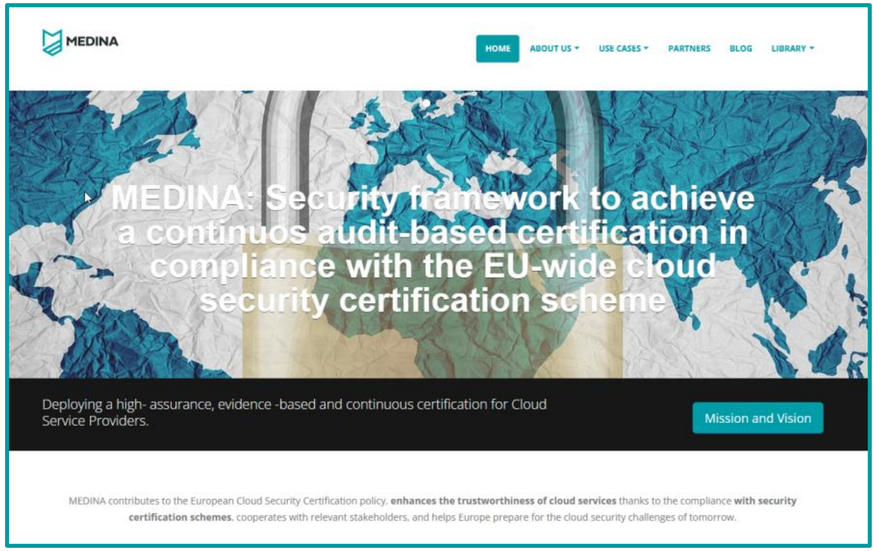
- Further information

MEDINA


Cloud Service to certify
Cloud Service Provider
Auditor
Integrated UI
EU
Certificate
Certification Language Tools
Automatic Evidence Collection
Catalogue of Controls & Metrics
Self-assessment Questionnaires
Assessment of collected evidence
Orchestrator
SSI-based certificate lifecycle management
Trustworthiness of evidence and assessment results
Risk Assessment
Continuous Certification Evaluation

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrators are available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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

MEDINA

Installation of the MEDINA Framework

Neda Jahandarpour, HPE

September 2023

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

Chapters

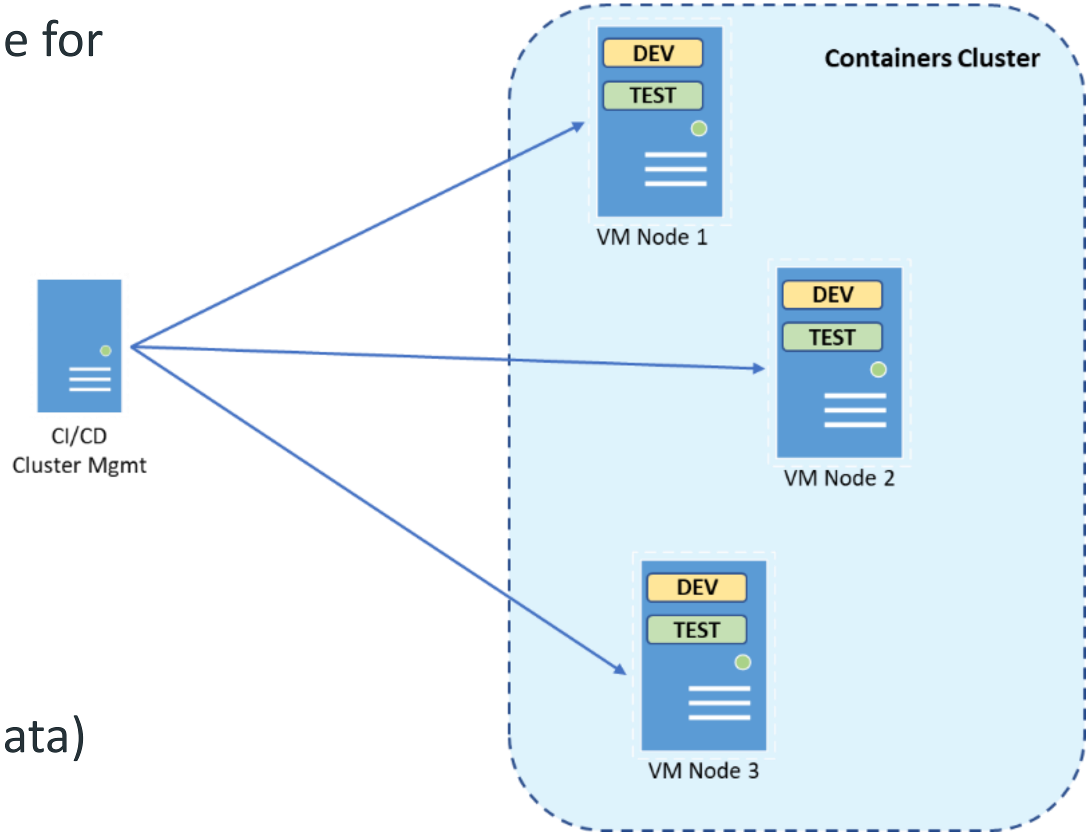
- Hardware Infrastructure
- Installation of Kubernetes cluster
- Tools used
- CI/CD Pipeline
- Demo
- Further information

Installation of the MEDINA Framework

- Hardware Infrastructure
- Installation of Kubernetes cluster

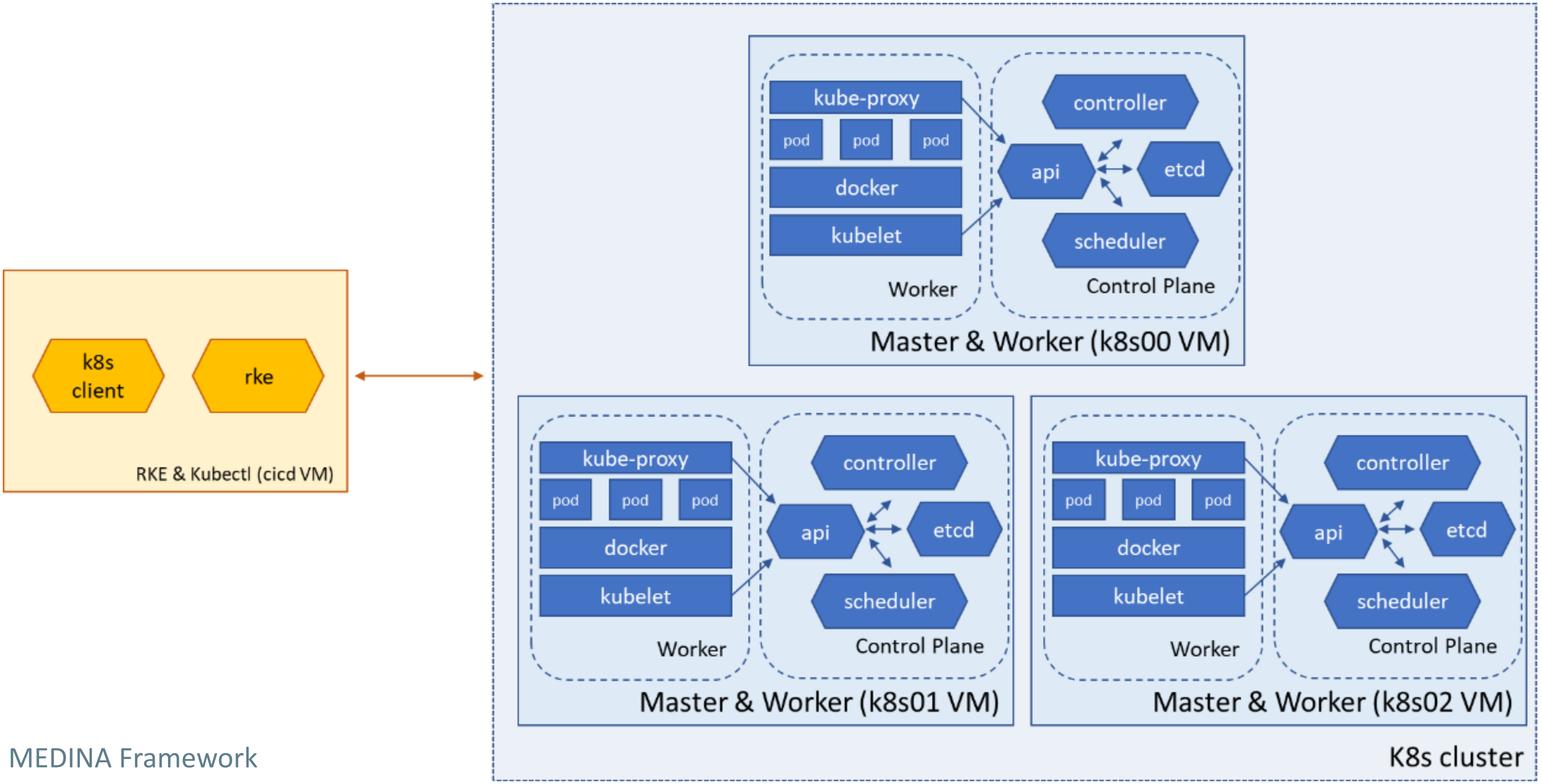
Hardware Infrastructure

- Four Virtual Machines (VMs):
  - One VM dedicated to the CI/CD automation engine for Agile/SecDevOps deployment.
    - RAM: 16 GB
    - Cores: 4
    - Hard Disk: 400 GB (sw)
    - OS: Ubuntu OS 20.04
  - Three VMs for the Kubernetes cluster:
    - RAM: 16 GB
    - Cores: 8
    - Hard Disk: 200 GB (sw) + 200 GB (persistent data)
    - OS: Ubuntu OS 20.04



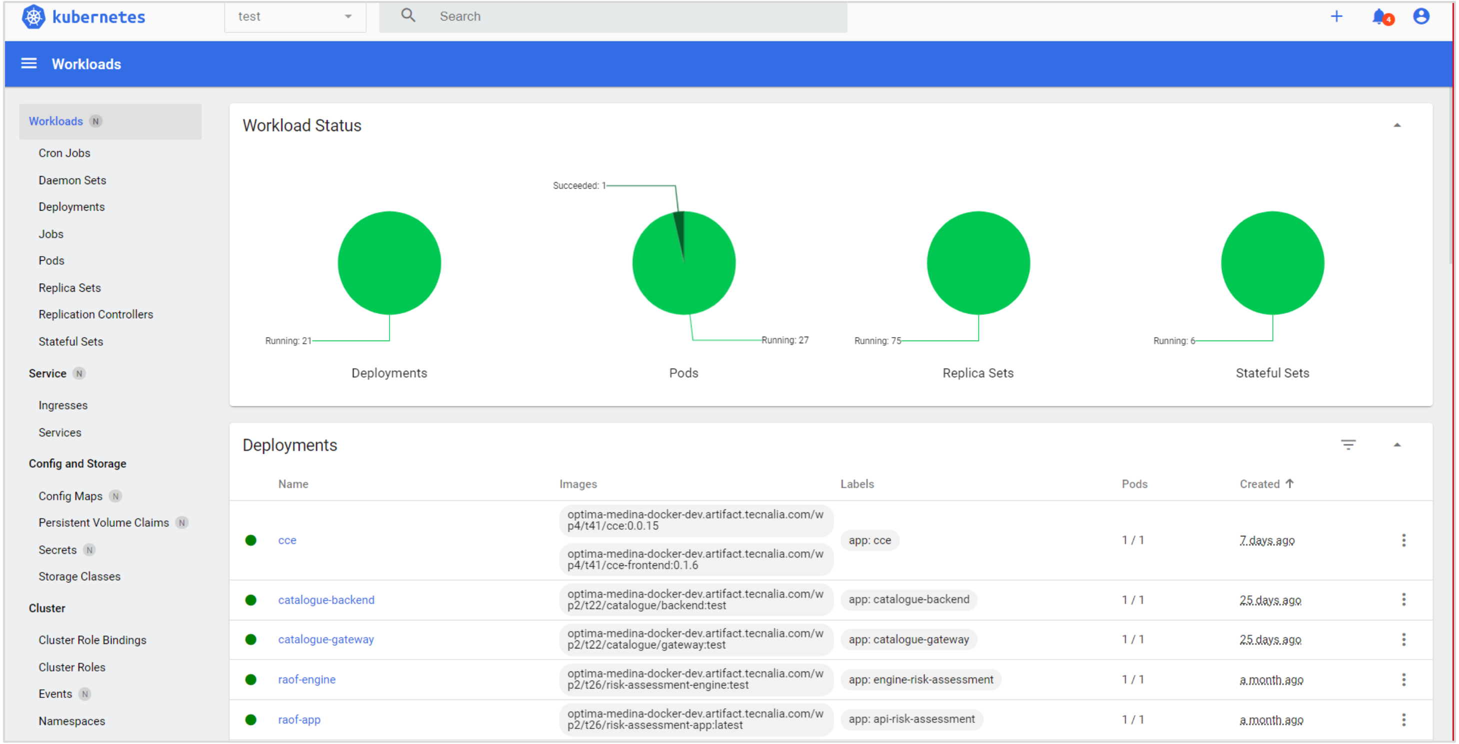
Installation of Kubernetes Cluster

Kubernetes orchestrates the deployment and management of the MEDINA containers running on multiple nodes. The Kubernetes cluster is configured and managed by Rancher Kubernetes Engine (RKE)



Kubernetes Dashboard

To deploy containerized applications to a Kubernetes cluster, troubleshoot them, and manage the cluster resources. Partners access the Dashboard with dedicated security profile.

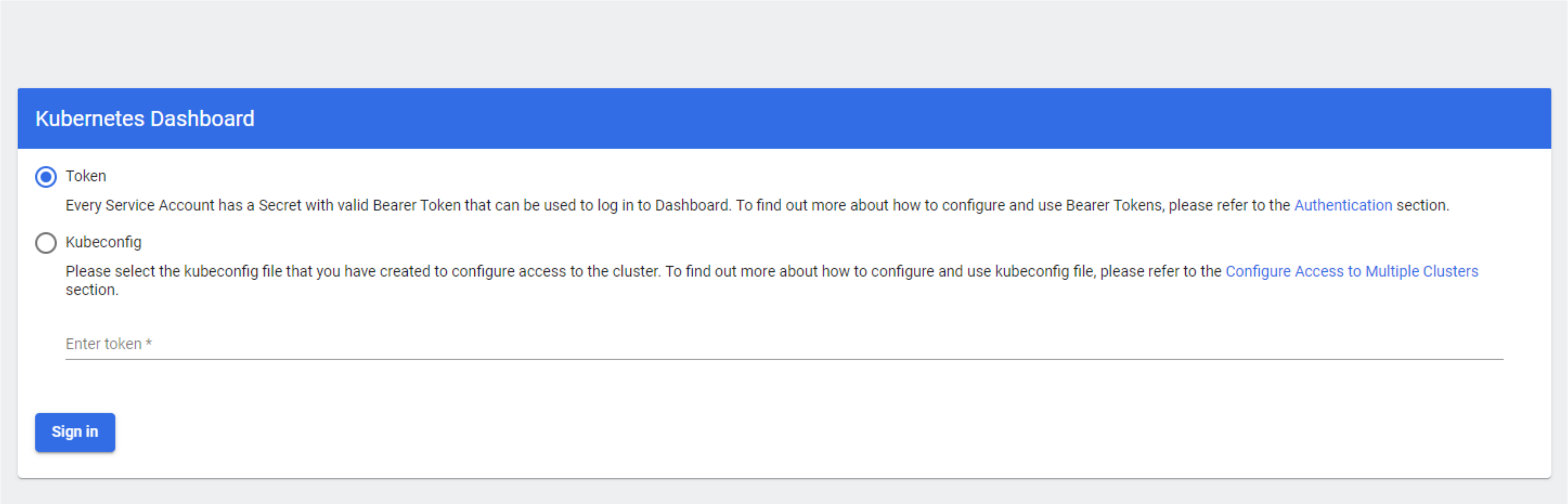


Deployments

	Name	Images	Labels	Pods	Created ↑
●	cce	optima-medina-docker-dev.artifact.tecnalia.com/wp4/t41/cce:0.0.15 optima-medina-docker-dev.artifact.tecnalia.com/wp4/t41/cce-frontend:0.1.6	app: cce	1 / 1	7 days ago
●	catalogue-backend	optima-medina-docker-dev.artifact.tecnalia.com/wp2/t22/catalogue/backend:test	app: catalogue-backend	1 / 1	25 days ago
●	catalogue-gateway	optima-medina-docker-dev.artifact.tecnalia.com/wp2/t22/catalogue/gateway:test	app: catalogue-gateway	1 / 1	25 days ago
●	raof-engine	optima-medina-docker-dev.artifact.tecnalia.com/wp2/t26/risk-assessment-engine:test	app: engine-risk-assessment	1 / 1	a month ago
●	raof-app	optima-medina-docker-dev.artifact.tecnalia.com/wp2/t26/risk-assessment-app:latest	app: api-risk-assessment	1 / 1	a month ago

Kubernetes Dashboard Access

Token-based authentication is needed by Partners to access the Dashboard.



Kubernetes Dashboard

● Token

Every Service Account has a Secret with valid Bearer Token that can be used to log in to Dashboard. To find out more about how to configure and use Bearer Tokens, please refer to the Authentication section.

○ Kubeconfig

Please select the kubeconfig file that you have created to configure access to the cluster. To find out more about how to configure and use kubeconfig file, please refer to the Configure Access to Multiple Clusters section.

Enter token *

Installation of the MEDINA Framework

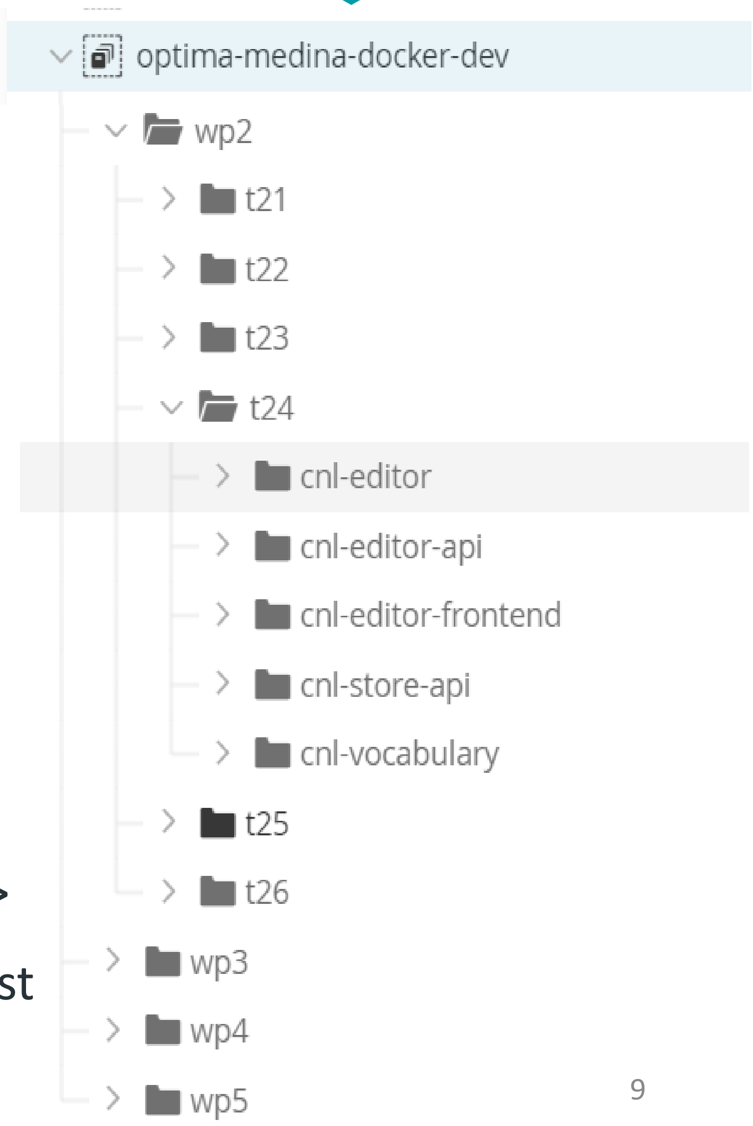
- Tools used:
  - Private Docker Registry
  - Ceph
  - Git
  - Jenkins

MEDINA Private Docker Registry

- The micro-services running on the Kubernetes cluster are packaged in Docker images
- Docker images are stored on the MEDINA private Docker Registry running on Artifactory
- When deploying to Kubernetes cluster, K8s reads the Docker images from the Registry
- Path convention:

<medina_registry_url>/<work_package>/<task >/<image>:<tag>

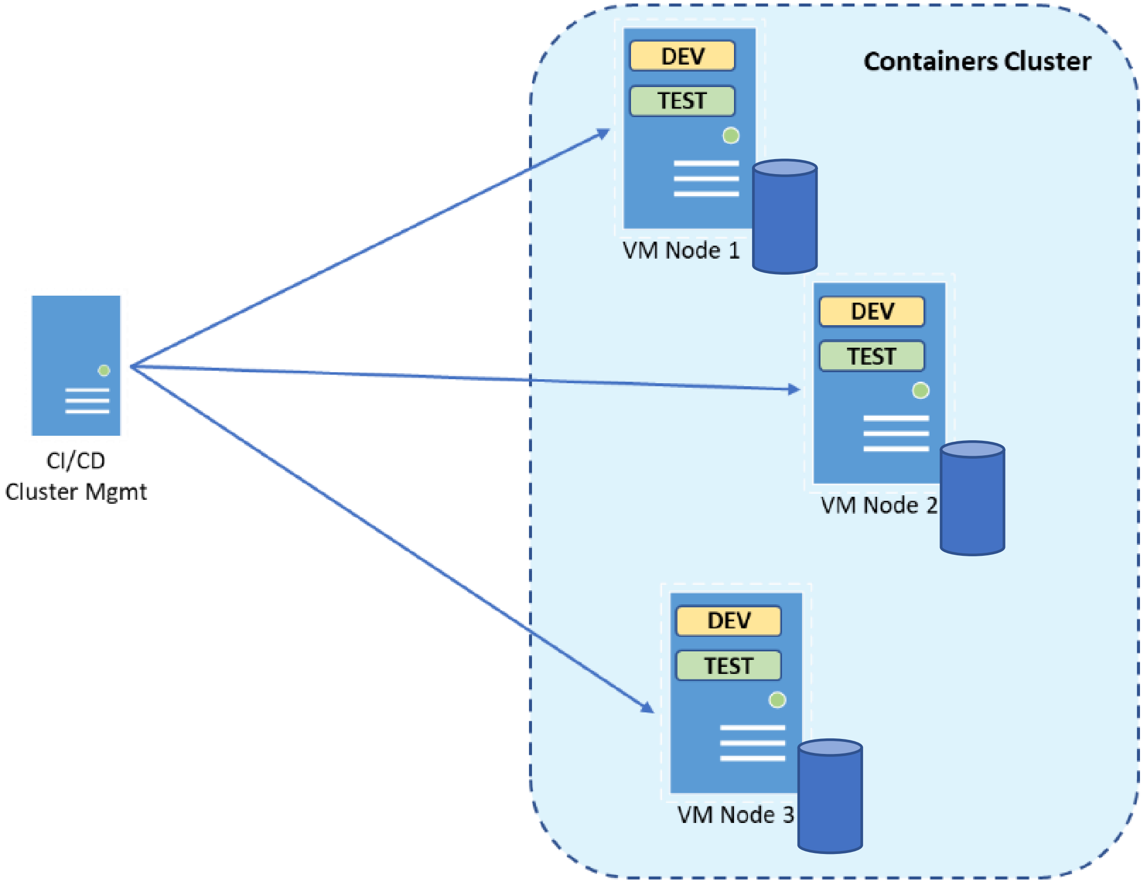
e.g optima-medina-docker-dev.artifact.tecnalia.com/wp2/t24/cnl-editor:latest



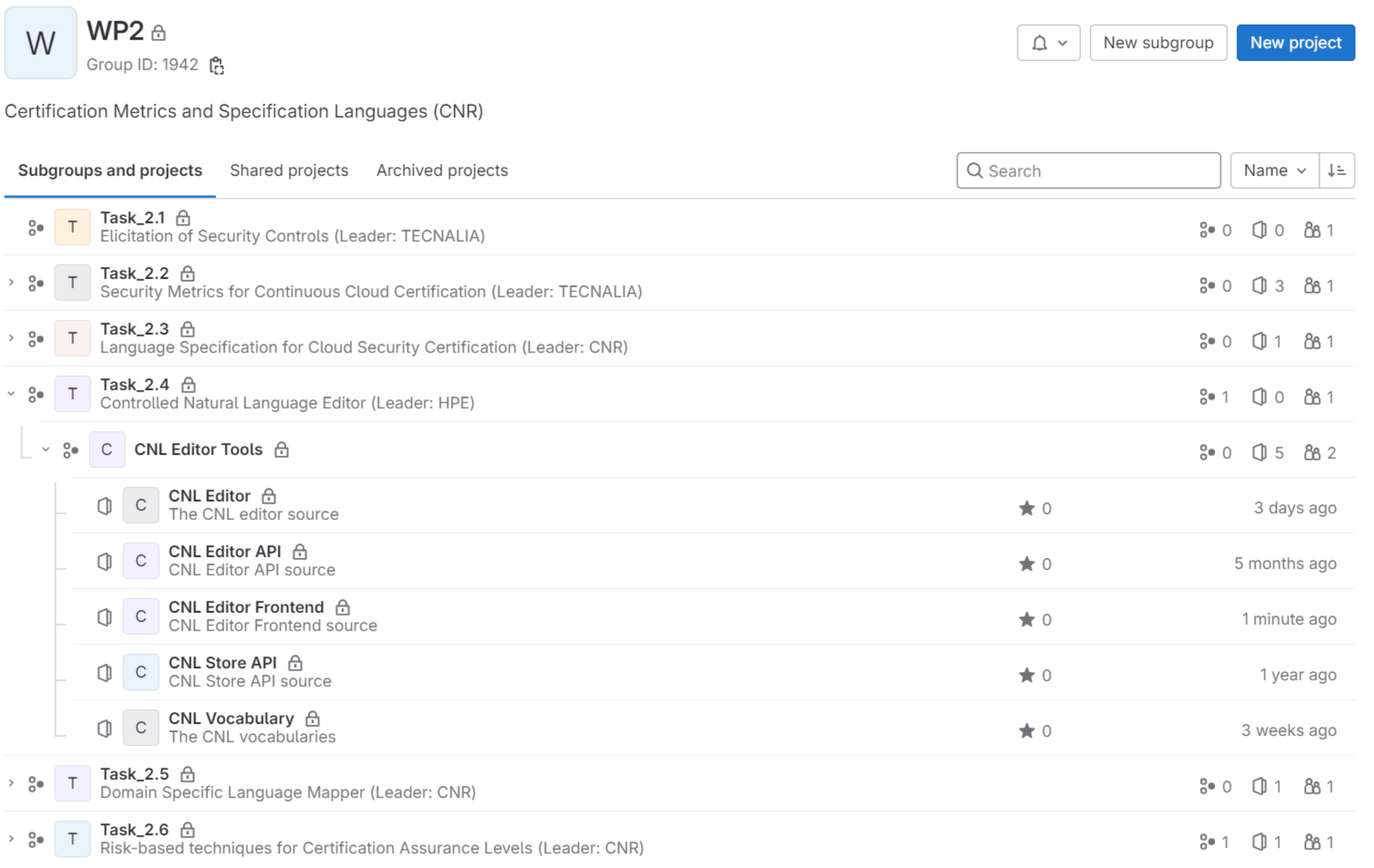
- optima-medina-docker-dev
  - wp2
    - t21
    - t22
    - t23
    - t24
      - cnl-editor
      - cnl-editor-api
      - cnl-editor-frontend
      - cnl-store-api
      - cnl-vocabulary
    - t25
    - t26
  - wp3
  - wp4
  - wp5

Ceph: distributed storage solution

- The 200 GB of storage of each K8s node is organized as a distributed clustered filesystem for the data persistence layer.
- The data is mirrored among the three nodes for high/availability purposes.
- Thanks to that, all the micro-services can store their data in an easy and fault-tolerant way.



Git: MEDINA source code service



W **WP2**

Group ID: 1942

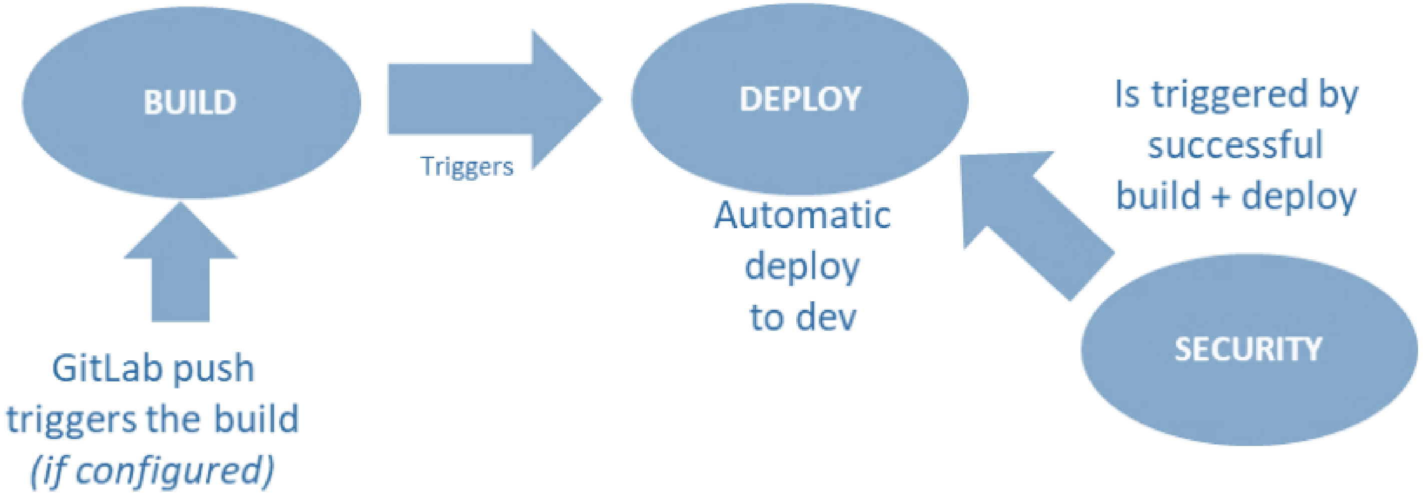
Certification Metrics and Specification Languages (CNR)

T	**Task_2.1** Elicitation of Security Controls (Leader: TECNALIA)	0	0	1
T	**Task_2.2** Security Metrics for Continuous Cloud Certification (Leader: TECNALIA)	0	3	1
T	**Task_2.3** Language Specification for Cloud Security Certification (Leader: CNR)	0	1	1
T	**Task_2.4** Controlled Natural Language Editor (Leader: HPE)	1	0	1
C	**CNL Editor Tools**	0	5	2
C	**CNL Editor** The CNL editor source	★ 0		3 days ago
C	**CNL Editor API** CNL Editor API source	★ 0		5 months ago
C	**CNL Editor Frontend** CNL Editor Frontend source	★ 0		1 minute ago
C	**CNL Store API** CNL Store API source	★ 0		1 year ago
C	**CNL Vocabulary** The CNL vocabularies	★ 0		3 weeks ago
T	**Task_2.5** Domain Specific Language Mapper (Leader: CNR)	0	1	1
T	**Task_2.6** Risk-based techniques for Certification Assurance Levels (Leader: CNR)	1	1	1

Jenkins: automation for Continuous Integration & Delivery (CI/CD)

Our solution uses Continuous Integration (CI) and Continuous Deployment (CD) Agile practices implemented by the Build, Deploy, and Security pipelines designed ad-hoc for MEDINA.

This is the SecDevOps implementation for MEDINA development.


BUILD
Triggers
DEPLOY
Is triggered by successful build + deploy
Automatic deploy to dev
SECURITY
GitLab push triggers the build *(if configured)*

MEDINA

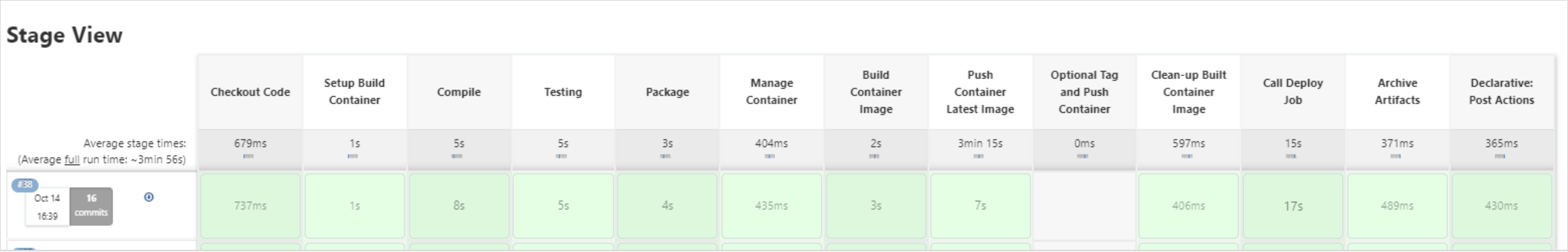
Installation of the MEDINA Framework

- CI/CD Pipelines:
  - Build
  - Deploy
  - Security

CI/CD Pipelines – BUILD

The Build pipeline is triggered automatically at every push of a project in the MEDINA public GitLab and automatizes:

- Build and testing of the project
- Creation of Docker image
- Push the Docker image to the private Docker Registry

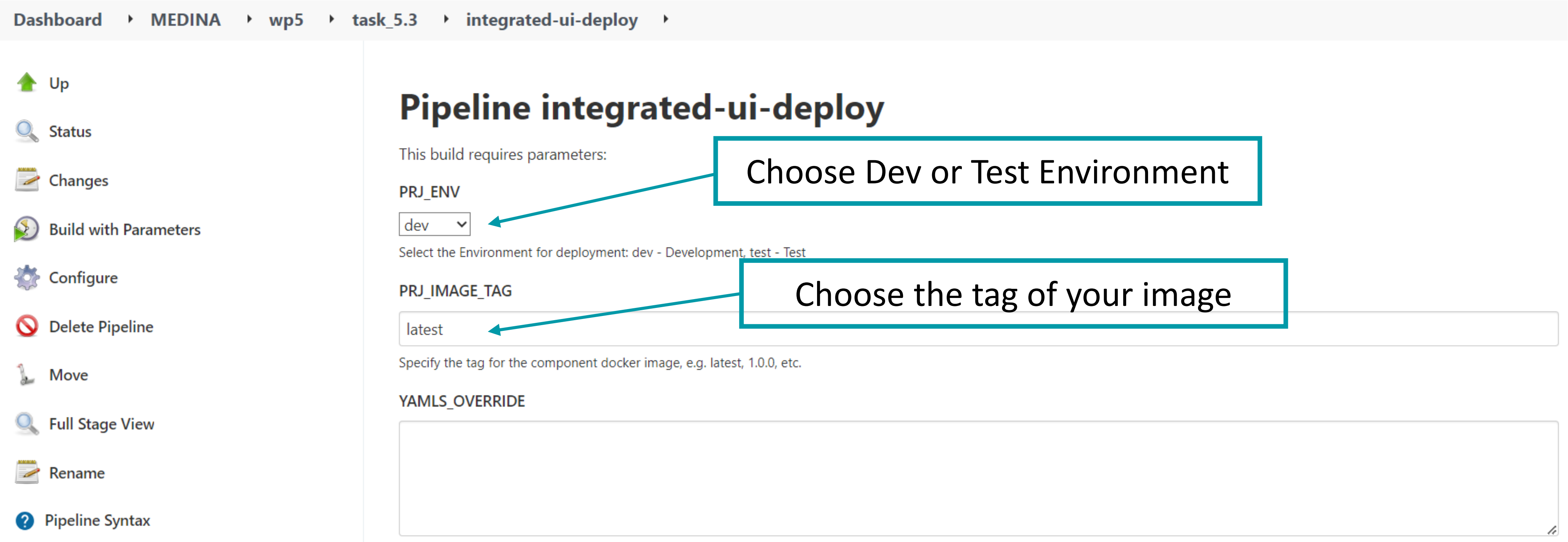


Stage View

	Checkout Code	Setup Build Container	Compile	Testing	Package	Manage Container	Build Container Image	Push Container Latest Image	Optional Tag and Push Container	Clean-up Built Container Image	Call Deploy Job	Archive Artifacts	Declarative: Post Actions
Average stage times: (Average full run time: ~3min 56s)	679ms	1s	5s	5s	3s	404ms	2s	3min 15s	0ms	597ms	15s	371ms	365ms
#38 Oct 14 16:39 16 commits	737ms	1s	8s	5s	4s	435ms	3s	7s		406ms	17s	489ms	430ms

CI/CD Pipelines – Deploy

The Deploy pipeline automatically deploys the component to the selected Kubernetes environment: Development or Test



Dashboard ‣ MEDINA ‣ wp5 ‣ task_5.3 ‣ integrated-ui-deploy ‣

Pipeline integrated-ui-deploy

This build requires parameters:

PRJ_ENV

dev

Select the Environment for deployment: dev - Development, test - Test

PRJ_IMAGE_TAG

latest

Specify the tag for the component docker image, e.g. latest, 1.0.0, etc.

YAMLS_OVERRIDE

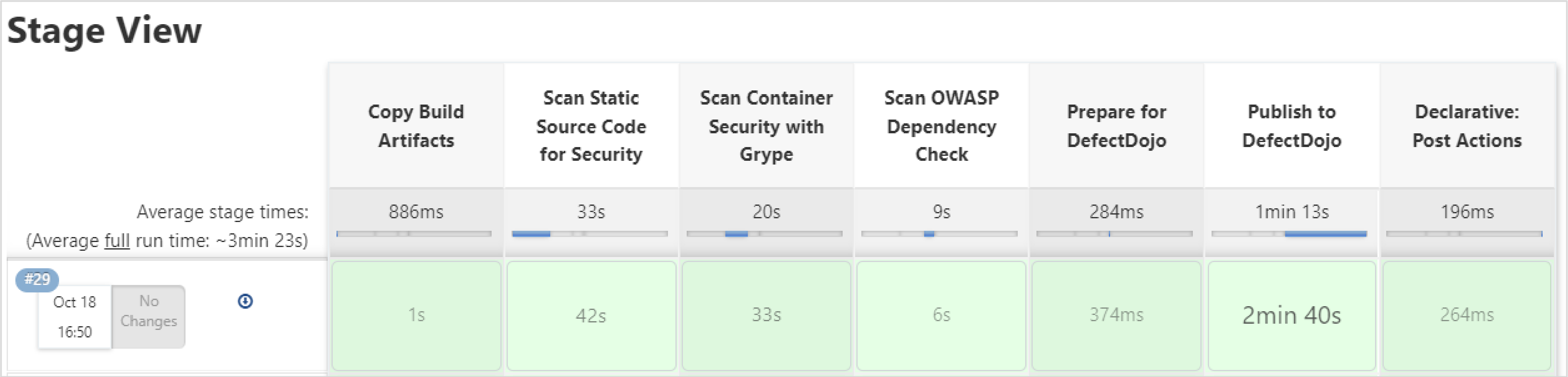
Choose Dev or Test Environment

Choose the tag of your image

CI/CD Pipelines – Security

Different types of security analysis are performed:

- Static Code Analysis for checking the source code security defects
- Container security for scanning vulnerabilities in the container packages
- Software Composition Analysis (SCA) for spotting security issues in third-party libraries.

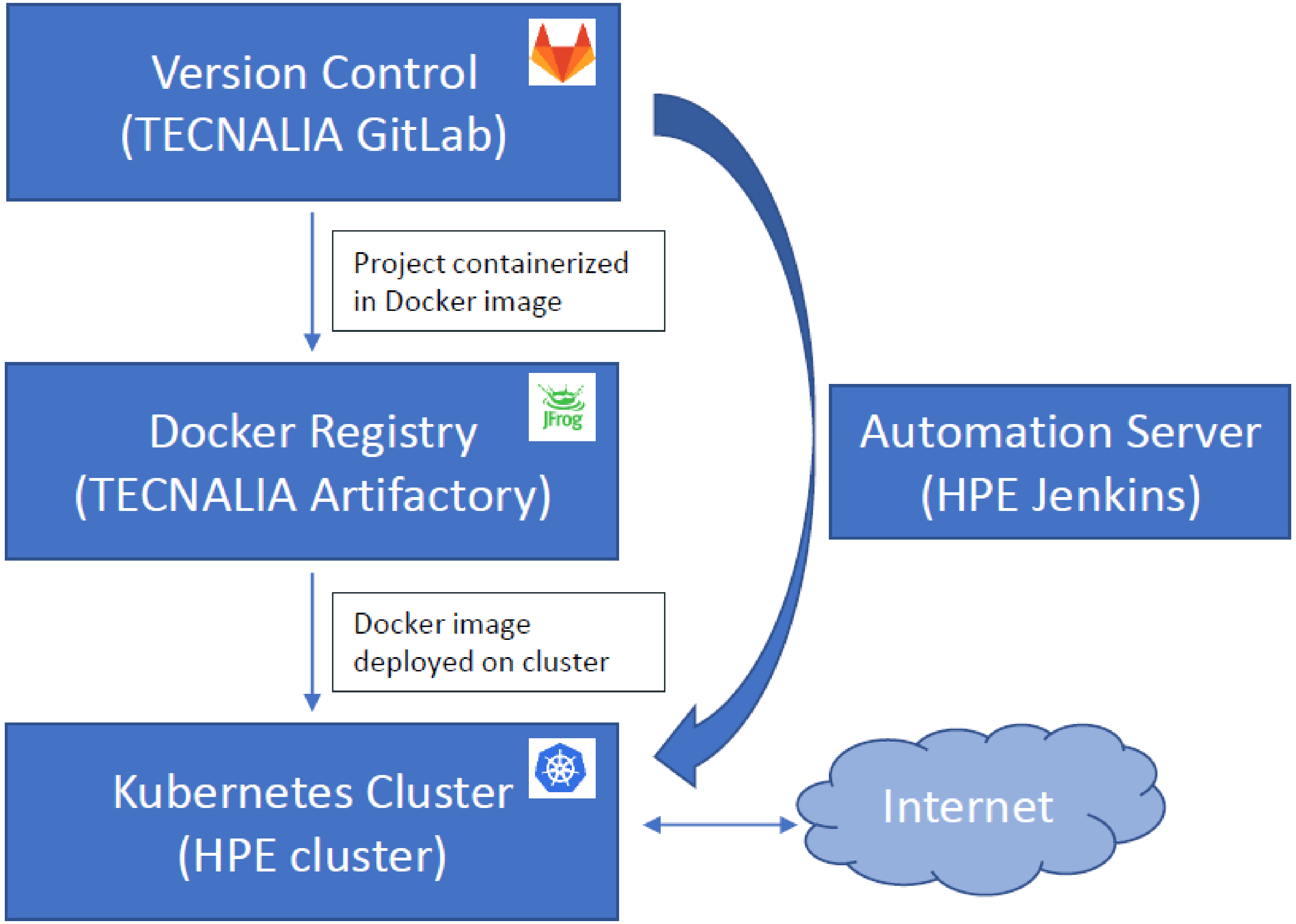


Stage View

	Copy Build Artifacts	Scan Static Source Code for Security	Scan Container Security with Grype	Scan OWASP Dependency Check	Prepare for DefectDojo	Publish to DefectDojo	Declarative: Post Actions
Average stage times: (Average full run time: ~3min 23s)	886ms	33s	20s	9s	284ms	1min 13s	196ms
#29 Oct 18 16:50 No Changes	1s	42s	33s	6s	374ms	2min 40s	264ms

MEDINA Integration Environment

- All projects are available on private GitLab.
- All Docker images are stored on the private Docker Registry Artifactory.
- Components run on the Kubernetes cluster
- The CI/CD pipelines automate all the deployments steps



Installation of the MEDINA Framework

- Demo

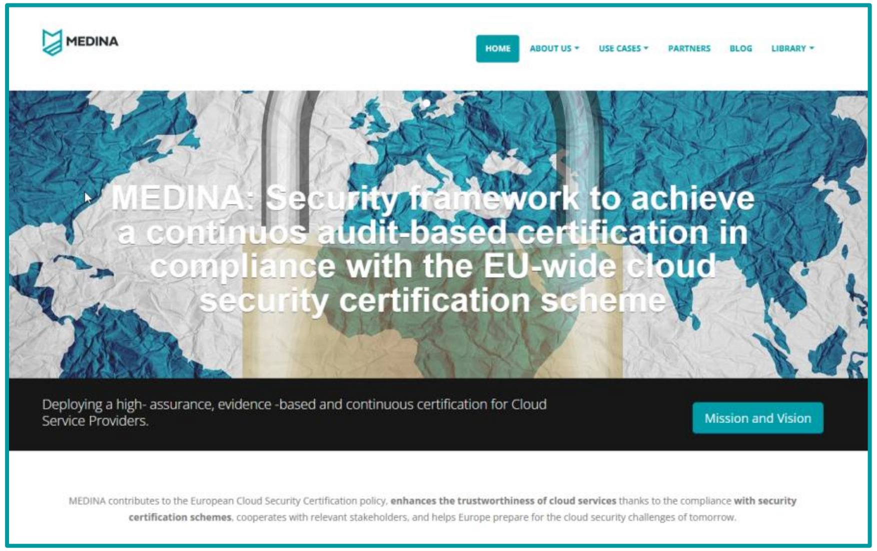
MEDINA

Installation of the MEDINA Framework

➤ Further information

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft

XLAB

nixu cybersecurity.

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

MEDINA

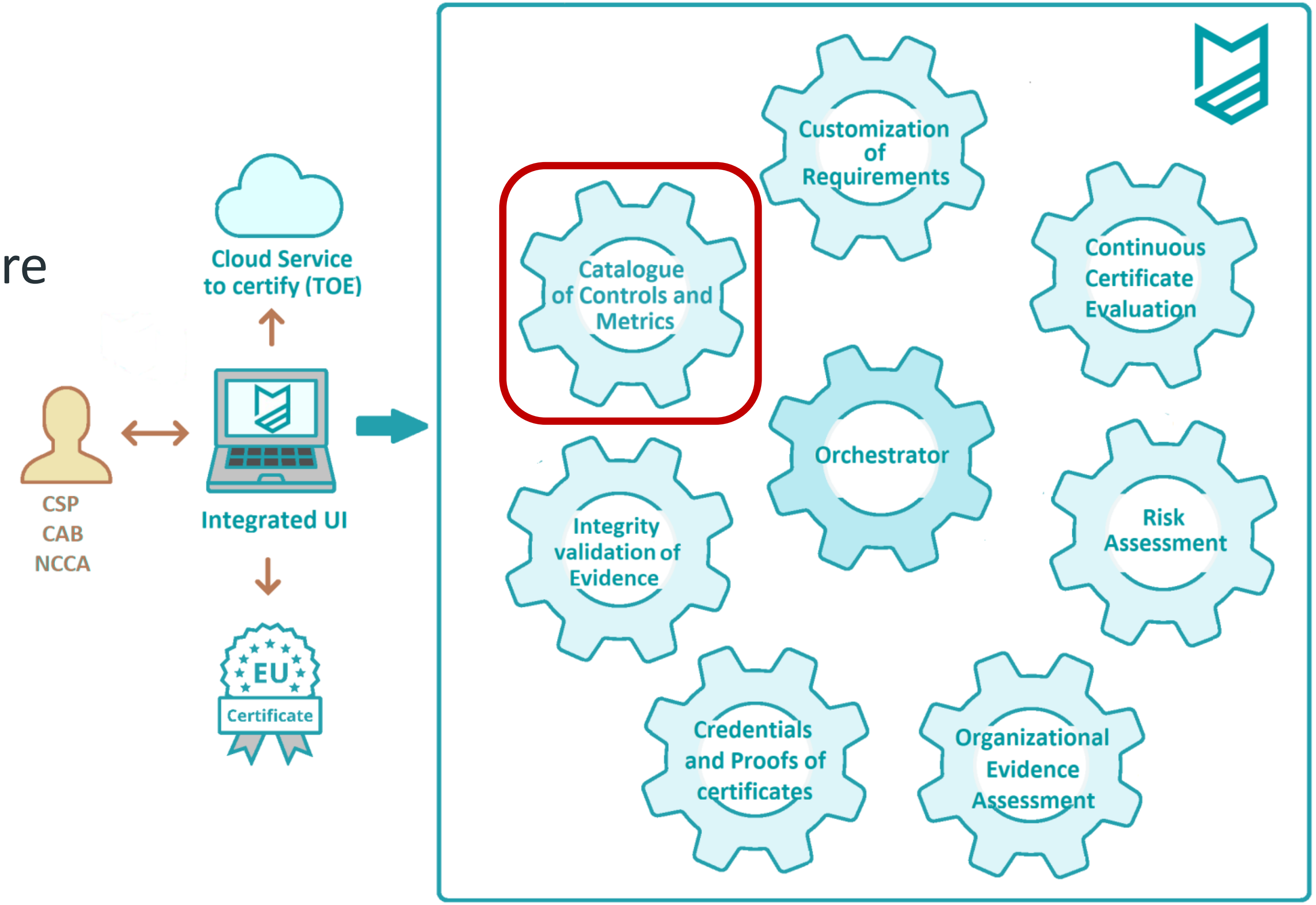
Catalogue of Controls and Metrics

Iñaki Etxaniz, TECNALIA

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

Chapters

- Overview
  - Purpose
  - Role in MEDINA architecture
- How to use it
  - Funtionalities
  - Demo
- Installation
- Further information



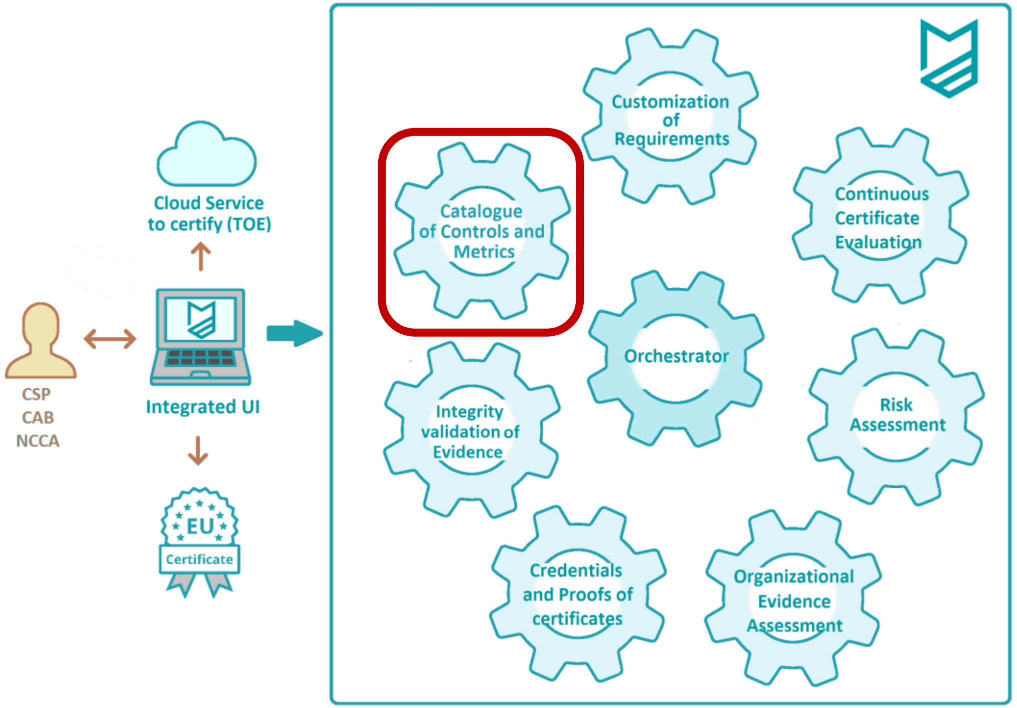
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Catalogue of Controls and Metrics

➤ Overview

- Purpose
- Role in MEDINA Architecture

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Catalogue of Controls and Metrics

MEDINA

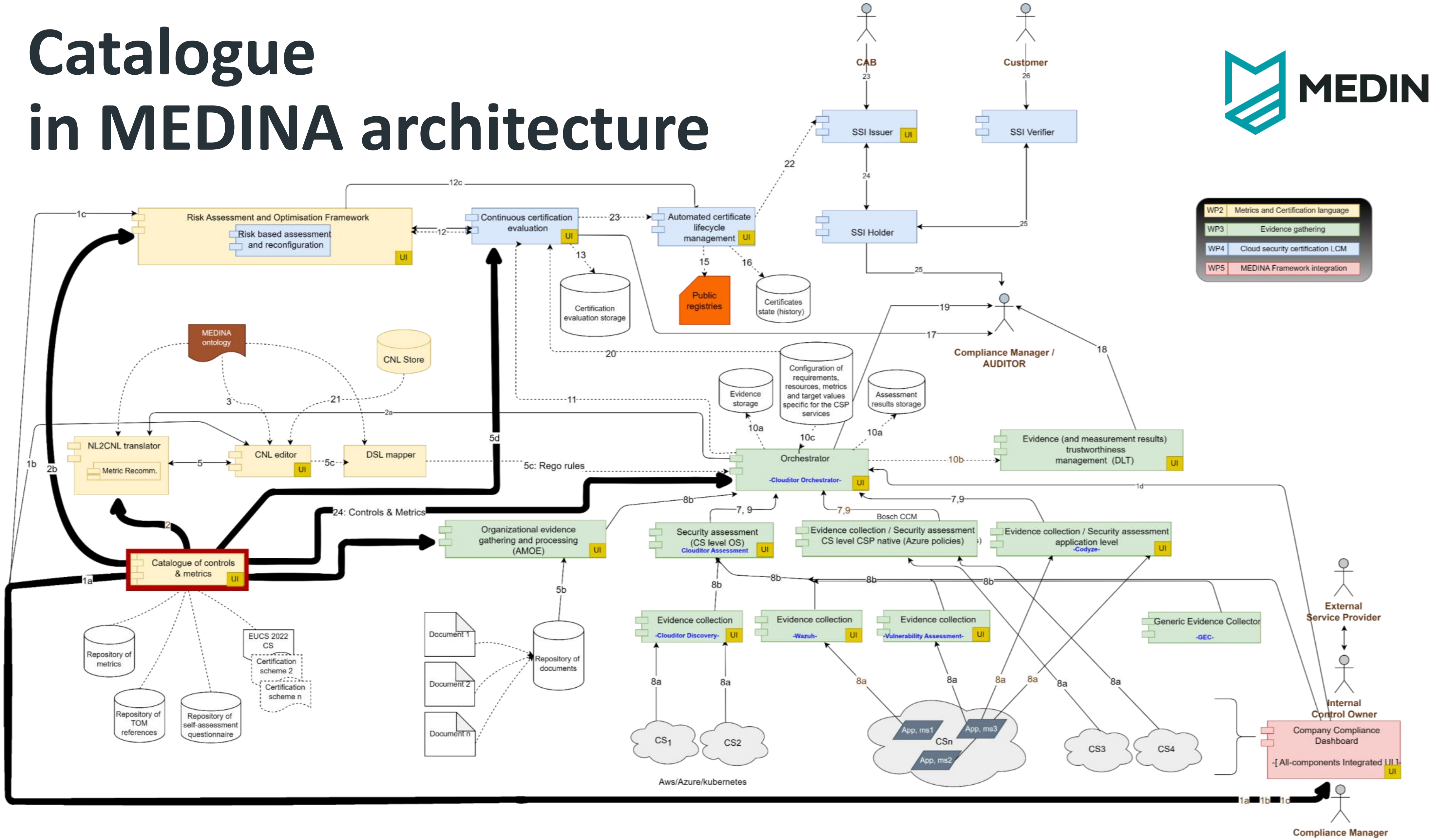
- The Catalogue is the component that stores the **EUCS certification scheme** (draft version August-2022)
- Offers an **API** to the rest of MEDINA components to get the information
- Has a navigable **user interface** that allows the user to consult and check the standard
- Data is pre-loaded (EUCS, Metrics, Guidelines...)

Catalogue of Controls and Metrics (II)

- The Catalogue is enhanced with some extra features:

  1. **Metrics** for the automatic assessment of EUCS requirements
  2. **Implementation guidelines** (for a set of EUCS requirements)
  3. **Mapping** of controls to other schemes
  4. **Self-assessment Questionnaires**
  5. **Administration** data

Catalogue in MEDINA architecture


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
24
SSI Holder
25
22
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
21
3
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Document 1
Document 2
Document n
Repository of documents
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1d
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Interactions with other components

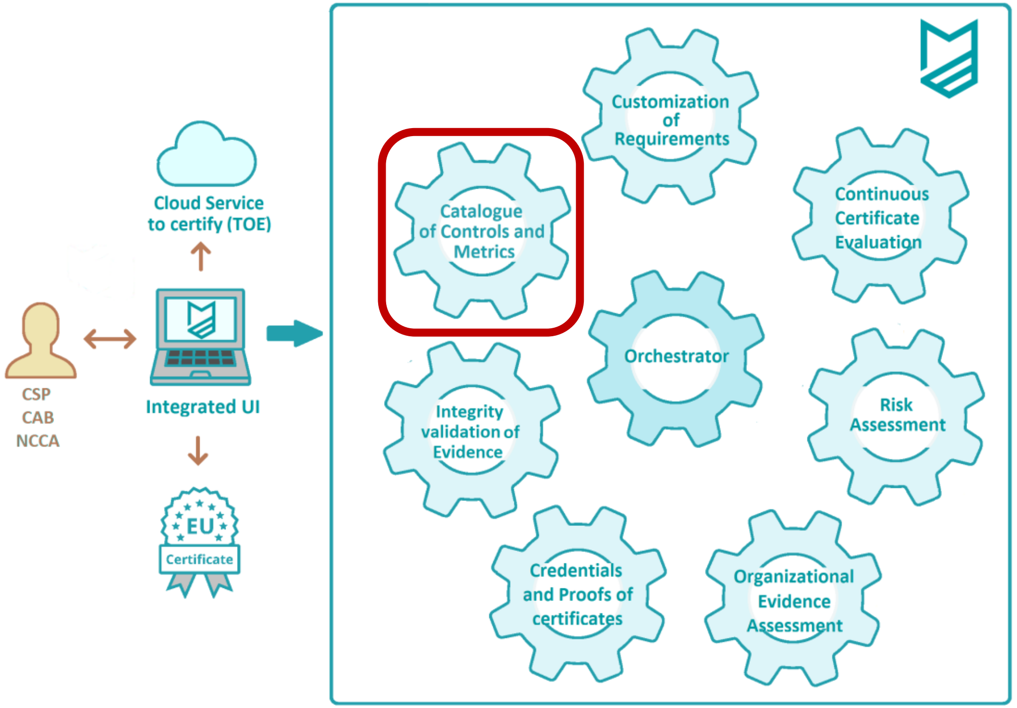
MEDINA

- Risk Assessment and Optimization Framework
  - Retrieves the EUCS schema specification
  - Receives the results of self-assessment questionnaire
- Continuous certification Evaluation (CCE)
  - Retrieves the EUCS schema specification
- NL2CNL translator
  - Requests the metrics and maps them to the MEDINA ontology
- Orchestrator
  - Retrieves the information about controls and metrics
- Assessment & Management of Organisational Evidence (AMOE)
  - Retrieves the information about controls and metrics
- User
  - Consults the EUCS schema
  - Performs self-assessment via questionnaires

Catalogue of Controls and Metrics

- How to use it
  - Functionalities
  - Demo(s)

MEDINA


CSP
CAB
NCCA
Cloud Service to certify (TOE)
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

EUCS schema and metrics

- **EUCS** is organized in:
  - 20 **Categories**
    - E.g., *A1: Organisation of Information Security (OIS)*
  - 119 **Controls**
    - E.g., *OIS-03: Contact with authorities and interest groups*
  - 998 **Requirements**
    - E.g., *OIS-03.1H: The CSP shall maintain regular contacts with relevant authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.*
    - Three level of assurance: Basic, Substantial and High
- MEDINA targets 34 selected requirements
  - *"MEDINA provides realizable metrics for the technical and organizational measures referenced in EUCS-High assurance level requiring '**continuous (automated)' monitoring**"*

EUCS schema and metrics (II)

- **Metrics:** used to measure the efficiency and effectiveness of the technical and organizational measures put in place
  - Must produce quantifiable information, to be compared with a target value
  - Are collected on a regular basis (frequency) for continuous monitoring
  - Defined as formulas. E.g.:

Metric	Control	Type	Scale	Operator	Target Value	Datatype	Interval (hours)	Target Resource Type
MalwareProtectionEnabled	OPS-05.3H	Technical	[true, false]	==	true	Boolean	1	VirtualMachine
PasswordPolicyQ2	IAM-08.1H	Organizational	days	<=	90	Integer	720	Policy Document

  - **157 metrics** in the Catalogue.

Implementation Guidelines

- Explanation of how a security **Requirement** can be implemented, in a vendor and technology-agnostic way
- Serve as:
  - A guidance for the user
  - Input to the NLP tool to refine the MEDINA certification language
- Defined for “the 34” selected Requirements

Mapping to other schemes

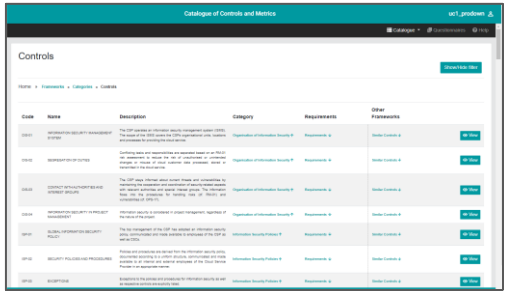
MEDINA

- Identify similar controls (in scope) between EUCS and other security schemes
- Maps EUCS controls to:
  - C5:2020 (Germany)
  - SecNumCloud (France)
  - ISO/IEC 27002
  - ISO/IEC 27017
  - Cisco Cloud Control Framework (CCF)

Catalogue of Controls and Metrics

- DEMO (I) -

EUCS Schema and metrics



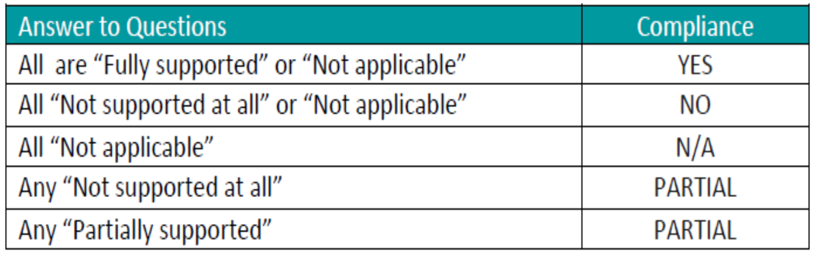
Controls

Home > Frameworks > Categories > Controls

Code	Name	Description	Category	Requirements	Other Frameworks	
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSP's organisational units, locations and processes for providing the cloud service.	Organisation of Information Security	Requirements	Similar Controls	View
OIS-02	SEGREGATION OF DUTIES	Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.	Organisation of Information Security	Requirements	Similar Controls	View
OIS-03	CONTACT WITH AUTHORITIES AND INTEREST GROUPS	The CSP stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks (cf. RM-01) and vulnerabilities (cf. OPS-17).	Organisation of Information Security	Requirements	Similar Controls	View
OIS-04	INFORMATION SECURITY IN PROJECT MANAGEMENT	Information security is considered in project management, regardless of the nature of the project.	Organisation of Information Security	Requirements	Similar Controls	View
ISP-01	GLOBAL INFORMATION SECURITY POLICY	The top management of the CSP has adopted an information security policy, communicated and made available to employees of the CSP as well as CSCs.	Information Security Policies	Requirements	Similar Controls	View
ISP-02	SECURITY POLICIES AND PROCEDURES	Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner.	Information Security Policies	Requirements	Similar Controls	View
ISP-03	EXCEPTIONS	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Information Security Policies	Requirements	Similar Controls	View

Self-assessment Questionnaires

- Questionnaires developed to assess the compliance with the EUCS requirements
- Two types of users
  - CSP: self-assessment / Auditor: audit with non-conformities
- Three assurance level of certification
  - Basic / Substantial / High
- Several questions for each requirement
  - Requirement *Compliance* value calculated as:
- A report generated with the results



Answer to Questions	Compliance
All are "Fully supported" or "Not applicable"	YES
All "Not supported at all" or "Not applicable"	NO
All "Not applicable"	N/A
Any "Not supported at all"	PARTIAL
Any "Partially supported"	PARTIAL

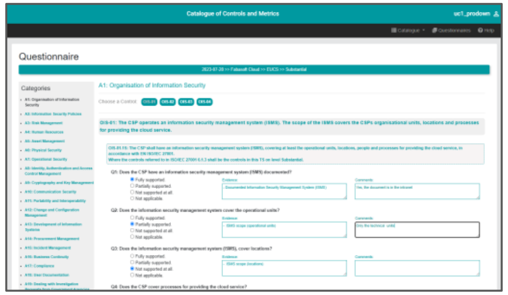
Features for administrator

- Open API interface
  - Allows to interact with the frontend, backend APIs
- Audit logs
  - Records user changes to the EUCS schema

Catalogue of Controls and Metrics

- DEMO (II) -

Self-assessment Questionnaires



Questionnaire

2023-07-20 >> Fabasoft Cloud >> EUCS >> Substantial

Categories

- A1: Organisation of Information Security
- A2: Information Security Policies
- A3: Risk Management
- A4: Human Resources
- A5: Asset Management
- A6: Physical Security
- A7: Operational Security
- A8: Identity, Authentication and Access Control Management
- A9: Cryptography and Key Management
- A10: Communication Security
- A11: Portability and Interoperability
- A12: Change and Configuration Management
- A13: Development of Information Systems
- A14: Procurement Management
- A15: Incident Management
- A16: Business Continuity
- A17: Compliance
- A18: User Documentation
- A19: Dealing with Investigation Requests from Government Agencies

A1: Organisation of Information Security

Choose a Control: OIS-01 OIS-02 OIS-03 OIS-04

OIS-01: The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service.

OIS-01.1S: The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service, in accordance with EN ISO/IEC 27001.
Where the controls referred to in ISO/IEC 27001 6.1.3 shall be the controls in this TS on level Substantial.

Q1: Does the CSP have an information security management system (ISMS) documented?

● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - Documented Information Security Management System (ISMS)

Comments: Yes, the document is in the intranet

Q2: Does the information security management system cover the operational units?

○ Fully supported.
● Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - ISMS scope (operational units)

Comments: Only the technical units

Q3: Does the information security management system (ISMS), cover locations?

○ Fully supported.
○ Partially supported.
● Not supported at all.
○ Not applicable.

Evidence: - ISMS scope (locations)

Comments:

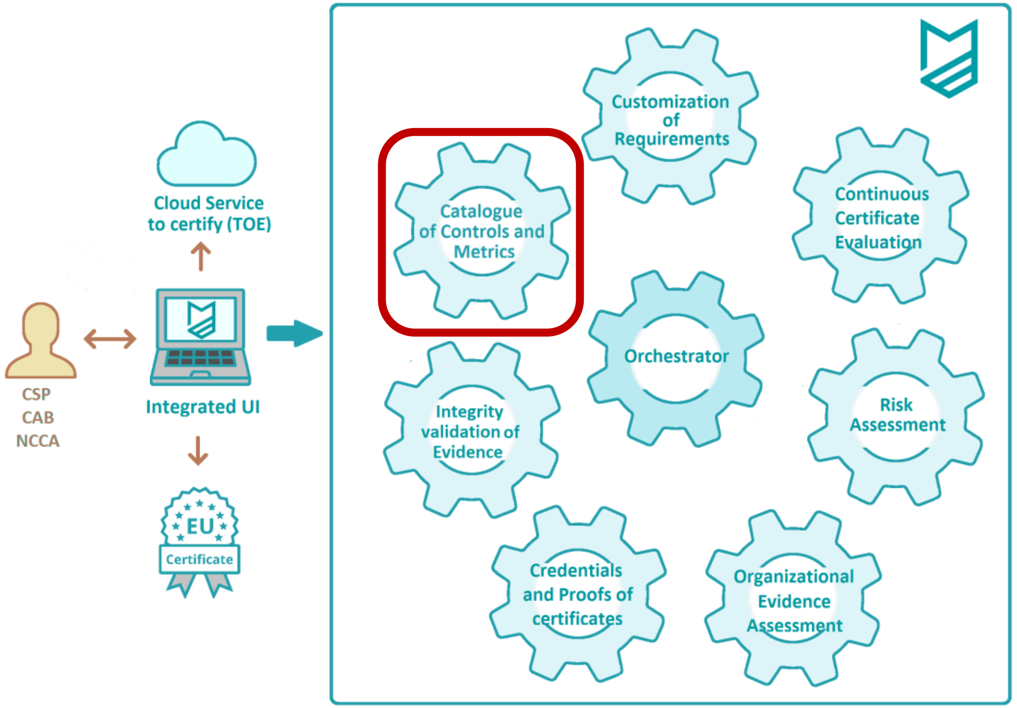
Q4: Does the CSP cover processes for providing the cloud service?

Catalogue of Controls and Metrics

- Installation

  - Technical Specifications

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

- Install for local deployment (for more options, see Readme file)
  - Clone the repository:

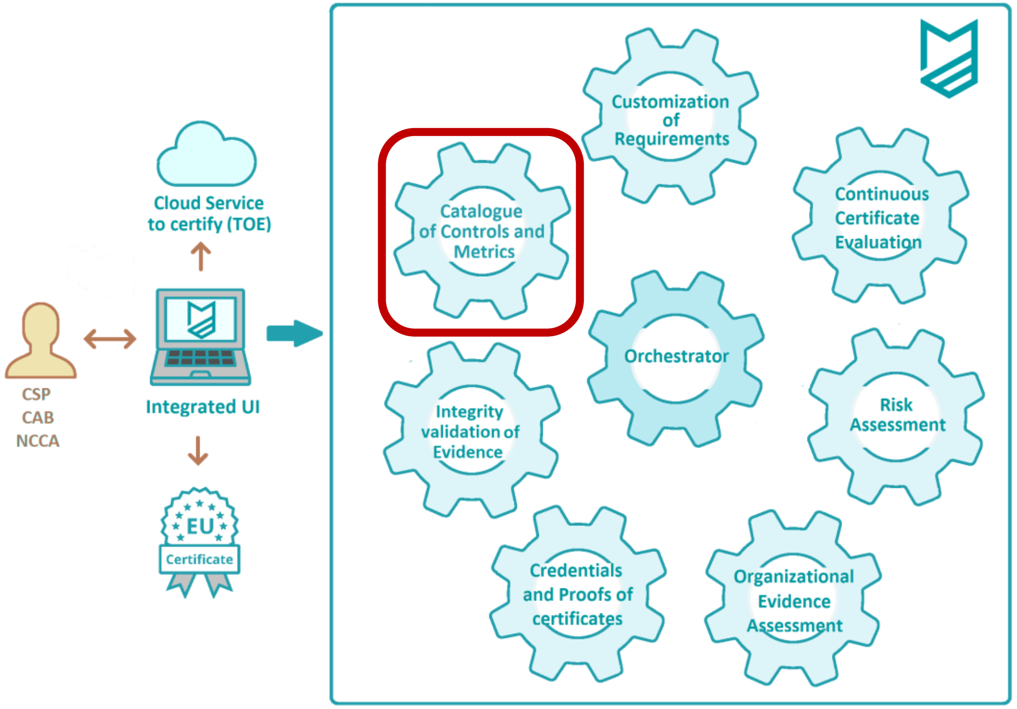
    git clone https://git.code.tecnalia.com/medina/public/catalogue-of-controls
  - Start JHipster and MySQL:

    docker-compose --env-file .env.local --project-directory ./ up
  - The Catalogue is available at https://192.168.56.1.nip.io/

- Technical specifications
  - jHipster framework-based microservices architecture
  - Java with Spring Boot stack on the server side
  - Frontend with Angular and Bootstrap
  - Docker-compose for installation

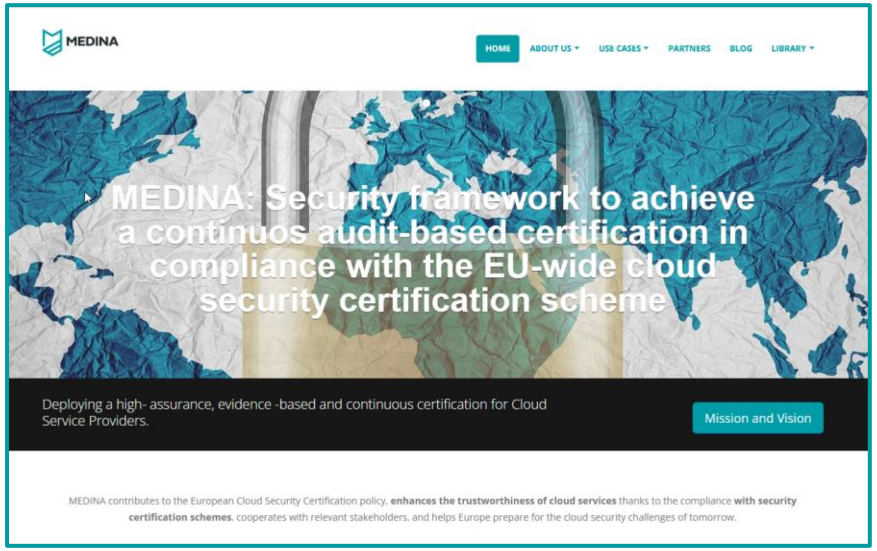
Catalogue of Controls and Metrics

- ➤ Further information


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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

MEDINA

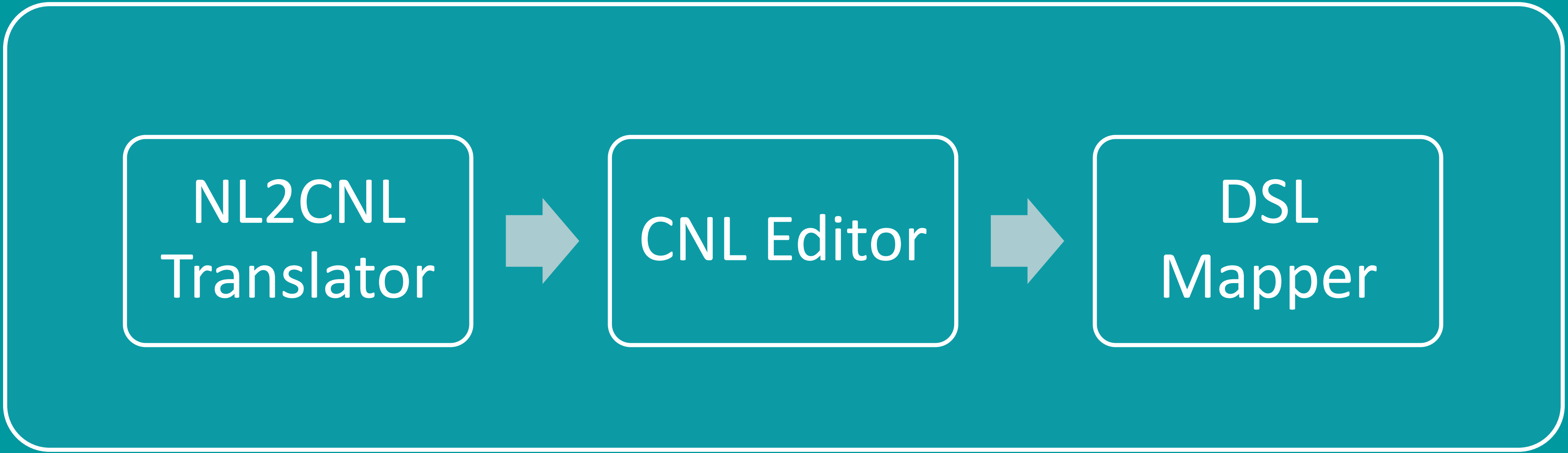
Customization of Requirements

HPE, CNR

July 2023

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

Customization of Requirements



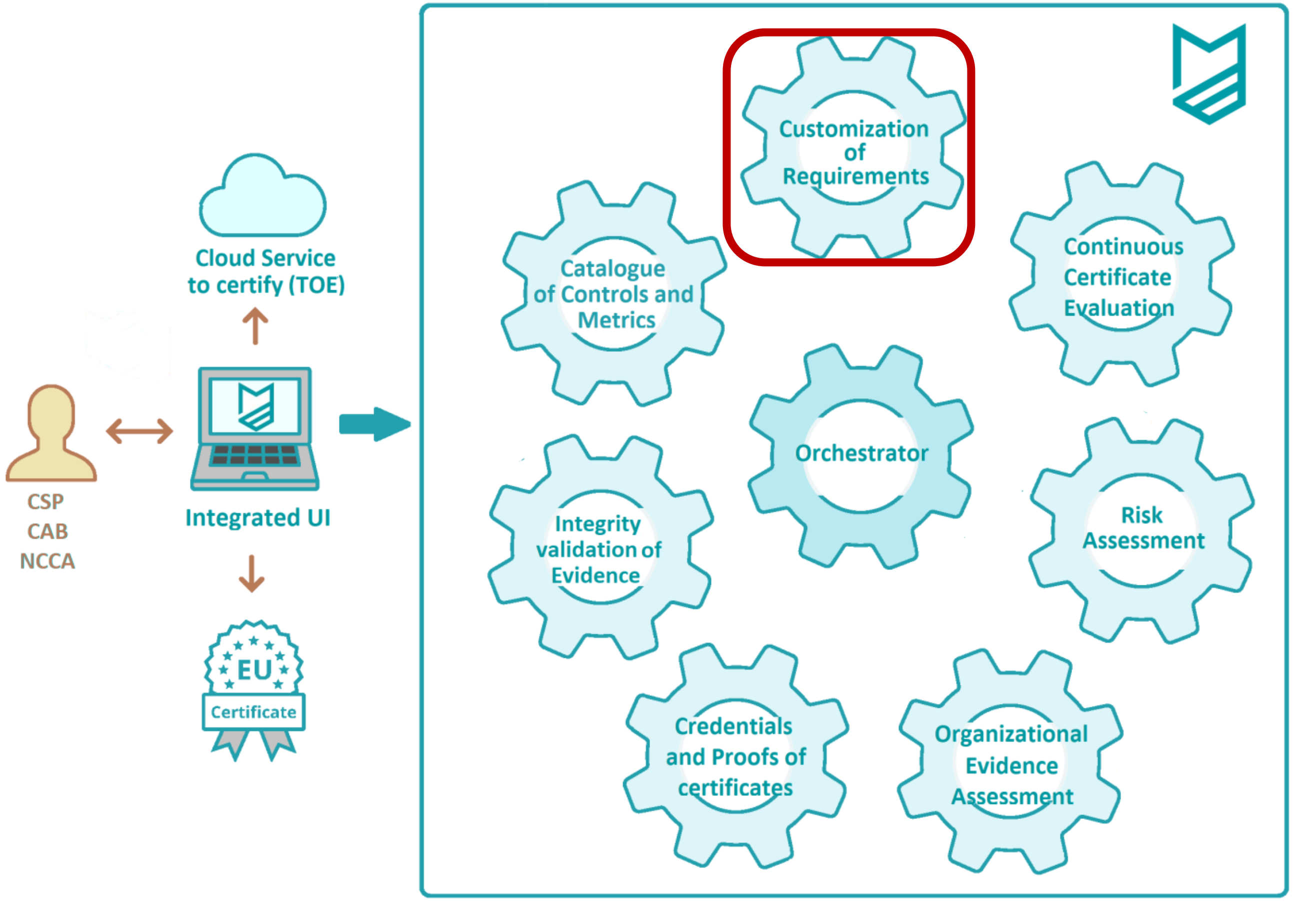
NL2CNL Translator

CNL Editor

DSL Mapper

Chapters

- Overview
- How to use it
- Installation
- Further information

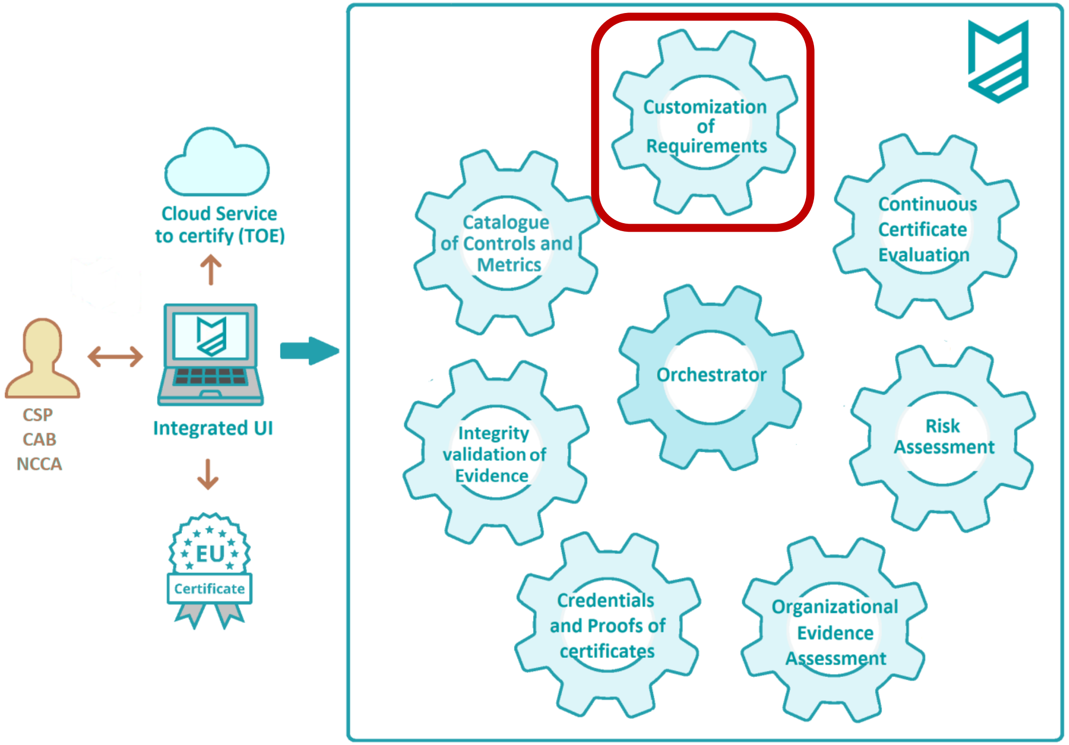


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

NL2CNL Translator

- Overview
  - Purpose
  - Role in MEDINA Architecture

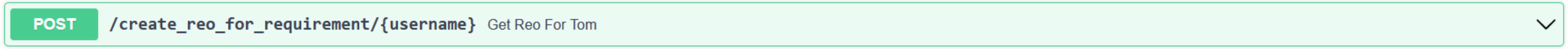
MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

NL2CNL Translator

MEDINA

- Component’s goals in MEDINA:
  - Associate a set of metrics with a requirement
  - Translate metrics into obligations
  - Store a requirement and its associated metrics into a REO object in the CNL Store
- It is **not** provided with a User Interface
- It offers a RESTful **API** to other MEDINA component

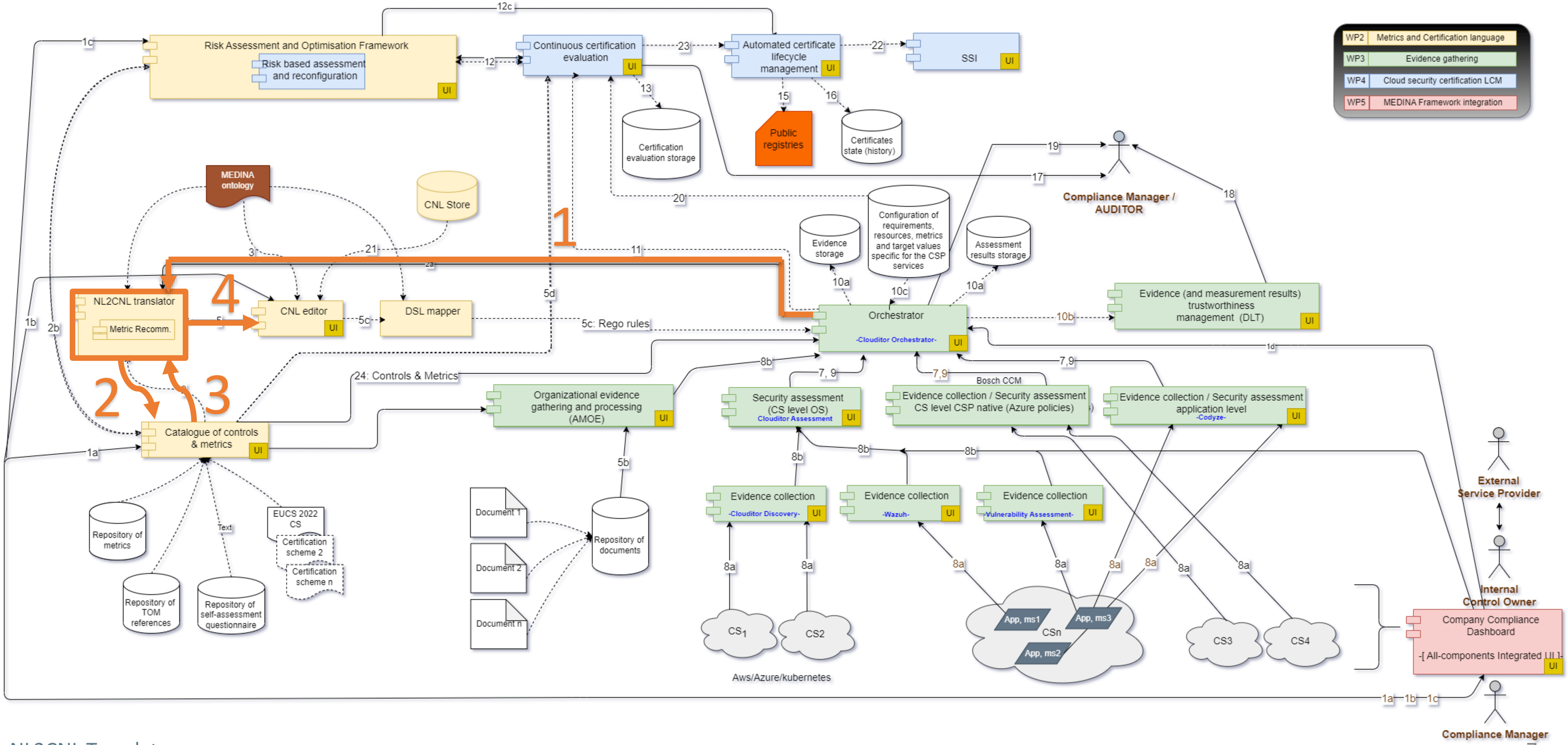


POST `/create_reo_for_requirement/{username}` Get Reo For Tom

NL2CNL Translator

- Input data
  - Requirements and metrics -> from the Catalogue of Controls and Metrics
  - NLP features -> precomputed and preloaded
- Output data
  - REO objects -> stored in the CNL Store of the CNL Editor

NL2CNL Translator
in MEDINA architecture



WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
Continuous certification evaluation
Automated certificate lifecycle management
SSI
12c
1c
12
23
22
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
MEDINA ontology
CNL Store
20
1
11
21
3
2a
4
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5c
5
5d
5c: Rego rules
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10b
Orchestrator
-Clouditor Orchestrator-
Evidence (and measurement results) trustworthiness management (DLT)
1d
1b
2b
2
3
24: Controls & Metrics
8b
7, 9
7,9
Bosch CCM
Catalogue of controls & metrics
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
1a
5b
Repository of metrics
Text
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
App, ms2
CSn
CS3
CS4
External Service Provider
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
1a
1b
1c
Compliance Manager

Interactions with other components

Orchestrator

- Invokes the NL2CNL Translator by passing a requirement to start the association with metrics and the translation into a REO object

Catalogue

- Provides the information about requirements and metrics available

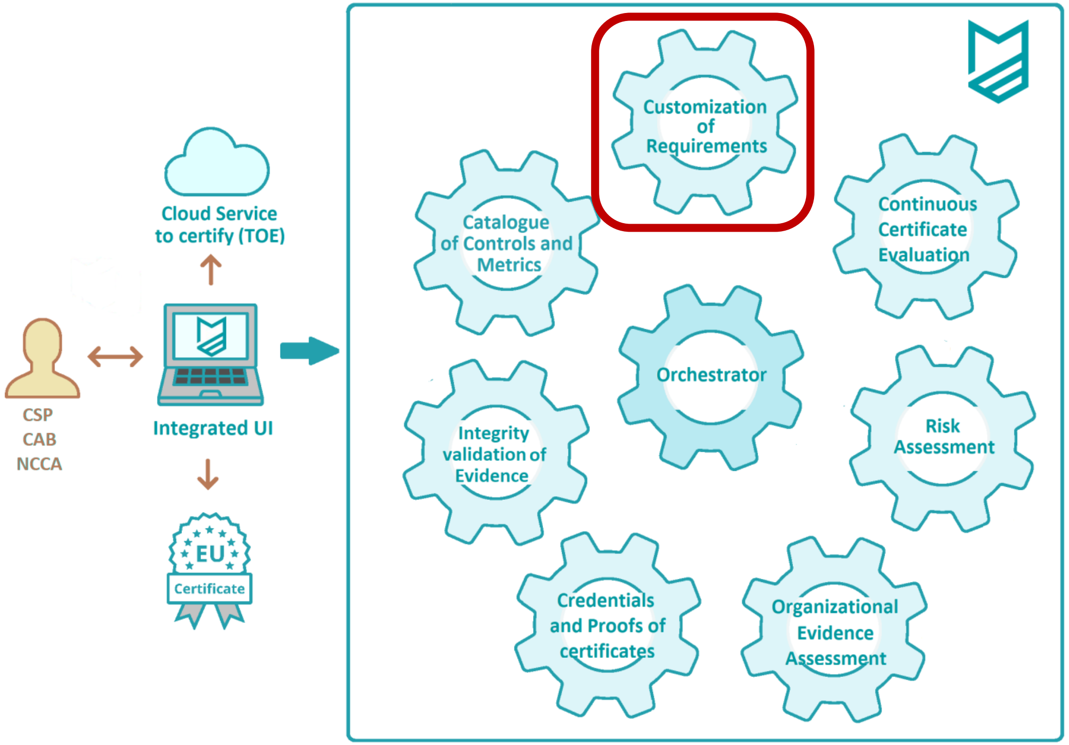
CNL Editor

- Provides the MEDINA vocabulary to be used to create the REO objects and provides the CNL Store to save the REO objects generated by the NL2CNL Translator

NL2CNL Translator

- How to use it
  - Functionalities

MEDINA



Association of requirements and metrics

- This process is **automatic** and **transparent** to the user
- The NL2CNL Translator relies on an internal module to associate metrics with requirements, called Metric Recommender
- This module compute the similarities among a requirement and metrics by using NLP features

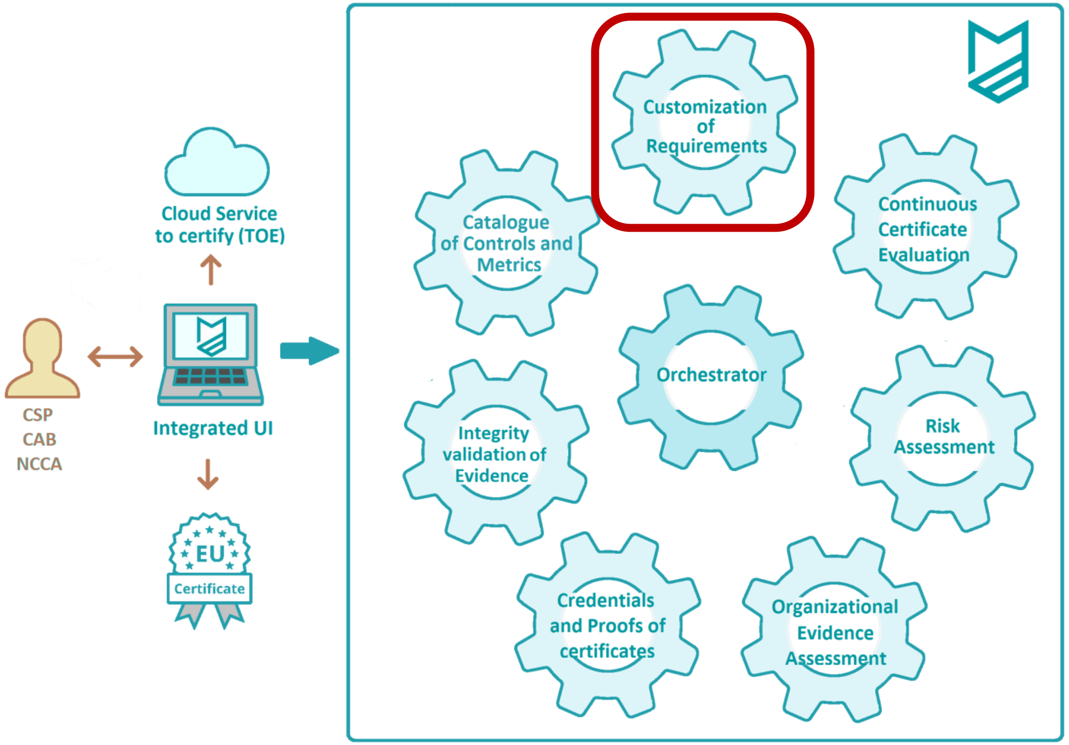
Translation

- This process is **automatic** and **transparent** to the user
- Once a requirement is associated with a set of metric, the NL2CNL Translator translates metrics into obligations and wraps all this information into an object called REO (Requirement & Obligations)

NL2CNL Translator

- ➤ Installation
  - - Deployment
  - - Technical Specifications

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

Local deployment

- The NL2CNL Translator is developed by using the *fastapi* web framework in Python 3.8 and it is containerized in Docker. The code is store in the GitLab repository of the project:
  - https://git.code.tecnalia.com/medina
- Build:

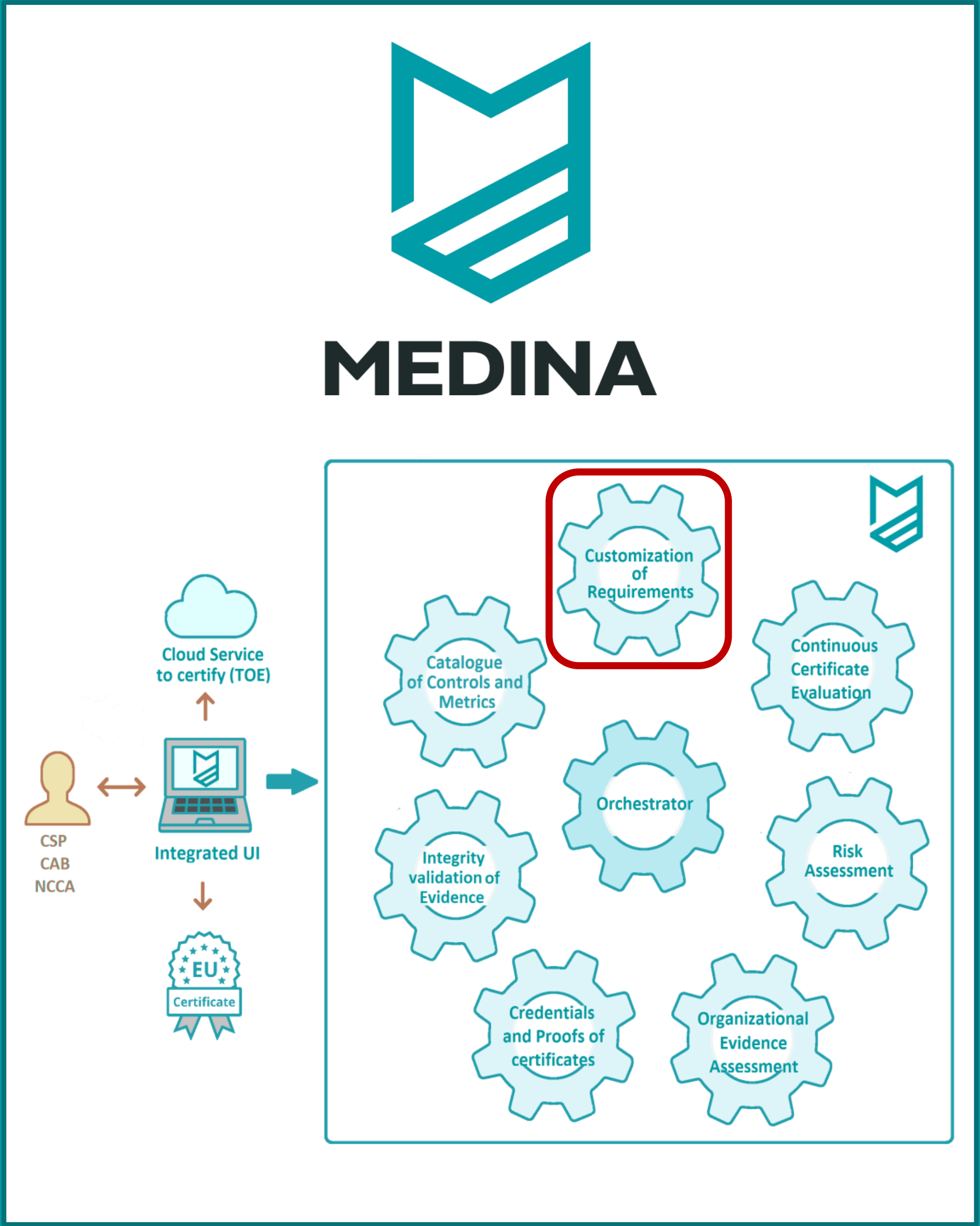
  docker build -t nl2cnl_translator_image .

Technical specifications

- Python 3.8+
- Docker-compose for installation

CNL Editor

- ➤ Overview
  - - Purpose
  - - Role in MEDINA Architecture


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

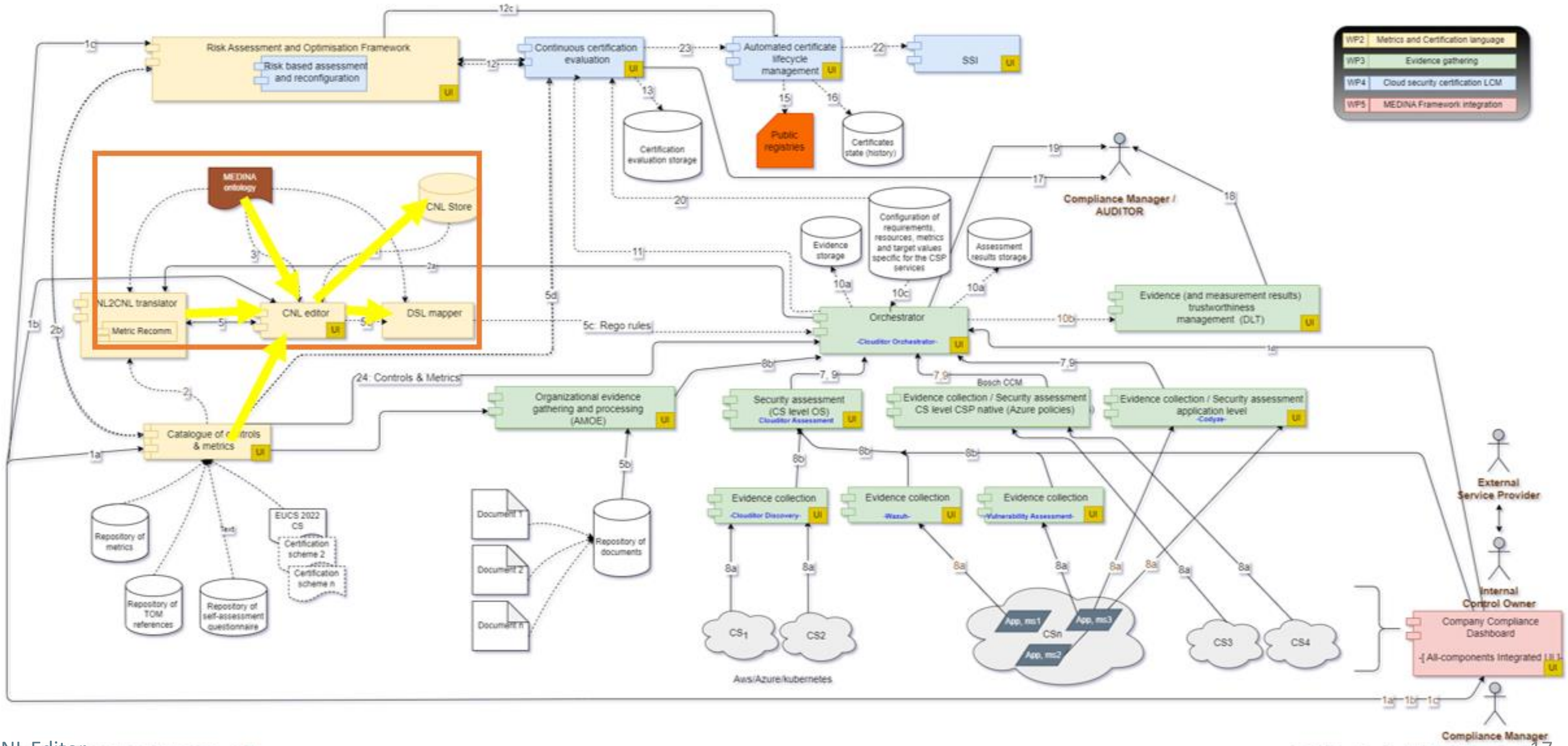
CNL Editor

- The CNL Editor is the component that allow, with a **Graphical Web Interface**, to make some **customization of REO objects**: Requirement and its associated Obligations.
  - Obligation is a statement written in CNL language to express a compliance policy in the form MetricName MUST ResourceType (operator, TargetValue).
- User can:
  - Visualize all REOs (pertaining to the CS_Id that user has in Keycloak profile)
  - Change REO:
    - Delete some Obligations
    - Change the TargetValue specified in Obligations
- It offers **APIs** to other MEDINA components to create, search and get REO objects
- This component uses a vocabulary (static .owl file) that contains Obligations Ontology as specified in Catalogue of Controls and Metrics (Actions=MetricName, Terms includes: ResourceType, TargetValueType, Operator)

CNL Editor

- The tool is enhanced with some extra features:
  1. **Tooltip** for help on information fields
  2. **User Manual** user can select help to see user manual for the tool (help button)

CNL Editor
in MEDINA architecture



Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
Continuous certification evaluation
Automated certificate lifecycle management
SSI
UI
12c
1c
12
23
22
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
MEDINA ontology
CNL Store
NL2CNL translator
Metric Recomm
CNL editor
DSL mapper
5c: Rego rules
5d
11
20
2a
3
5
2
1b
2b
24: Controls & Metrics
Catalogue of controls & metrics
1a
Organizational evidence gathering and processing (AMOE)
5b
Repository of metrics
Repository of TOM references
Repository of self-assessment questionnaire
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Compliance Manager / AUDITOR
19
17
18
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10b
Orchestrator
-Clouditor Orchestrator-
Evidence (and measurement results) trustworthiness management (DLT)
8b
7, 9
Bosch CCM
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
Evidence collection
-Clouditor Discovery-
-Wazuh-
-Vulnerability Assessment-
8a
CS1
CS2
CSn
App, ms1
App, ms2
App, ms3
CS3
CS4
Aws/Azure/kubernetes
External Service Provider
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
Compliance Manager

Interactions with other components

NL2CNL translator

- Create REOs, as .xml files, that can be customised by CNL Editor

DSL Mapper

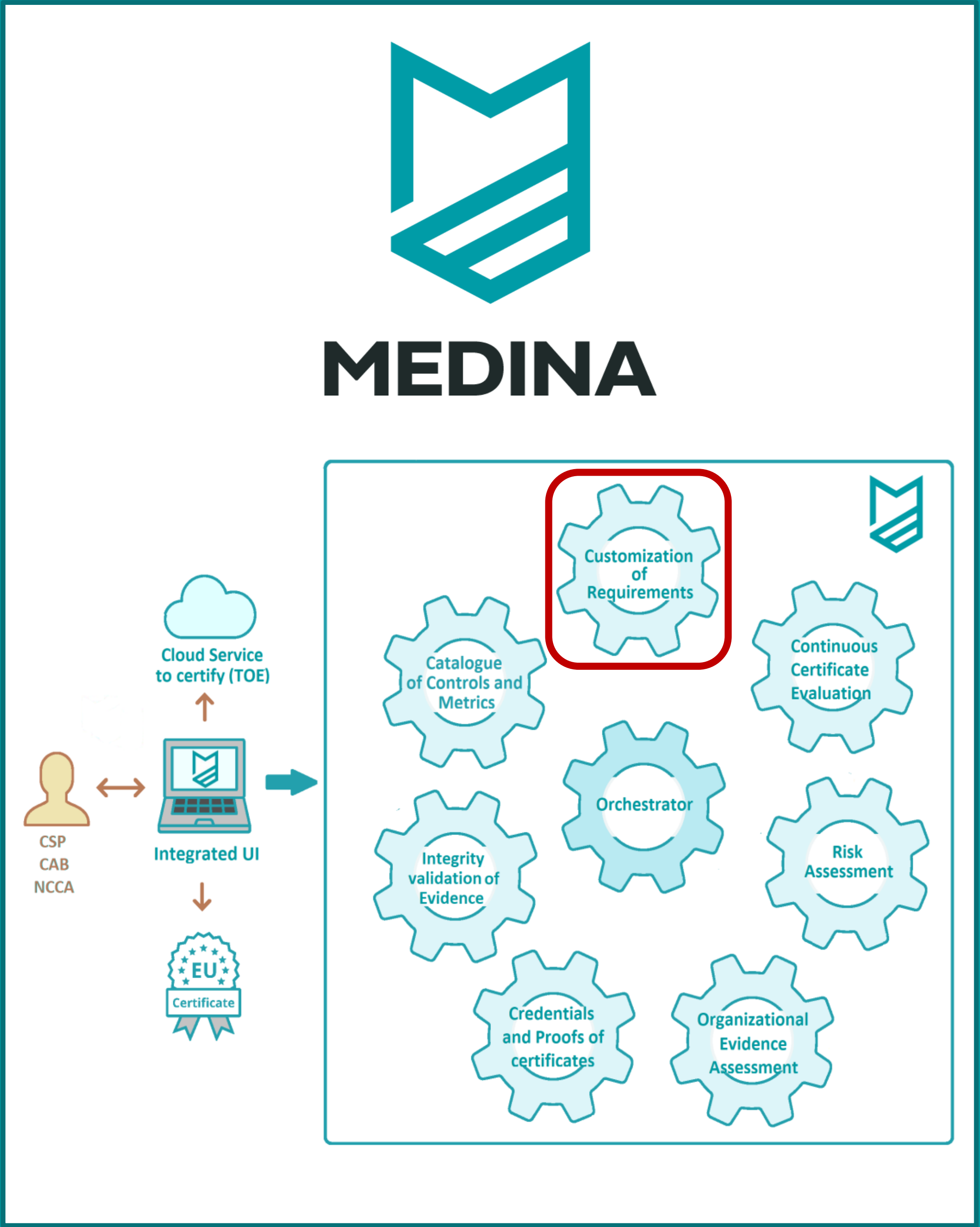
- Invoked by CNL Editor, Translate Obligations into Rego policies

User

- Consults the REOs pertaining to Cloud Service Id whose the user is authorised
- Performs customisation (Edit)

CNL Editor

- How to use it
  - Functionalities
  - Demo


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

CNL Editor

- **User** making login to CNL Editor can:
  - Consult a **List of REOs** filtered based on CS_Id (Cloud Service Id). Cloud_Service_Id is stored inside each REO and for each user the list of Cloud_Service_Ids are store in user Keycloak profile
  - Select, from this list of REOs, a specific REO to makes operations on it:
    - **Show** REO details: Controls and Obligations expressed as
      - *ResourceType MUST MetricsName (operator, TargetValue)*
    - **Edit** a REO to:
      - Change Operator between a restricted choice
      - Customise TargetValue
      - Delete Obligations (user can delete all Obligations except one)
    - **Map** a REO to invoke DSL Mapper on it
    - **Delete** a REO

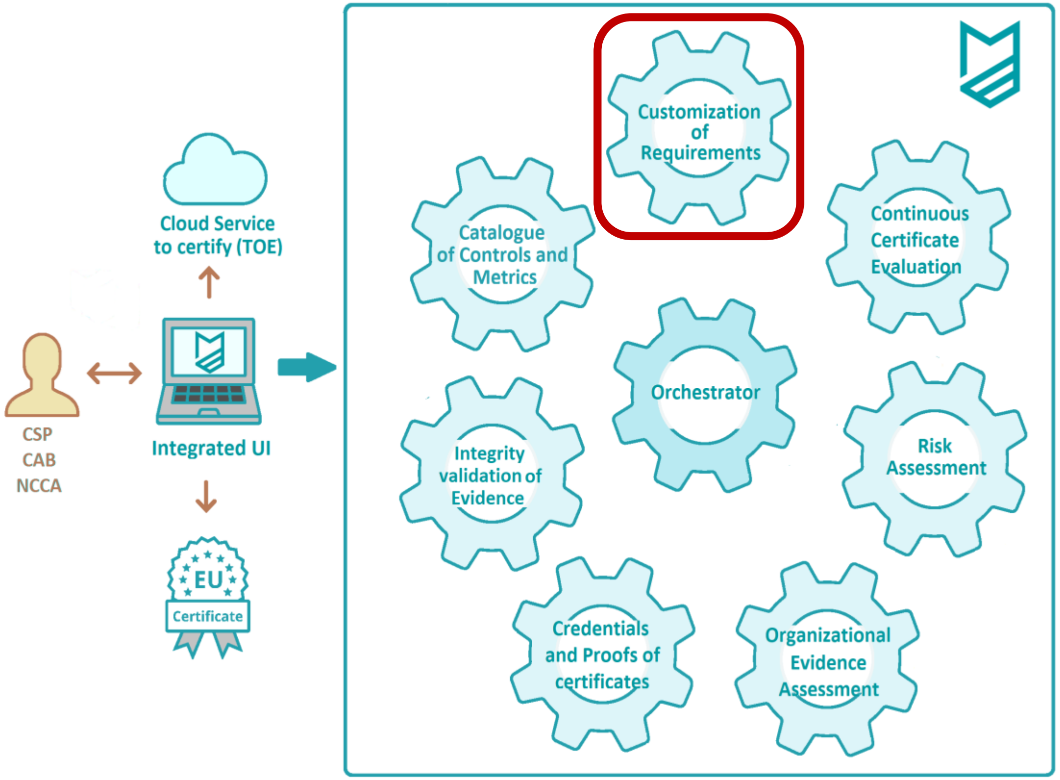
CNL Editor

- DEMO -

CNL Editor

- ➤ Installation
  - Deployment
  - Technical Specifications

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

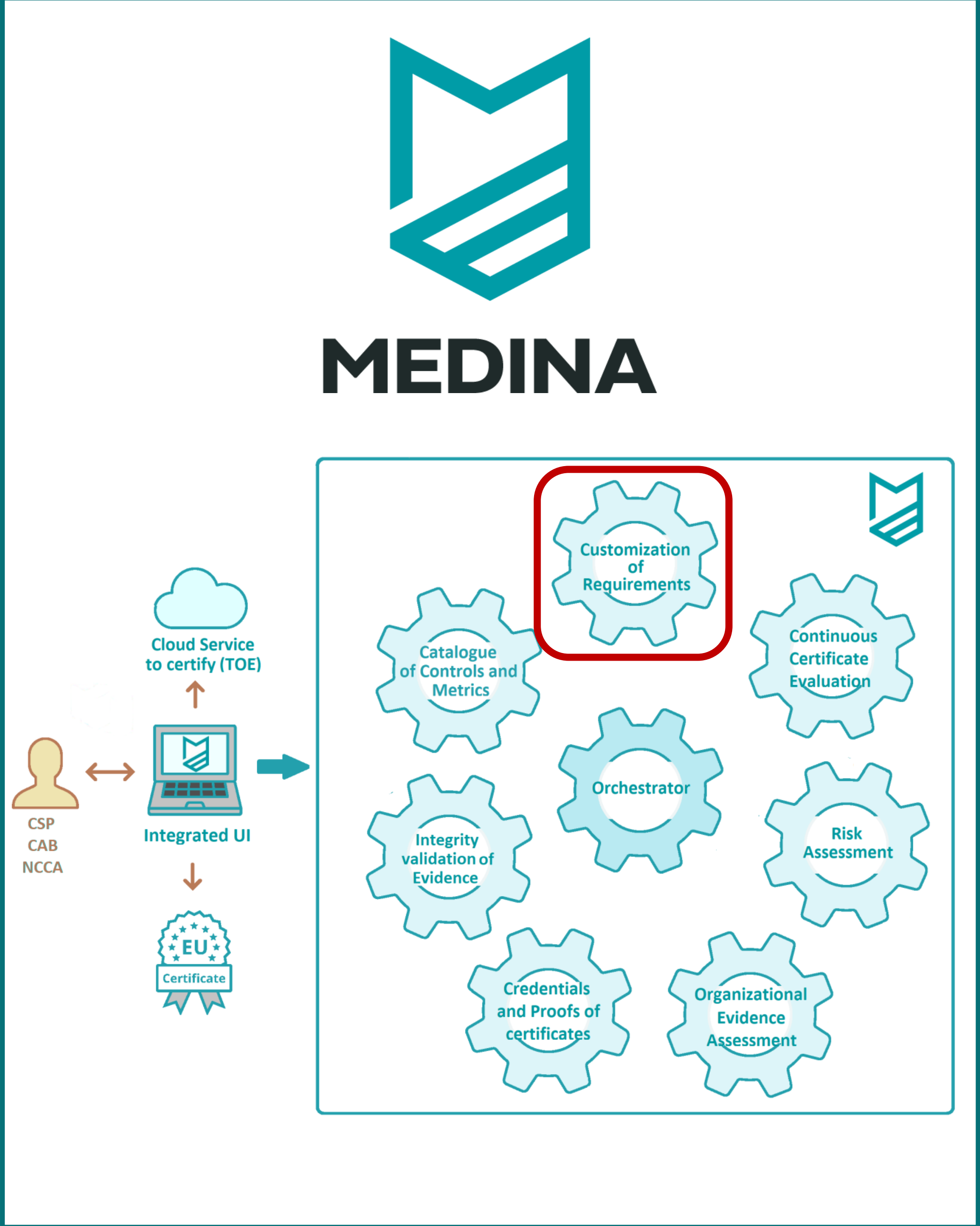
- Install for local deployment
  - The CNL Editor is developed using the microservice architecture and is composed of 5 microservices containerized in Docker. Component software is on the GitLab repository:
    - https://git.code.tecnalia.com/medina
  - Build:

    docker build -t <project-name> ./<microservice-name>

- Technical specifications
  - Java with the use of Spring Boot used for all the API and the CNL Editor Web Application logic
  - GWT (Google Web Toolkit) and Vaadin frameworks for the UI
  - CRUD (Create, Read, Update, Delete) operations on REO are available through REST APIs
  - Docker-compose for installation

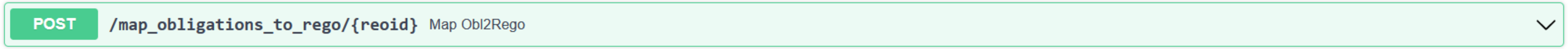
DSL Mapper

- Overview
  - Purpose
  - Role in MEDINA Architecture


MEDINA
Customization of Requirements
Cloud Service to certify (TOE)
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
CSP
CAB
NCCA
Integrated UI
Integrity validation of Evidence
Risk Assessment
EU
Certificate
Credentials and Proofs of certificates
Organizational Evidence Assessment

DSL Mapper

- Component’s goals in MEDINA:
  - Translate obligations into Rego policies/rules
  - Send Rego policies/rules to the Orchestrator
- It is **not** provided with a User Interface
- It offers an **API** to other MEDINA components to use its functionalities

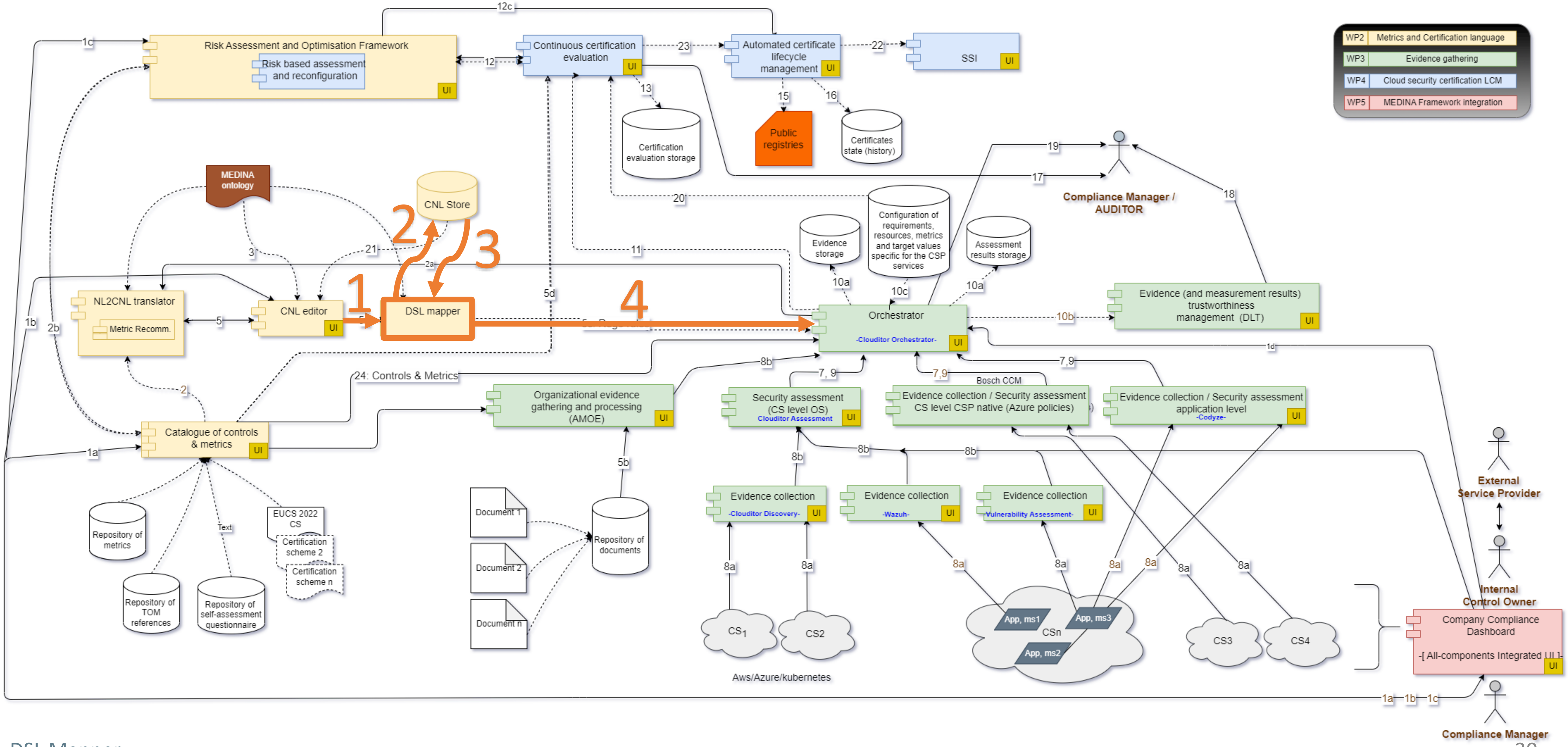


POST /map_obligations_to_rego/{reoid} Map Obl2Rego

DSL Mapper

- Input data
  - REO objects -> from the CNL Store of the CNL Editor
  - A REO object is read from the CNL Store and its obligations are translated into Rego rules
- Output data
  - Rego rules-> sent to the Orchestrator
  - The Orchestrator will assess obligations according to specified operator and Target Value

DSL Mapper in MEDINA architecture


Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
Continuous certification evaluation
UI
Automated certificate lifecycle management
UI
SSI
UI
12c
1c
12
23
22
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
MEDINA ontology
CNL Store
2
3
20
21
3
2a
11
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
1
DSL mapper
5d
4
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Catalogue of controls & metrics
UI
1a
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
External Service Provider
5b
8b
8b
8b
Repository of metrics
Text
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
8a
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager
WP2
Metrics and Certification language
WP3
Evidence gathering
WP4
Cloud security certification LCM
WP5
MEDINA Framework integration

Interactions with other components

CNL Editor

- It invokes the DSL Mapper passing the identifier of a REO to translate its obligations into Rego policies/rules
- It is also queried by the DSL Mapper to retrieve the REO object from the CNL Store corresponding to a certain REO identifier

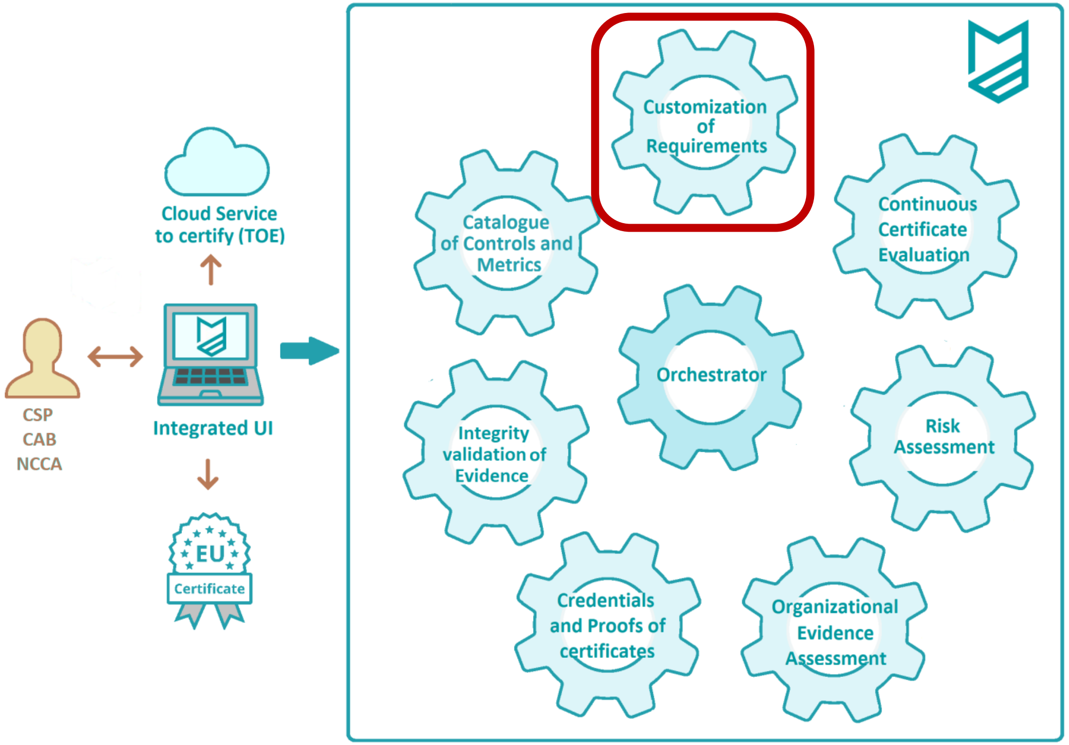
Orchestrator

- It is invoked by the DSL Mapper, which sends the Rego policies/rules corresponding to the metrics to be assessed

DSL Mapper

- How to use it
  - Functionalities

MEDINA



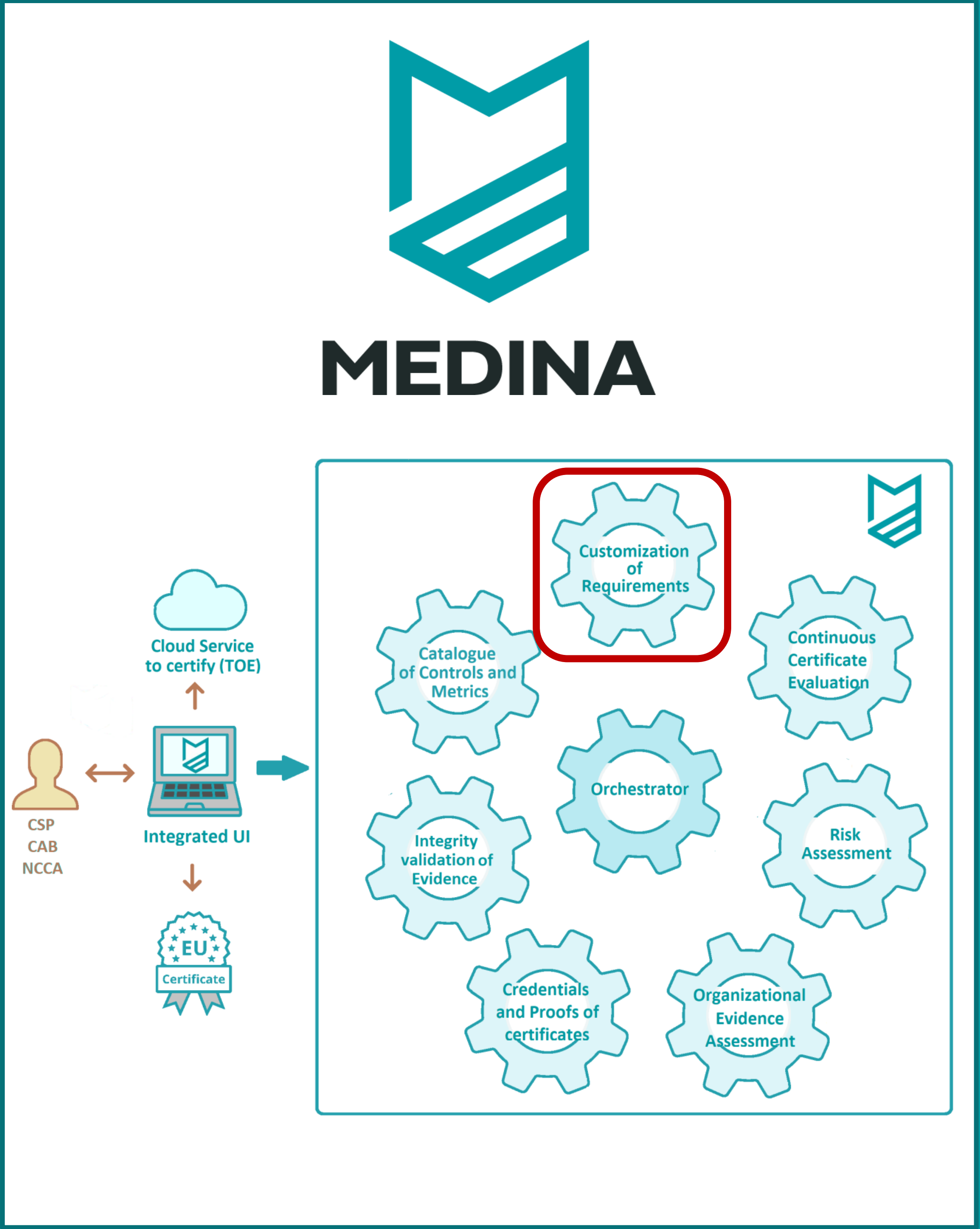
Customization of Requirements
Continuous Certificate Evaluation
Catalogue of Controls and Metrics
Cloud Service to certify (TOE)
Orchestrator
Risk Assessment
Integrity validation of Evidence
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Credentials and Proofs of certificates
Organizational Evidence Assessment

From obligations to rego policies

- This process is **automatic** and **transparent** to the user
- This functionality is invoked on a REO object from the CNL Editor
- The DSL Mapper read the specified REO object from the CNL Store and translated all the obligations into Rego policies/rules
- Each Rego rule is sent to the Orchestrator to be assessed

DSL Mapper

- Installation
  - Deployment
  - Technical Specifications


MEDINA
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment
Cloud Service to certify (TOE)
Integrated UI
CSP
CAB
NCCA
EU
Certificate

Installation

MEDINA

Local deployment

- The DSL Mapper is developed by using the *fastapi* web framework in Python 3.8 and it is containerized in Docker. The code is store in the GitLab repository of the project:
  - https://git.code.tecnalia.com/medina
- Build:

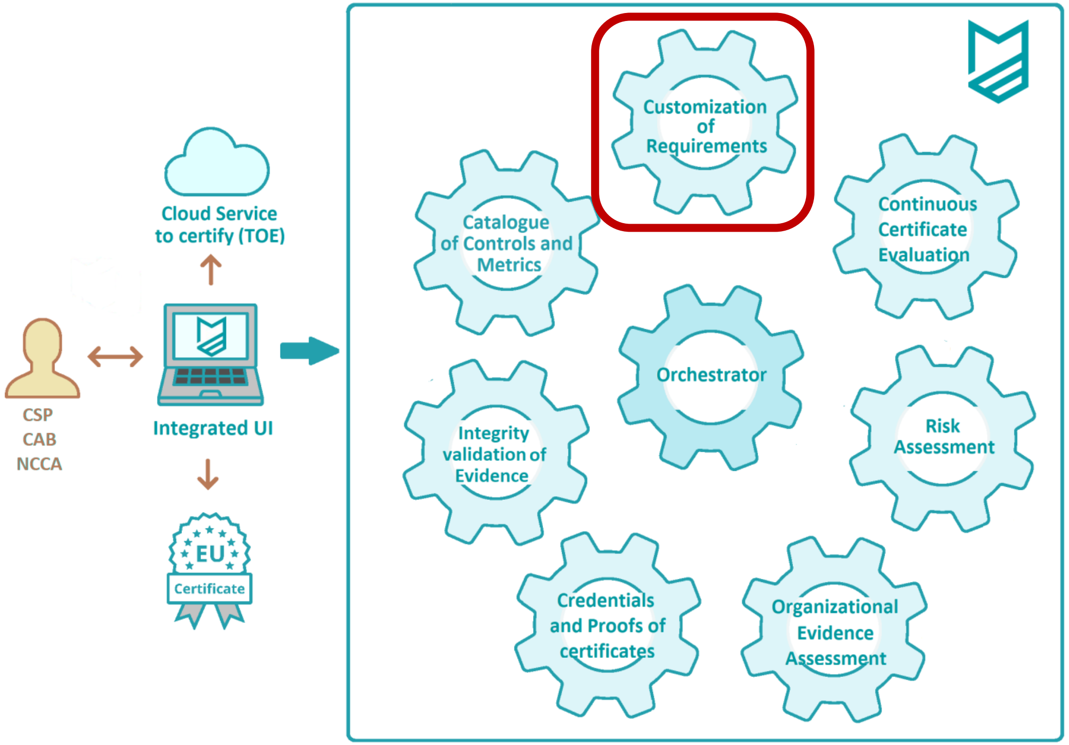
```
docker build -t dsl_mapper_image .
```

Technical specifications

- Python 3.8+
- Docker-compose for installation

➤ Further Information

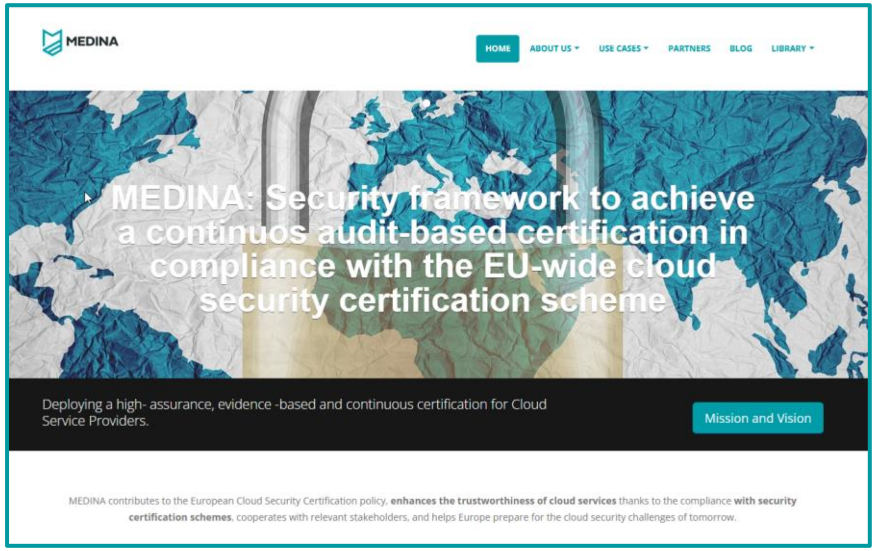
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** *https://medina-project.eu/public-deliverables*
- Framework demonstrator is available in the MEDINA **YouTube channel** *https://www.youtube.com/@MedinaprojectEU*
- MEDINA Community in **Zenodo** *https://zenodo.org/communities/medina*
- Source code in the public **GitLab** *https://git.code.tecnalia.com/medina/public*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Fraunhofer
AISEC

Hewlett Packard
Enterprise

Consiglio Nazionale
delle Ricerche

BOSCH

Fabasoft

XLAB

NIXU
cybersecurity.

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

MEDINA

Risk assessment and optimization framework

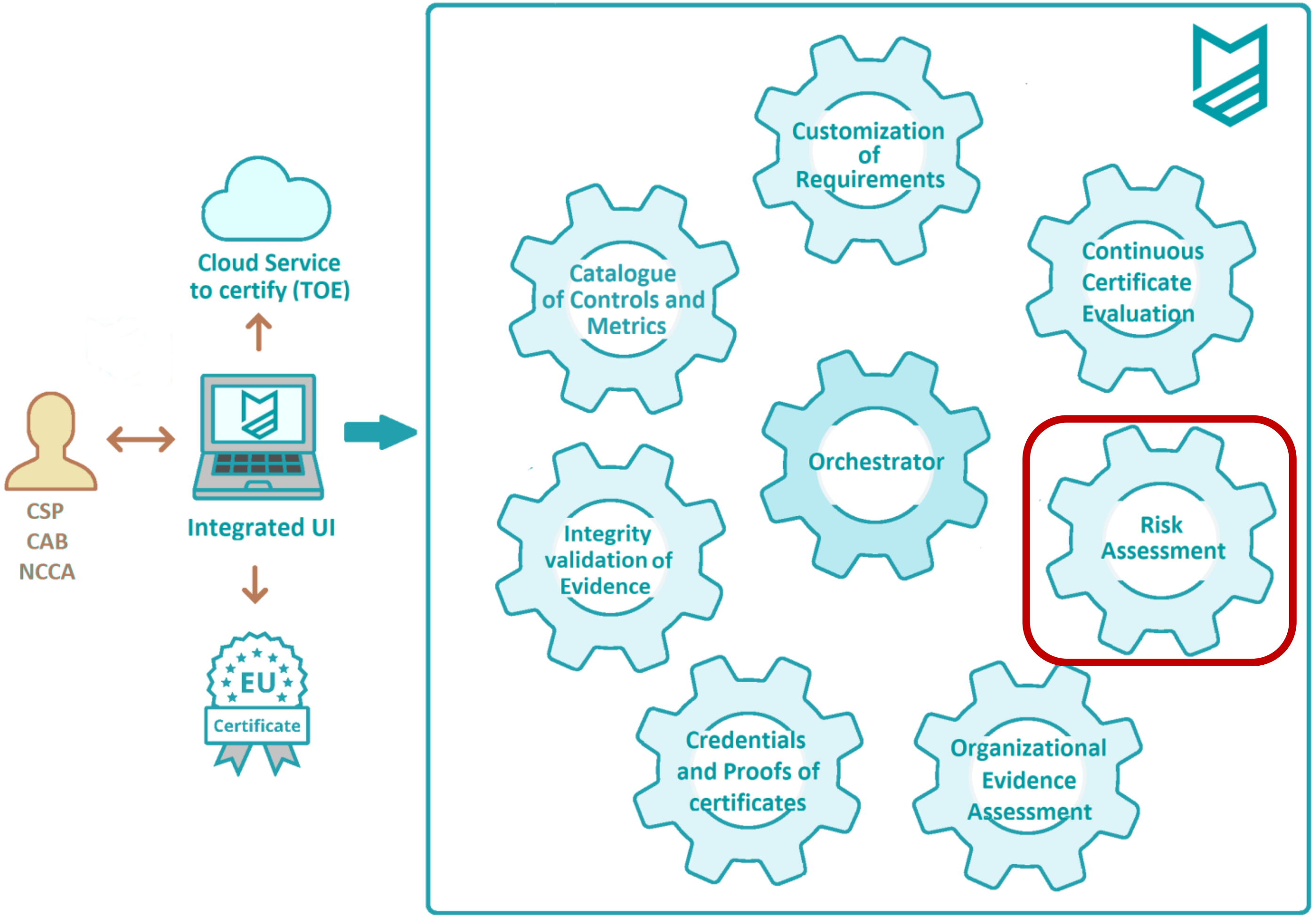
Artsiom Yautsiukhin, Stefano Fagnano (CNR, Italy)

September 2023

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

Chapters

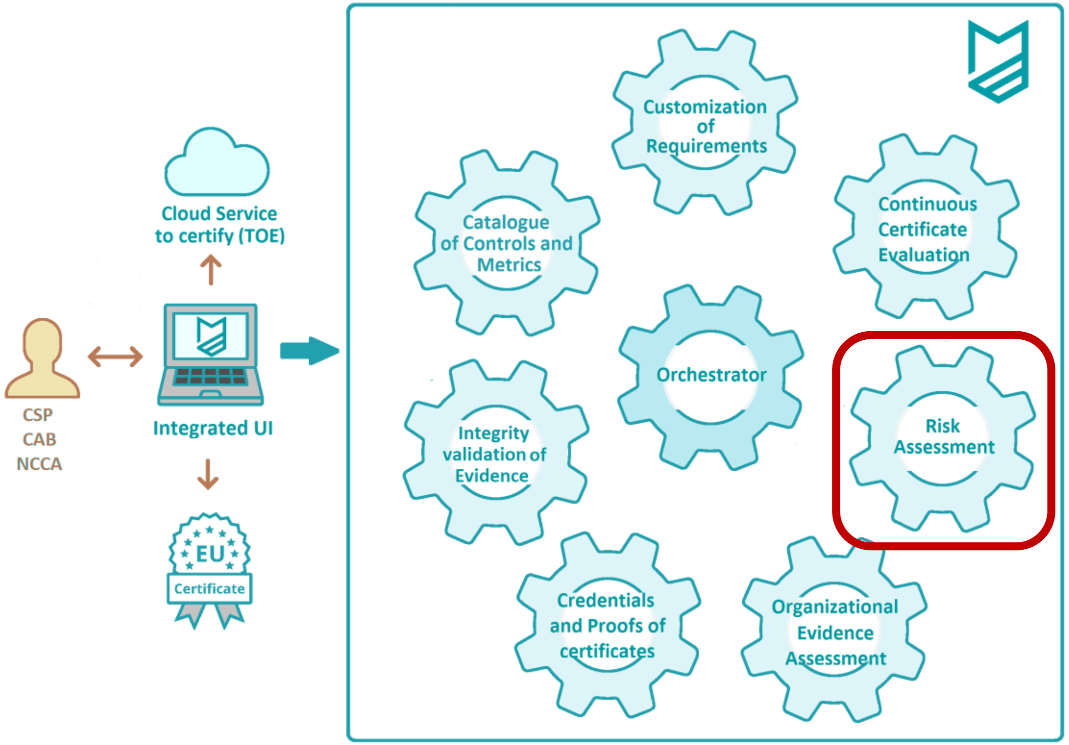
- Overview
- How to use it
- Installation
- Further information


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Risk assessment and optimization framework

- Overview
  - Purpose
  - Role in MEDINA Architecture

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Risk assessment and optimization framework (RAOF)

MEDINA

The goal

- To provide a risk-based analysis of non-conformities (with EUCS) for Cloud services

Every CSP performs Risk Assessment (in-house risk assessment)

- We do not aim to substitute it
- But, our tool can be used for that

Our risk assessment:

- supports certification evaluation process (against EUCS)
- is set up for Cloud
- can be used
    - for “manual” analysis by an operator (e.g., compliance manager)
    - for automatic analysis (assuming that up-to-date information is automatically provided)
- supports optimization of the future effort for ensuring compliance

Two phases for risk assessment

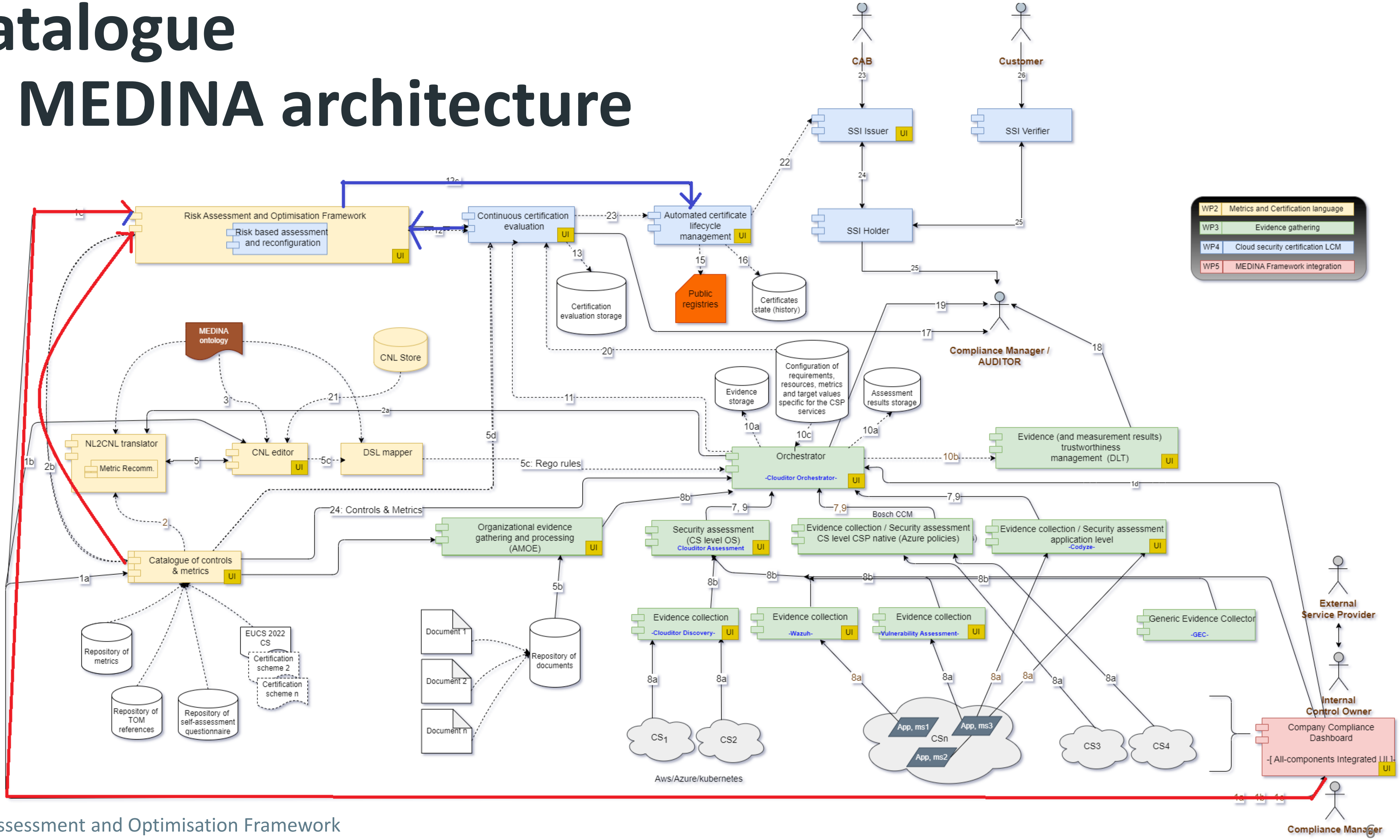
Bootstrapping phase

- Fulfilled **requirements** are provided by a *Dashboard (API) or an operator (GUI)*
- Relevant for analysis of non-conformities (major/minor)
- Can be used for optimization analysis

Continuous monitoring phase

- Based on measured **metrics** provided by *monitoring tools (API)*
- Useful for analysis of non-conformities (major/minor)
- Can be used for dynamic monitoring

Catalogue in MEDINA architecture



CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
24
SSI Holder
25
22
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
MEDINA ontology
CNL Store
20
3
21
2a
11
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
5d
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
External Service Provider
Internal Control Owner
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
8a
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration

Risk Assessment and Optimisation Framework

Interactions with other components

User (GUI)

- Conduct risk assessment
- Conduct risk optimisation

Compliance Dashboard (API)

- Conduct risk assessment
- Conduct risk optimisation

Catalogue of controls and metrics

- Get status of requirements

Continuous Certificate Evaluation

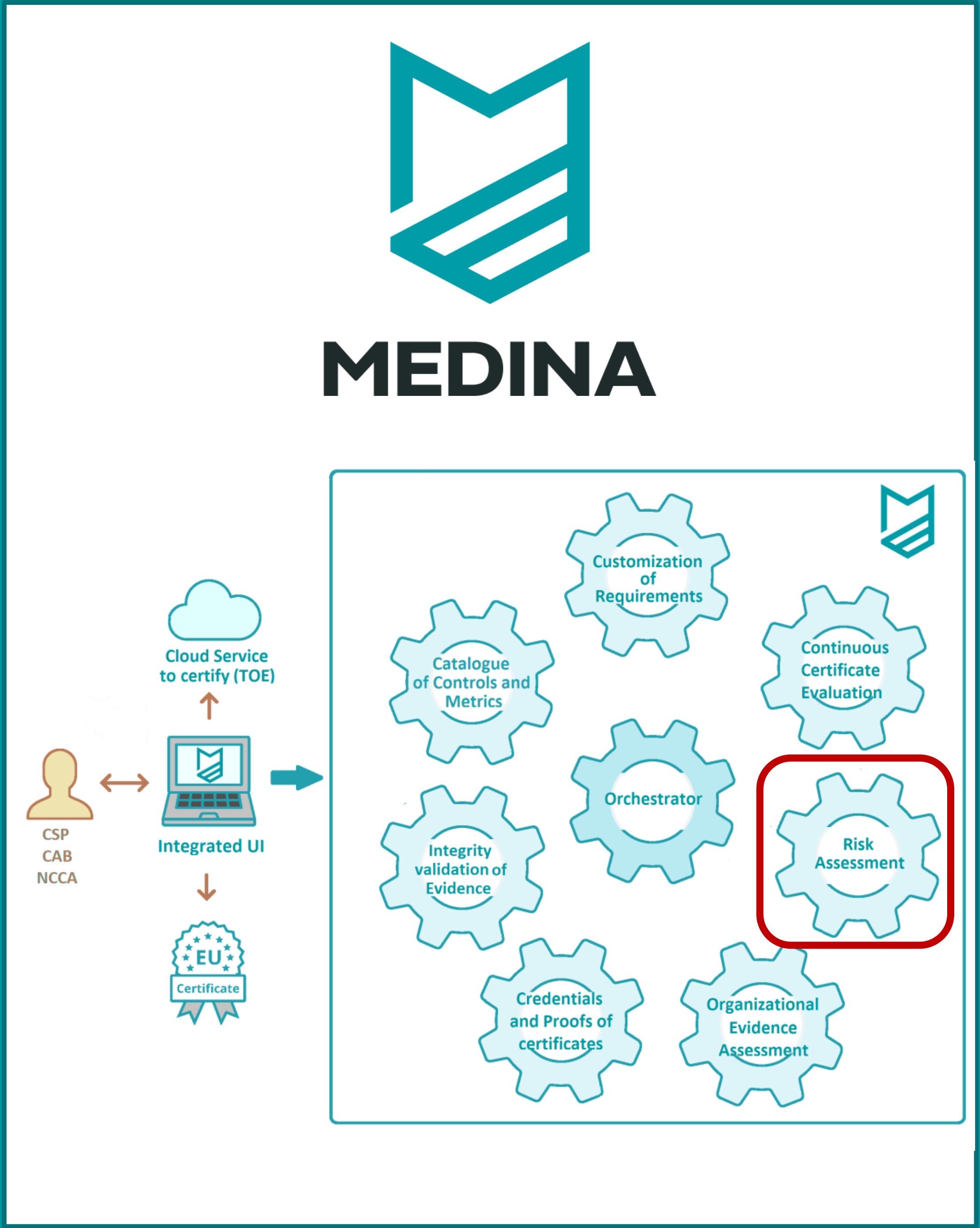
- Get measured status of requirements

Certificate Life-Cycle Manager

- Send non-conformity assessment result

Risk assessment and optimization framework

- How to use it
  - Functionalities
  - Demo


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Self-Assessment Tool for Risk Analysis (SATRA)

- Implemented as a service
- Allows conducting fast and simple cyber risk assessment for CSP
- Requires only providing information about
  - Addressed security requirements
  - Main assets
- Based on cyber security certification schemas for CSP
  - EUCS
  - Can be extended for other C5, SecNumCloud, ISO 27001, etc.

SATRA operation in a nutshell

Input

- **Threats** (and *frequency*) – enlisted in the tool
- **Assets** (CIA *impact*) – provided by an operator
- Requirements/**Vulnerabilities** (success *probability*) – collected with a questionnaire or monitored

Processing

- Fully **automatic** way combining frequency, impact and success/survival probability.
- Result: *real risk* value

Non-compliance evaluation

- *Real risk – ideal risk*
- Major or minor deviation: compare the difference with a threshold

Optimisation

- Helps a compliance manager to identify the failed requirements which can improve security in the most cost-effective way.
- Input:
  - Assessed risk
  - Cost of failed requirements
  - Available (additional) budget
- Processing:
  - Optimising expenditure
- Output:
  - Selection of requirements to implement
  - Updated risk/non-compliance (if these requirements are implemented)

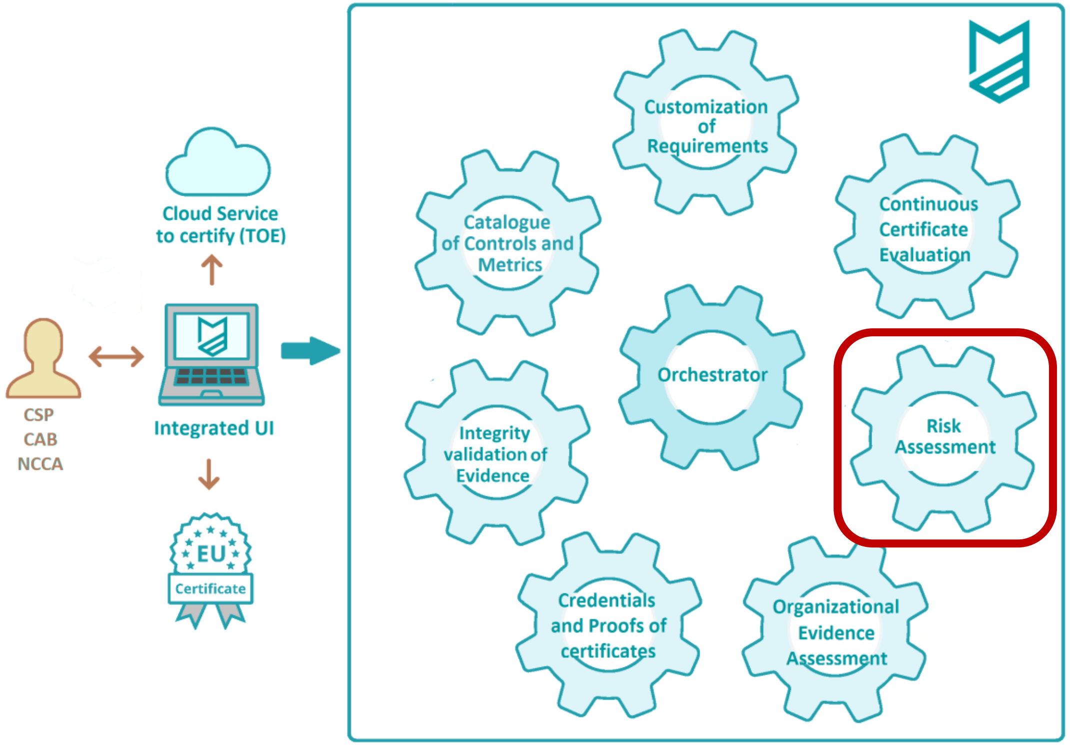
Risk assessment and optimization framework

- DEMO -

Risk assessment and optimization framework

- Installation
  - Deployment
  - Technical Specifications

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

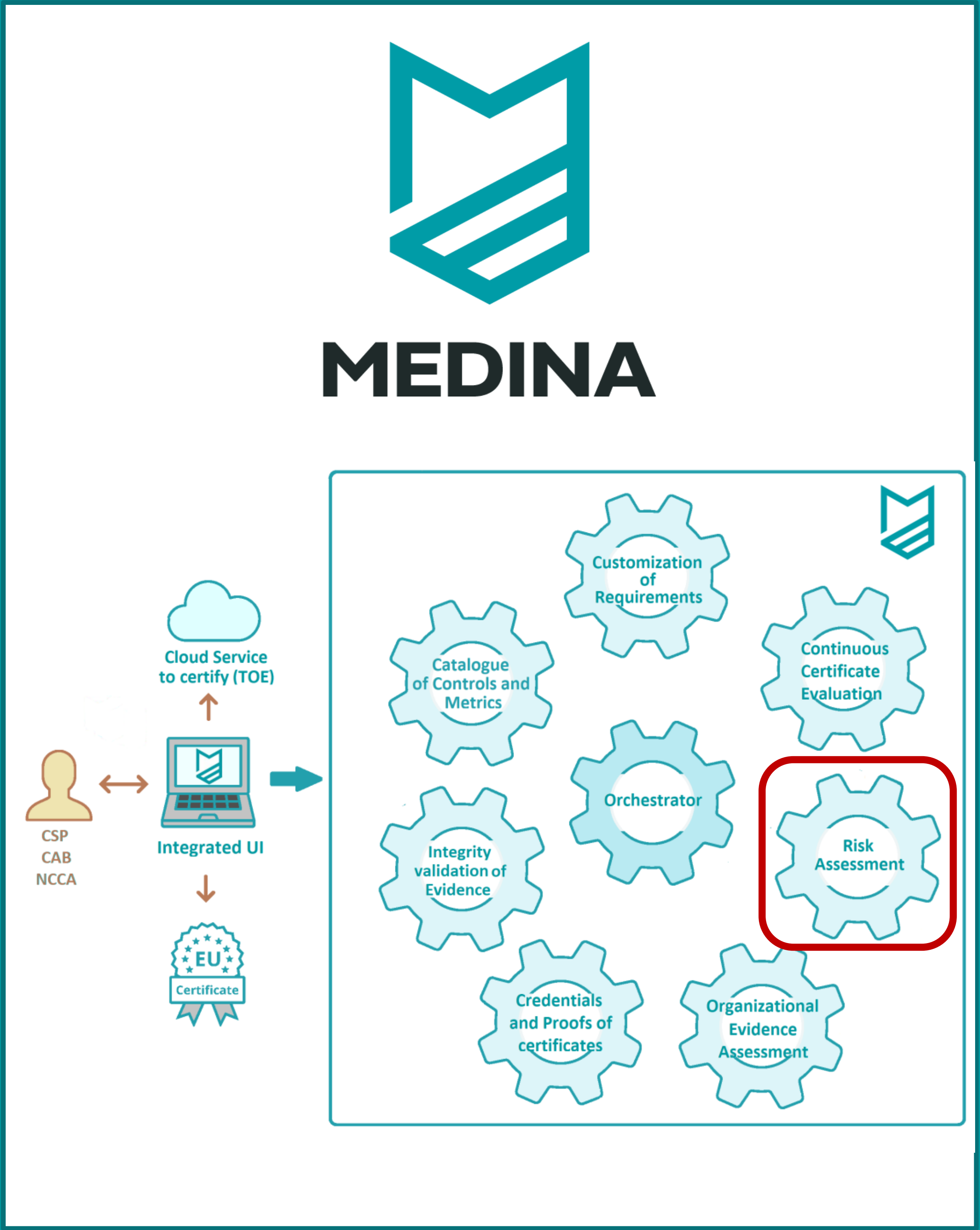
MEDINA

- RAOF uses docker-compose to execute and deploy the GUI and the API interfaces (for more options, see Readme file)
  - There are four containers:
    - **engine**: this container contains the risk assessment module, the risk-based decision support, and the GUI;
    - **app**: this container contains the API interface;
    - **db**: this container is a DBMS;
    - **dmm**: this container instances the risk optimizer service.

- Technical specifications
  - Uses the Springboot 5 framework
  - Runs over a Tomcat 8 and is running on Apache2 Web Service
  - The MySQL DBMS for data storage
  - Docker-compose for installation

Risk assessment and optimization framework

- ➤ Further information


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

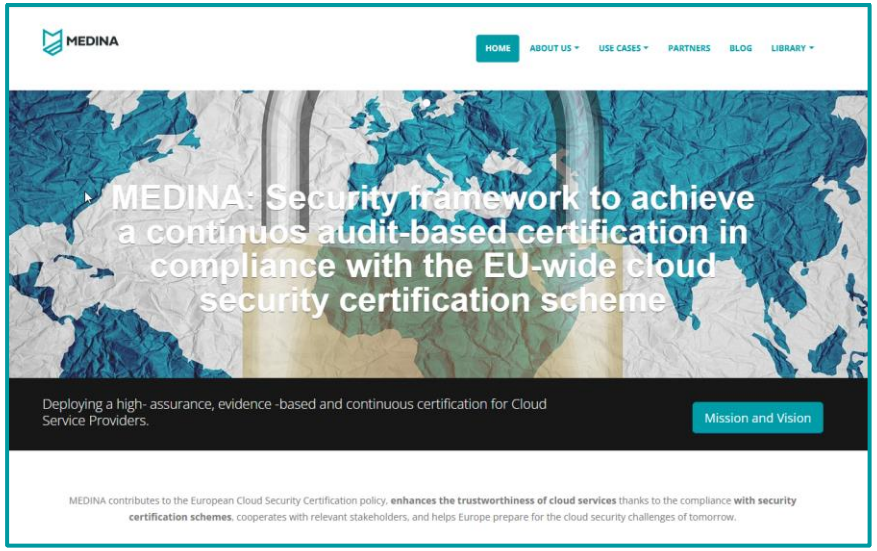
MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** *https://medina-project.eu/public-deliverables*

- Framework demonstrator is available in the MEDINA **YouTube channel** *https://www.youtube.com/@MedinaprojectEU*

- MEDINA Community in **Zenodo** *https://zenodo.org/communities/medina*

- Source code in the public **GitLab** *https://git.code.tecnalia.com/medina/public*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

NIXU cybersecurity.

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

MEDINA

Cloud Evidence Collector Security Assessment Orchestrator

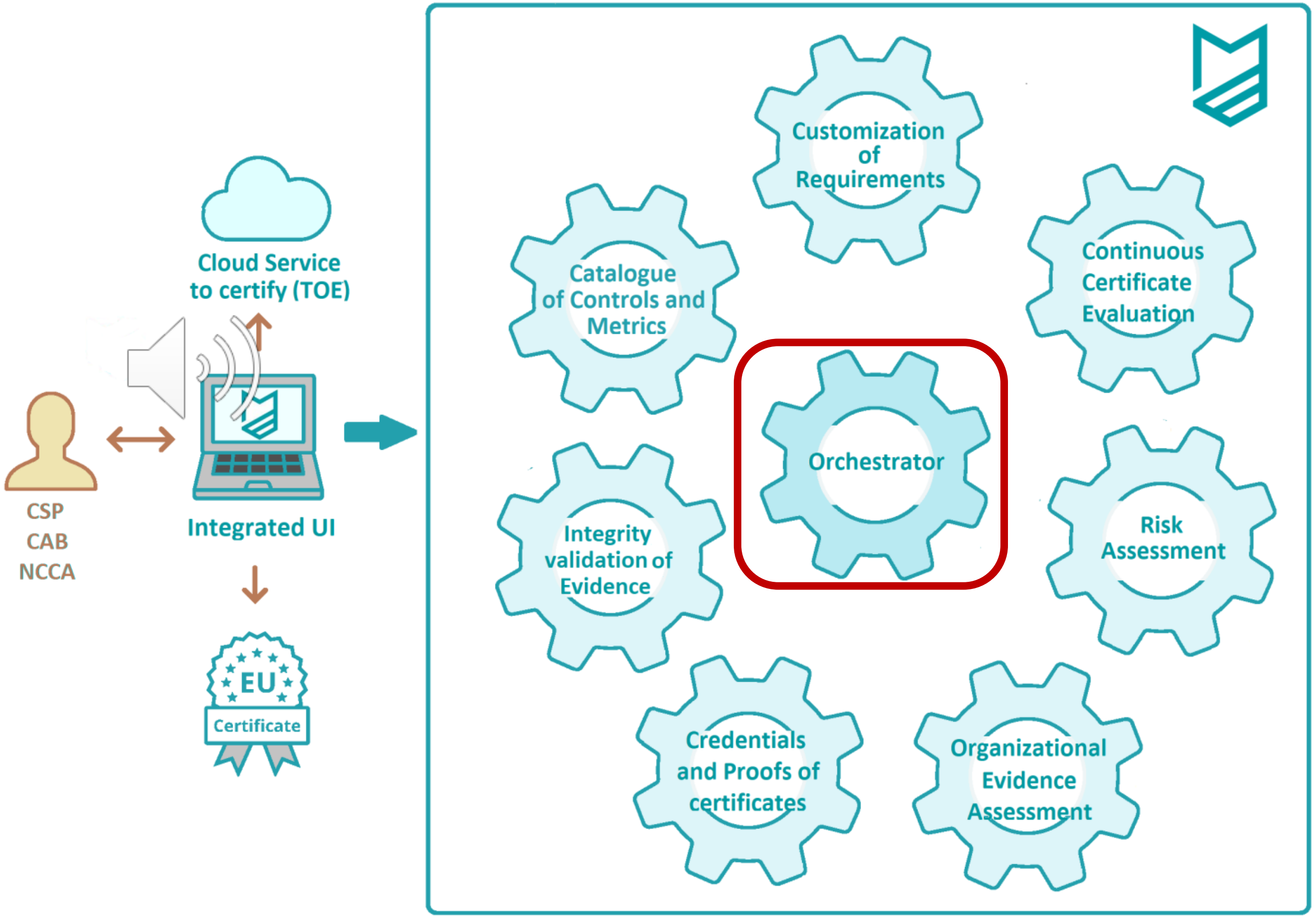
Fraunhofer AISEC

September 2023

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

Chapters

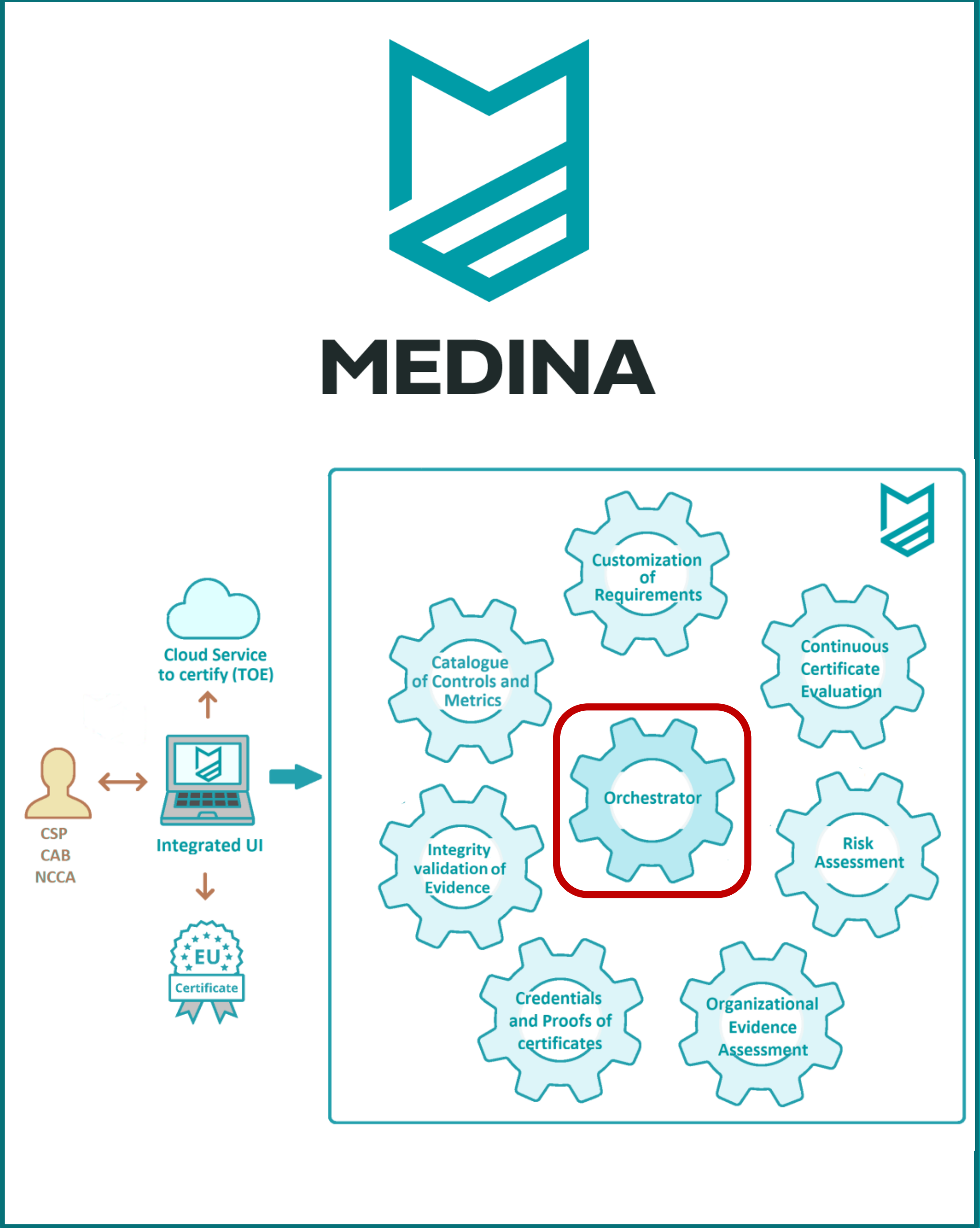
- Overview
- How to use it
- Installation
- Further information


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Clouditor Components

- Cloud Evidence Collector
- Security Assessment
- Orchestrator

- Overview
  - - Purpose
  - - Role in MEDINA Architecture

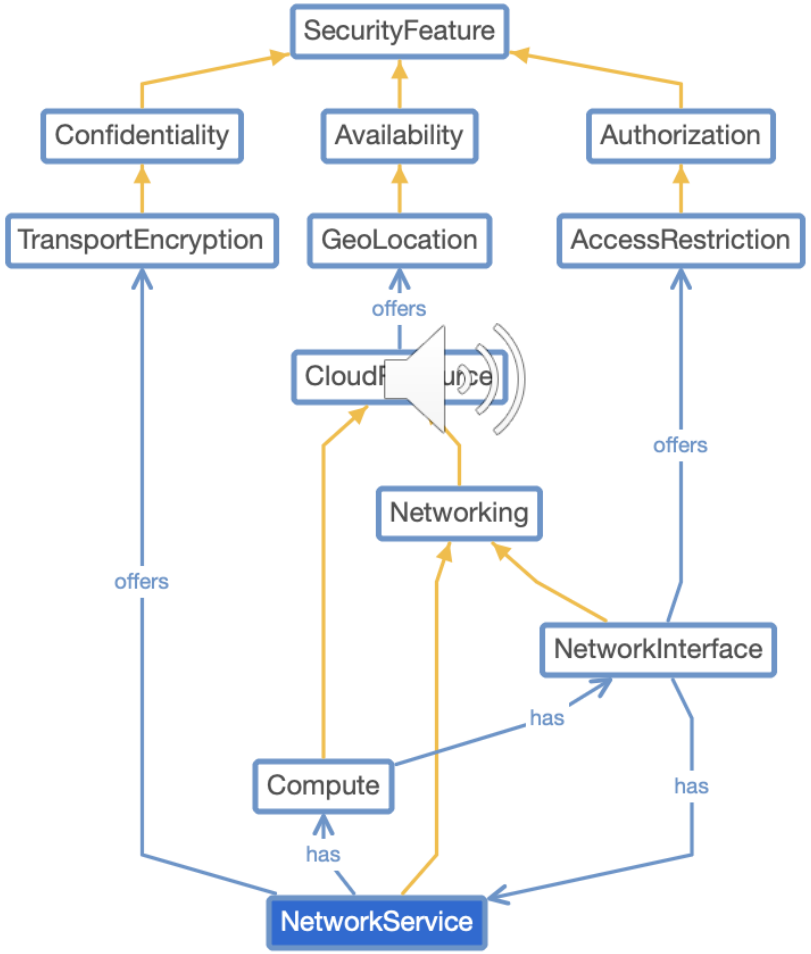

MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Cloud Evidence Collector

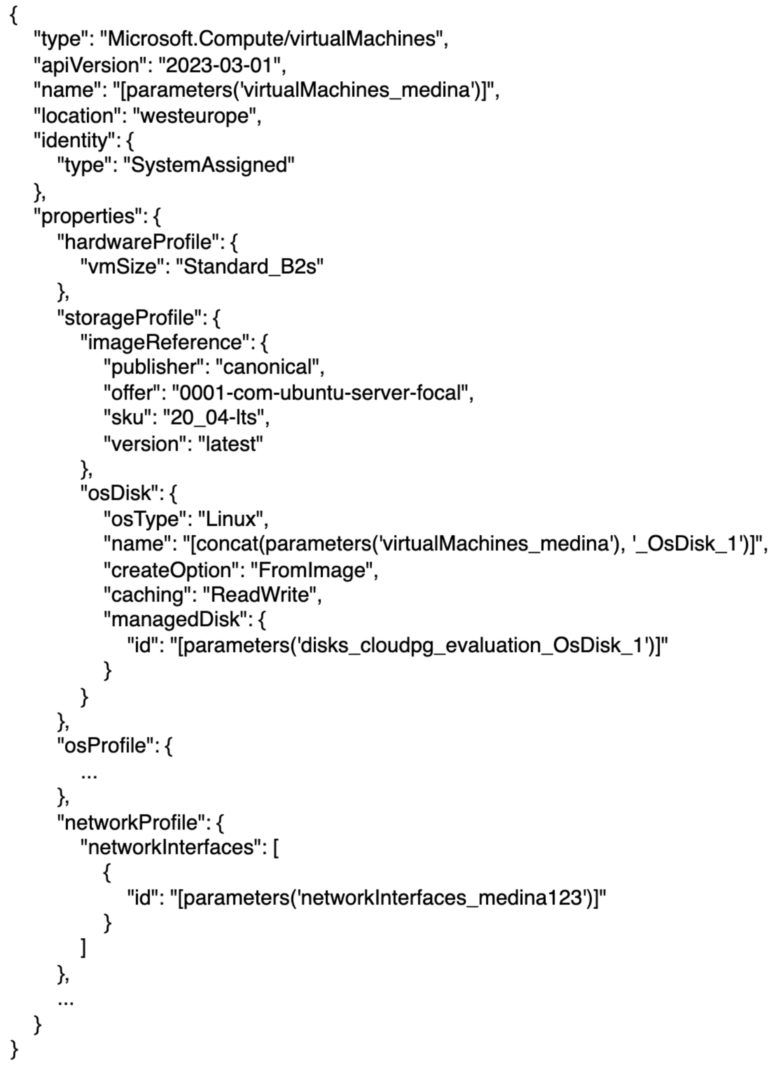
MEDINA

- The Cloud Evidence Collector collects evidence using cloud APIs, such as configurations of virtual machines and storages
- It enriches the evidence with **ontological information**, assigning each resource description to a generic cloud resource type
- The evidences are stored with the Orchestrator and are accessible via the **Orchestrator UI**

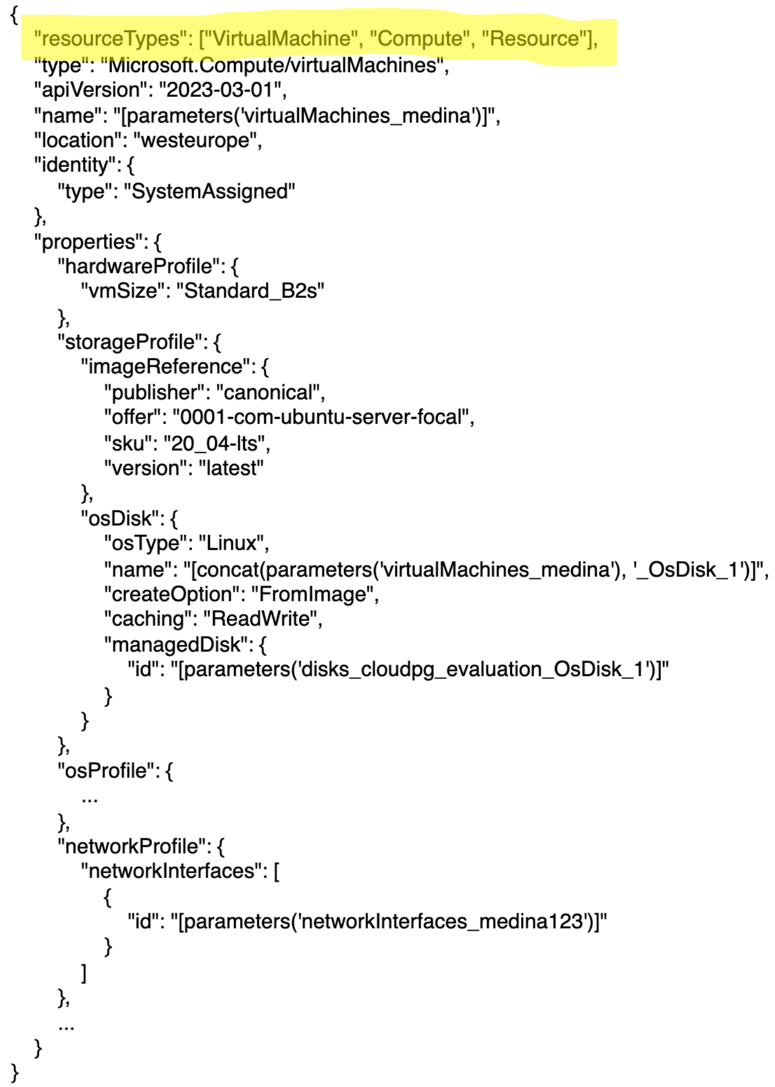
Cloud Resource Ontology



Cloud Resource Ontology



```
{
  "type": "Microsoft.Compute/virtualMachines",
  "apiVersion": "2023-03-01",
  "name": "[parameters('virtualMachines_medina')]",
  "location": "westeurope",
  "identity": {
    "type": "SystemAssigned"
  },
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_B2s"
    },
    "storageProfile": {
      "imageReference": {
        "publisher": "canonical",
        "offer": "0001-com-ubuntu-server-focal",
        "sku": "20_04-lts",
        "version": "latest"
      },
      "osDisk": {
        "osType": "Linux",
        "name": "[concat(parameters('virtualMachines_medina'), '_OsDisk_1')]",
        "createOption": "FromImage",
        "caching": "ReadWrite",
        "managedDisk": {
          "id": "[parameters('disks_cloudpg_evaluation_OsDisk_1')]"
        }
      }
    },
    "osProfile": {
      ...
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[parameters('networkInterfaces_medina123')]"
        }
      ]
    },
    ...
  }
}
```



```
{
  "resourceTypes": ["VirtualMachine", "Compute", "Resource"],
  "type": "Microsoft.Compute/virtualMachines",
  "apiVersion": "2023-03-01",
  "name": "[parameters('virtualMachines_medina')]",
  "location": "westeurope",
  "identity": {
    "type": "SystemAssigned"
  },
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_B2s"
    },
    "storageProfile": {
      "imageReference": {
        "publisher": "canonical",
        "offer": "0001-com-ubuntu-server-focal",
        "sku": "20_04-lts",
        "version": "latest"
      },
      "osDisk": {
        "osType": "Linux",
        "name": "[concat(parameters('virtualMachines_medina'), '_OsDisk_1')]",
        "createOption": "FromImage",
        "caching": "ReadWrite",
        "managedDisk": {
          "id": "[parameters('disks_cloudpg_evaluation_OsDisk_1')]"
        }
      }
    },
    "osProfile": {
      ...
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "[parameters('networkInterfaces_medina123')]"
        }
      ]
    },
    ...
  }
}
```

Security Assessment

MEDINA

- The Security Assessment receives evidences from the Cloud Evidence Collector and assesses them using pre-defined metrics
- The metrics are retrieved from the Catalogue of Controls and Metrics (via the Orchestrator)
- The Assessment Results are stored via the Orchestrator and are accessible via the **Orchestrator UI**

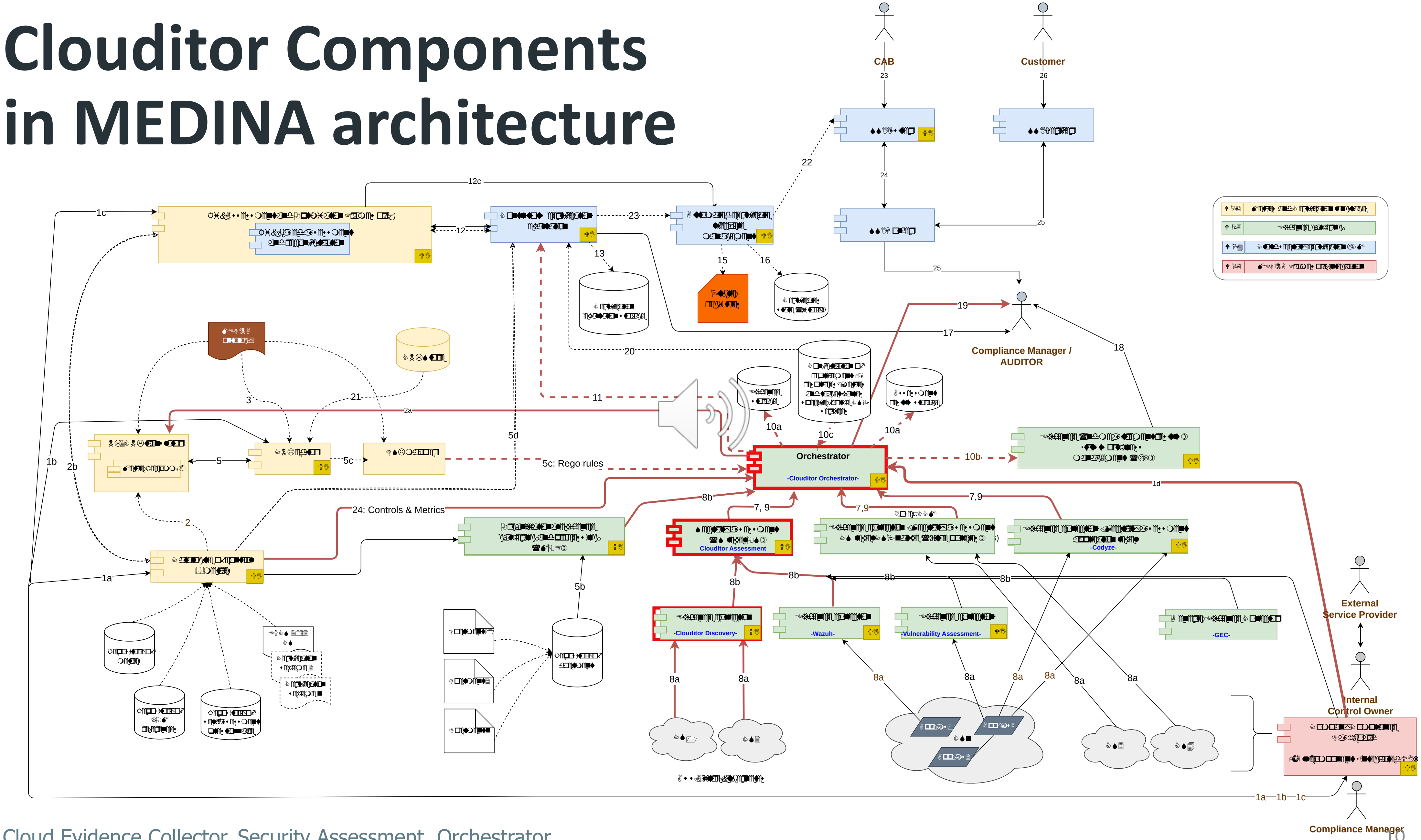
Security Assessment: Metrics

Control ID	Control	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type	Security Feature
OPS-18.6H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	AutomaticUpdatesEnabled	[true, false]	==	true	Boolean	VirtualMachine	automaticUpdates.enabled

Orchestrator

- The Orchestrator receives, forwards, and stores evidences and assessment results
- It offers many interfaces to other components, such as the Catalogue of Controls and Metrics and the Continuous Certification Evaluation (see next slide).
- The Orchestrator and the information it stores are accessible via the **Orchestrator UI**

Clouditor Components in MEDINA architecture



Cloud Evidence Collector, Security Assessment, Orchestrator

Interactions with other components

MEDINA

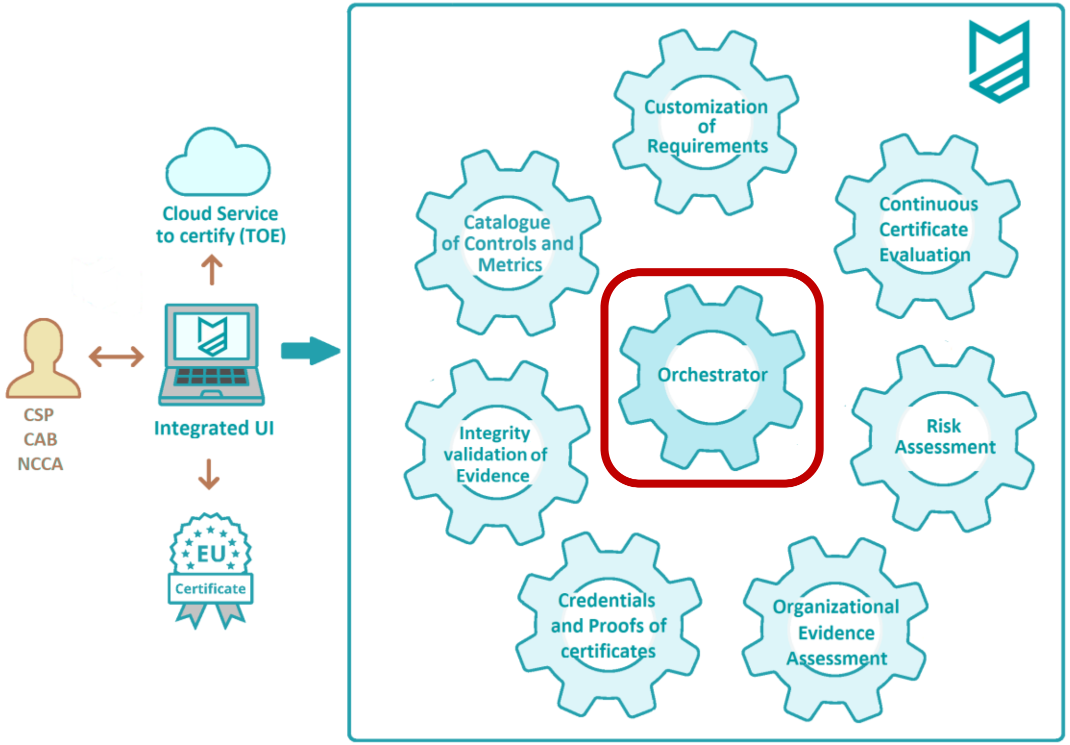
- Catalogue of Controls and Metrics
  - Retrieves catalog and metric information
- Continuous certification Evaluation (CCE)
  - Forwards ToEs and assessment results
- Risk Assessment and Optimisation Framework (RAOF)
  - Forwards ToEs and assessment results
- NL2CNL Translator
  - Forwards ToEs and assessment results
- DSL Mapper
  - Receives customized Rego code for the metrics
- Orchestrator
  - Retrieves the information about controls and metrics
- Assessment & Management of Organisational Evidence (AMOE)
  - Retrieves the information about controls and metrics
- User
  - Creates cloud services and Targets of Evaluation (ToEs)
  - Views evidences, assessment results, and other information

Clouditor Components
- Cloud Evidence Collector
- Security Assessment
- Orchestrator

➤ How to use them

- Functionalities
- Demo

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Evidence Collection

- Evidence Collection can be performed for Microsoft Azure and Amazon Web Services
- Evidences are enriched with ontological information (see D2.3 or our scientific publications https://dl.acm.org/doi/10.1145/3555776.3577600 and https://ieeexplore.ieee.org/abstract/document/9582243) to make them generically assessable

Security Assessment

MEDINA

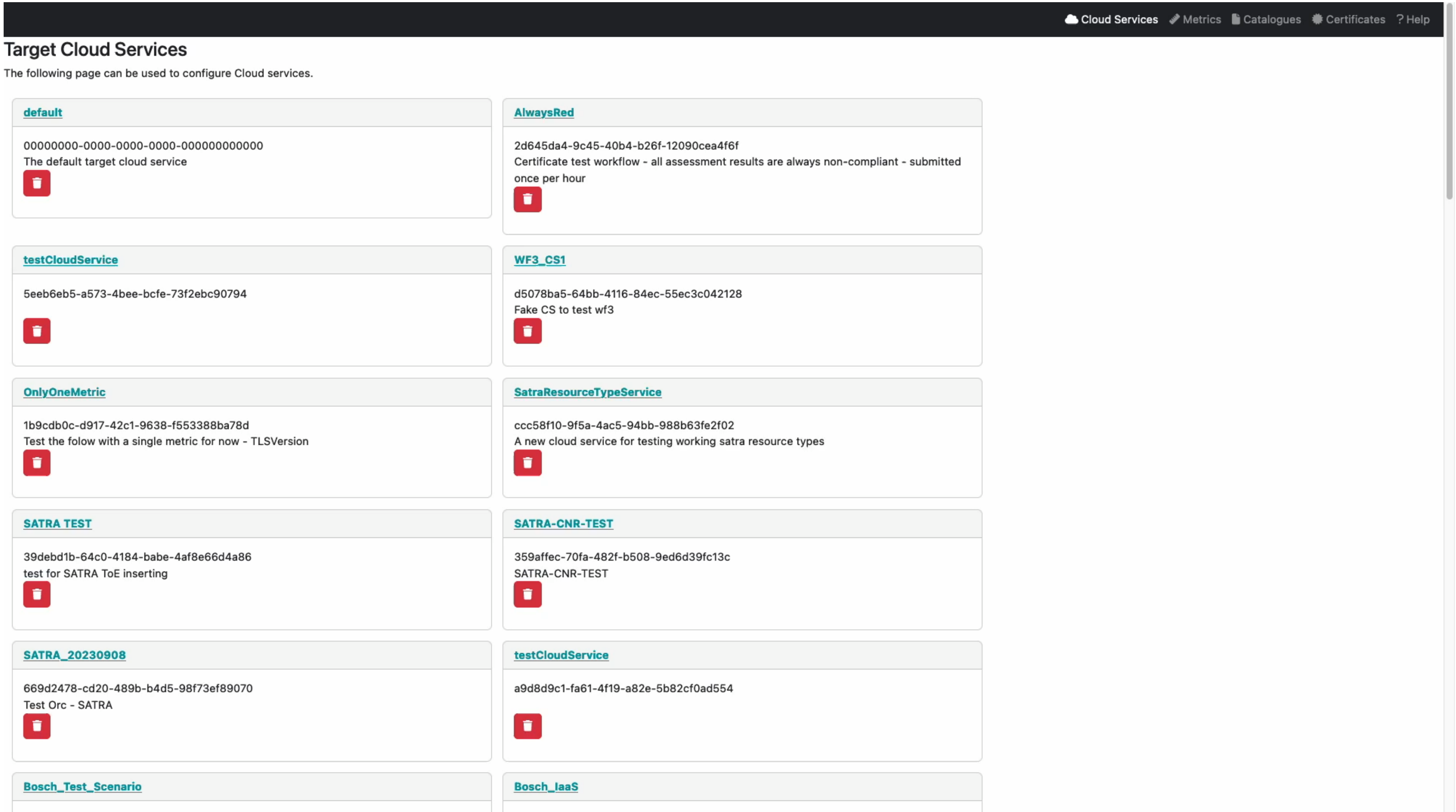
- The Security Assessment obtains metrics and their configurations (e.g., currently configured target values) from the Orchestrator
- Any metric that matches the ontological information in an evidence is applied to check if the resource conforms to the expected conformity state

Orchestration

MEDINA

- The Orchestrator allows users to manage many of the basic data objects in MEDINA: cloud services, targets of evaluation, evidences, assessment results, etc.
- It also manages many functionalities behind the scenes: forwarding assessment results between Security Assessment and Continuous Certification Evaluation, updating metric target values, etc.
- Its user interface allows users to interact with the Orchestrator

Orchestrator Demo



Target Cloud Services

The following page can be used to configure Cloud services.

default

00000000-0000-0000-0000-000000000000
The default target cloud service

AlwaysRed

2d645da4-9c45-40b4-b26f-12090cea4f6f
Certificate test workflow - all assessment results are always non-compliant - submitted once per hour

testCloudService

5eeb6eb5-a573-4bee-bcfe-73f2ebc90794

WF3_CS1

d5078ba5-64bb-4116-84ec-55ec3c042128
Fake CS to test wf3

OnlyOneMetric

1b9cdb0c-d917-42c1-9638-f553388ba78d
Test the folow with a single metric for now - TLSVersion

SatraResourceTypeService

ccc58f10-9f5a-4ac5-94bb-988b63fe2f02
A new cloud service for testing working satra resource types

SATRA TEST

39debd1b-64c0-4184-babe-4af8e66d4a86
test for SATRA ToE inserting

SATRA-CNR-TEST

359affec-70fa-482f-b508-9ed6d39fc13c
SATRA-CNR-TEST

SATRA_20230908

669d2478-cd20-489b-b4d5-98f73ef89070
Test Orc - SATRA

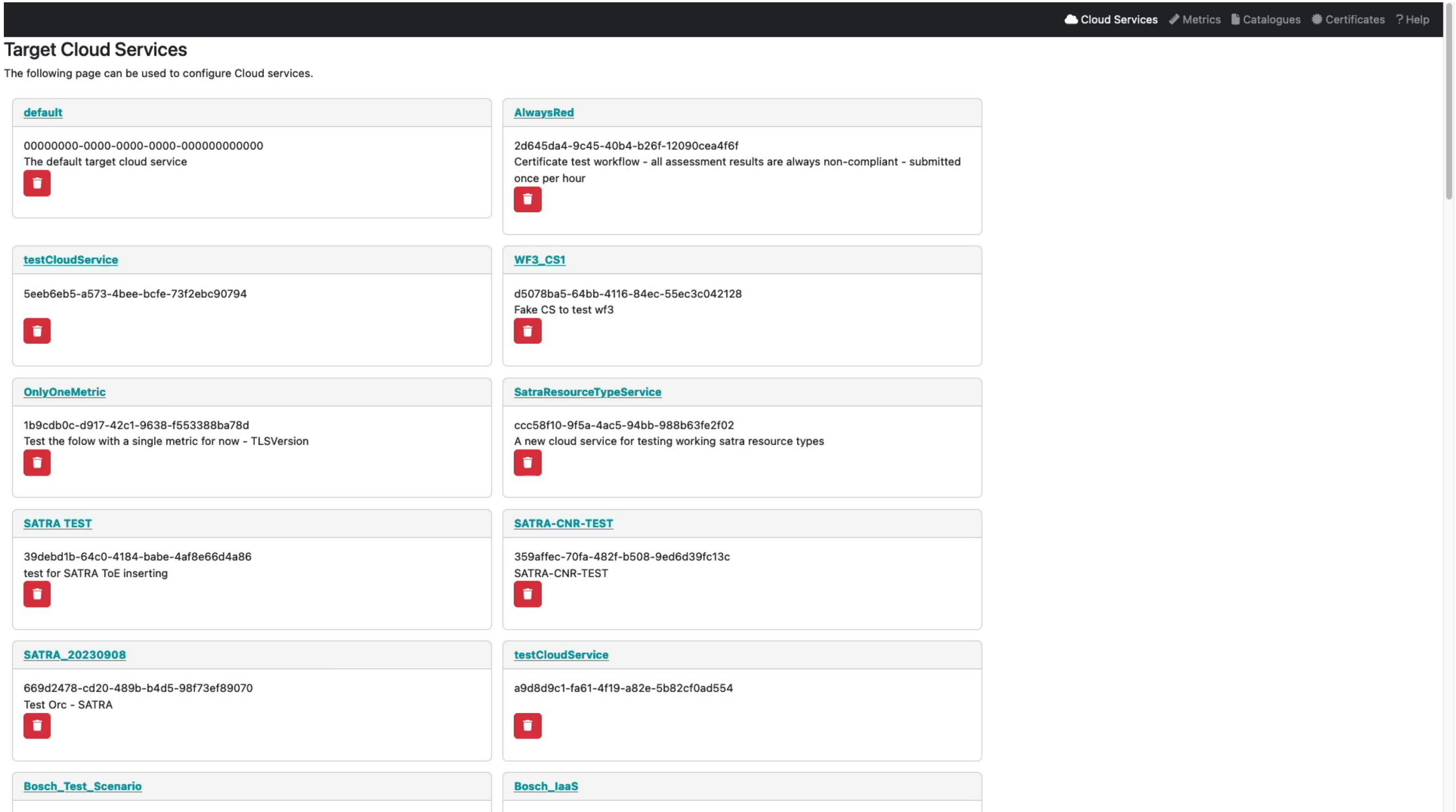
testCloudService

a9d8d9c1-fa61-4f19-a82e-5b82cf0ad554

Bosch_Test_Scenario

Bosch_IaaS

Orchestrator Demo



Target Cloud Services

The following page can be used to configure Cloud services.

default
00000000-0000-0000-0000-000000000000
The default target cloud service

AlwaysRed
2d645da4-9c45-40b4-b26f-12090cea4f6f
Certificate test workflow - all assessment results are always non-compliant - submitted once per hour

testCloudService
5eeb6eb5-a573-4bee-bcfe-73f2ebc90794

WF3_CS1
d5078ba5-64bb-4116-84ec-55ec3c042128
Fake CS to test wf3

OnlyOneMetric
1b9cdb0c-d917-42c1-9638-f553388ba78d
Test the folow with a single metric for now - TLSVersion

SatraResourceTypeService
ccc58f10-9f5a-4ac5-94bb-988b63fe2f02
A new cloud service for testing working satra resource types

SATRA TEST
39debd1b-64c0-4184-babe-4af8e66d4a86
test for SATRA ToE inserting

SATRA-CNR-TEST
359affec-70fa-482f-b508-9ed6d39fc13c
SATRA-CNR-TEST

SATRA_20230908
669d2478-cd20-489b-b4d5-98f73ef89070
Test Orc - SATRA

testCloudService
a9d8d9c1-fa61-4f19-a82e-5b82cf0ad554

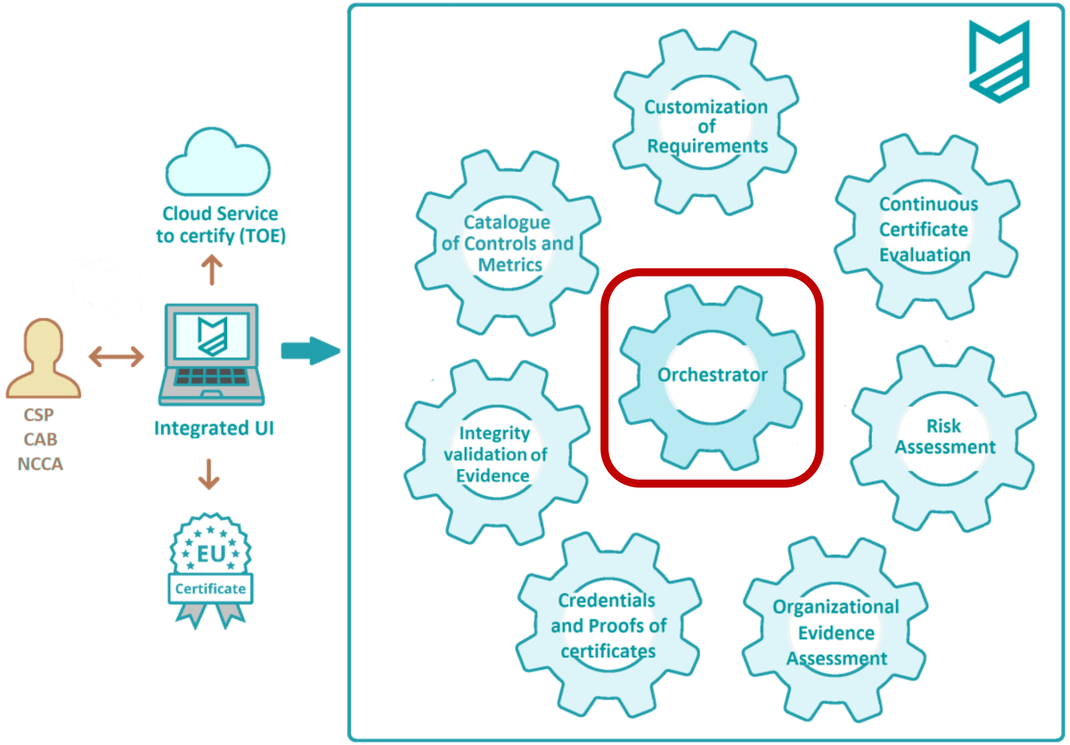
Bosch_Test_Scenario

Bosch_IaaS

Clouditor Components
- Cloud Evidence Collector
- Security Assessment
- Orchestrator

- Installation
  - Deployment
  - Technical Specifications

MEDINA

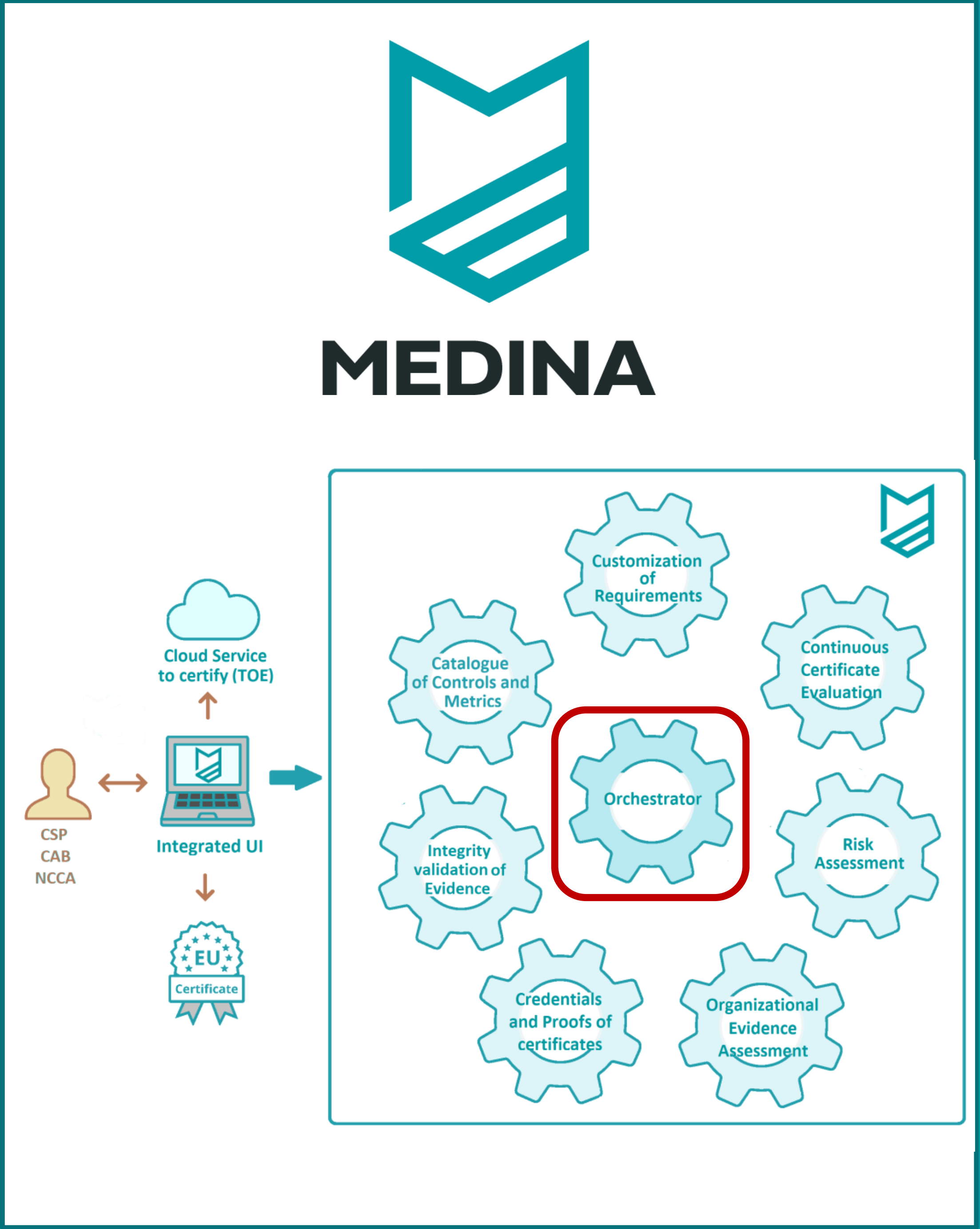

Cloud Service
to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

- Installation and Deployment
  - go generate ./...
  - go build -o ./engine cmd/engine/engine.go
  - Configure Cloud Service ID and possibly the resource group
  - See also the README at https://github.com/clouditor/clouditor/
- Technical specifications
  - Go
  - PostgreSQL or in-memory DB

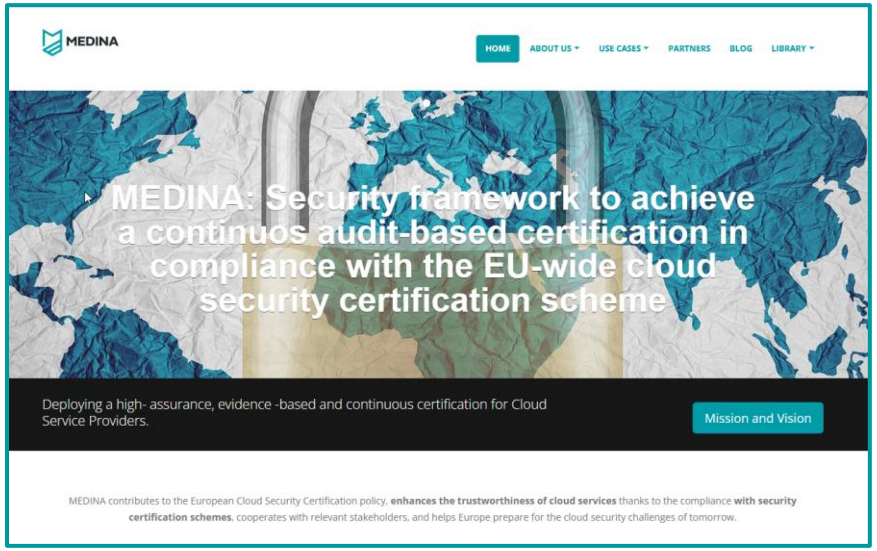
Clouditor Components
- Cloud Evidence Collector
- Security Assessment
- Orchestrator

➤ Further information


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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

MEDINA

Assessment and Management of Organisational Evidence (AMOE)

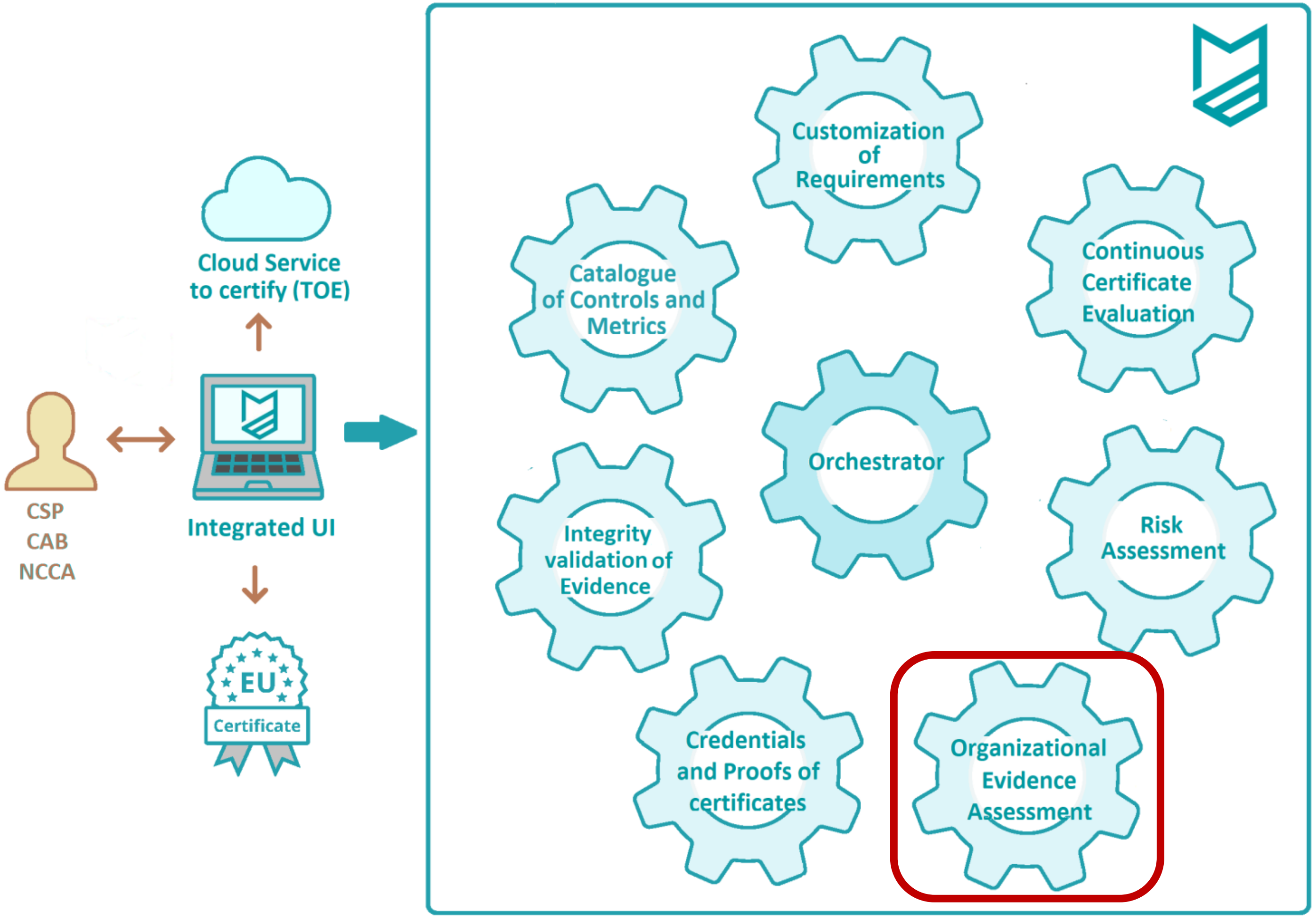
Franz Deimling, Fabasoft

September 2023

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

Chapters

- Overview
- How to use it
- Installation
- Further information

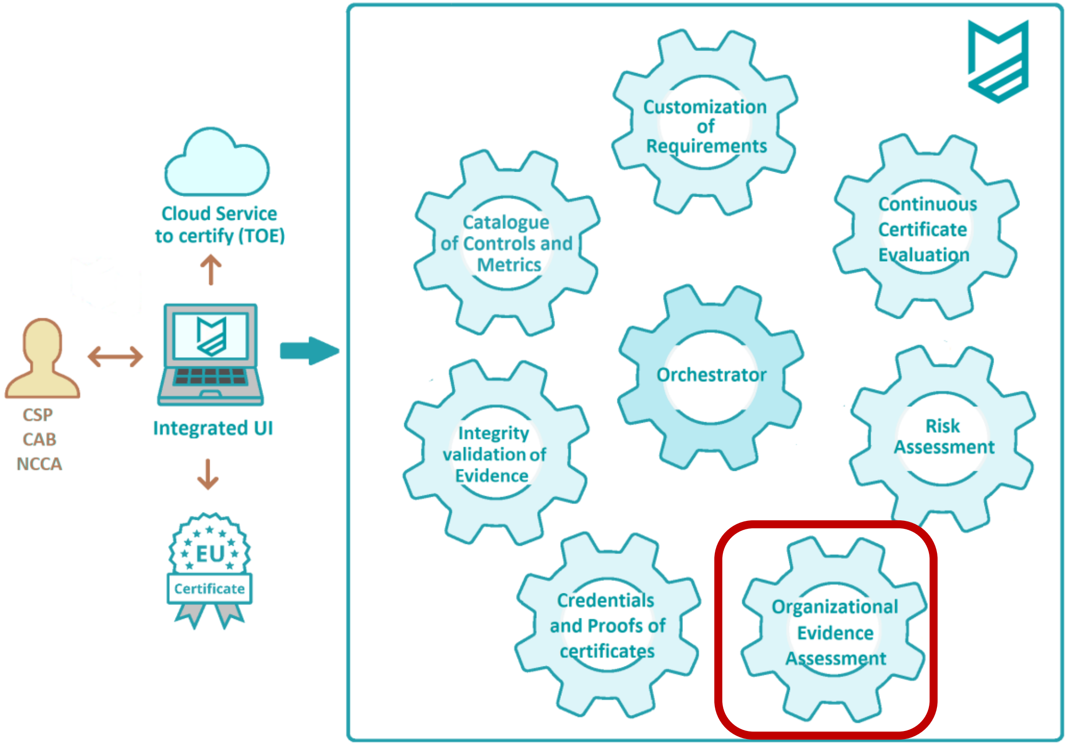


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Assessment and Management of Organisational Evidence (AMOE)

- Overview
  - - Purpose
  - - Role in MEDINA Architecture

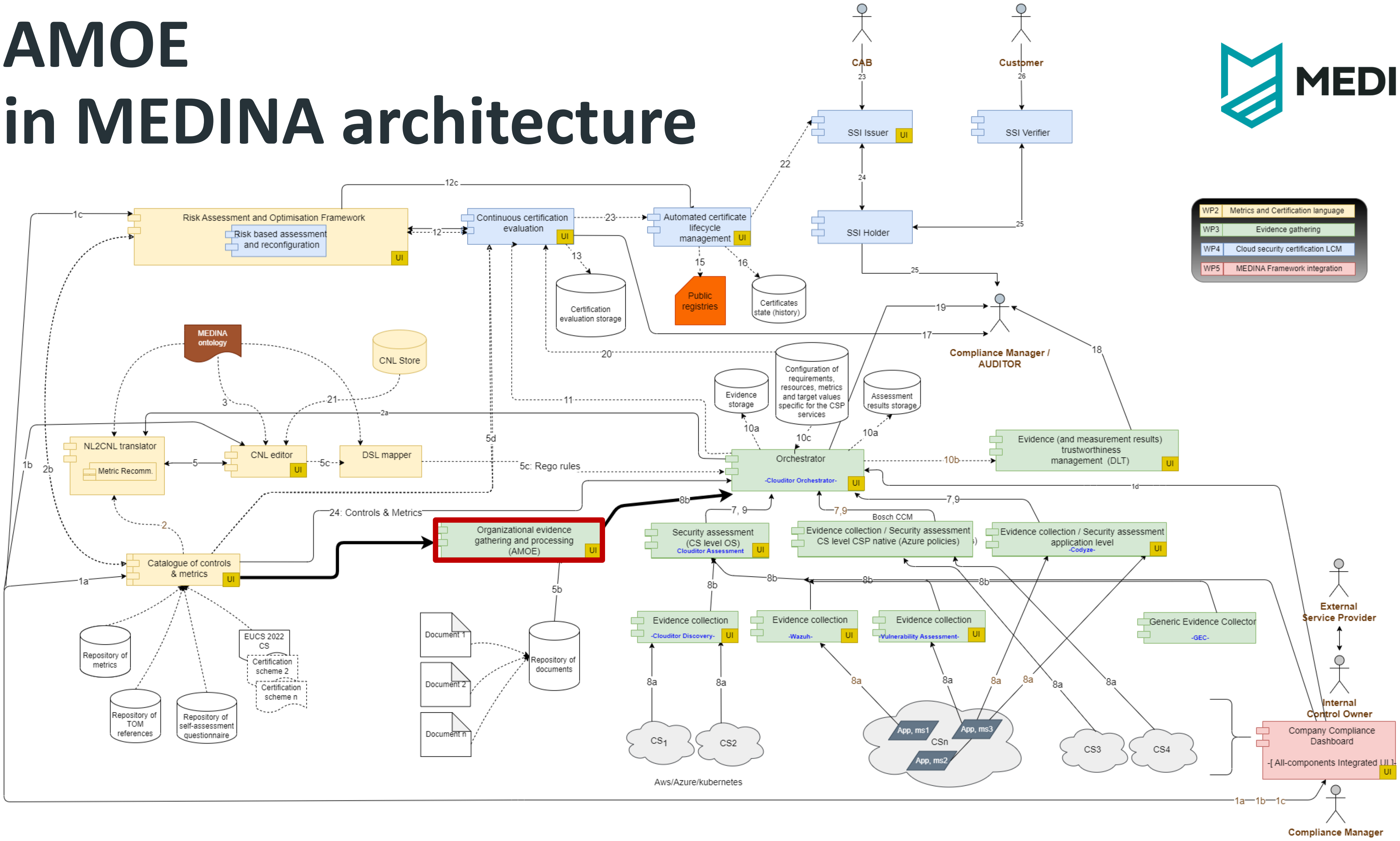
MEDINA


Cloud Service
to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Assessment and Management of Organisational Evidence (AMOE)

- AMOE is an evidence gathering tool and assessment tool for policy documents
- Offers an **API** to the rest of MEDINA components to get the information
- Has a navigable **user interface** that allows the user to view and check the extracted evidence
- Data is loaded on demand (EUCS, Metrics,...)

AMOE
in MEDINA architecture



CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
24
SSI Holder
25
22
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
MEDINA ontology
CNL Store
3
21
20
11
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
1a
Catalogue of controls & metrics
UI
5b
8b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
Internal Control Owner
Repository of TOM references
Repository of self-assessment questionnaire
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated]-
UI
1a—1b—1c
Compliance Manager

Interactions with other components

Catalogue of Controls and Metrics

- AMOE retrieves the information about controls/requirements and metrics

Orchestrator

- AMOE retrieves the information about metrics (custom target values)
- AMOE sends evidence and assessment results

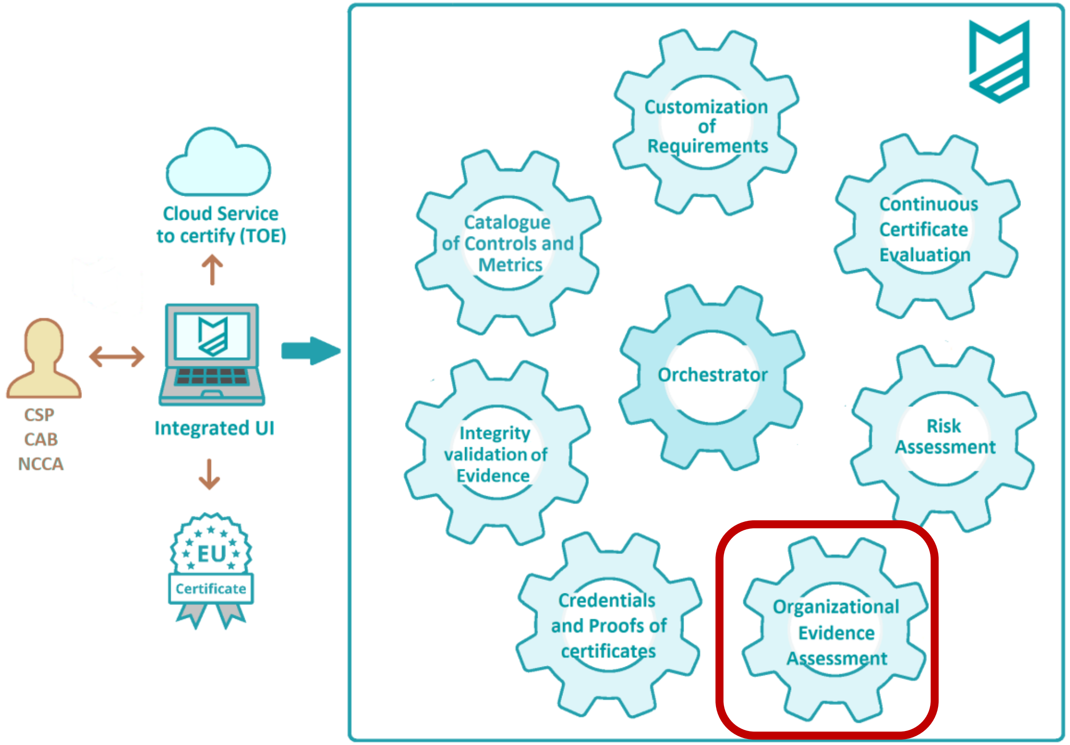
User

- Uploads policy document
- Views pre-assessments and extracted evidence
- Sets assessment status and submits assessment results

Assessment and Management of Organisational Evidence (AMOE)

- ➤ How to use it
  - - Functionalities
  - - Demo

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA metrics

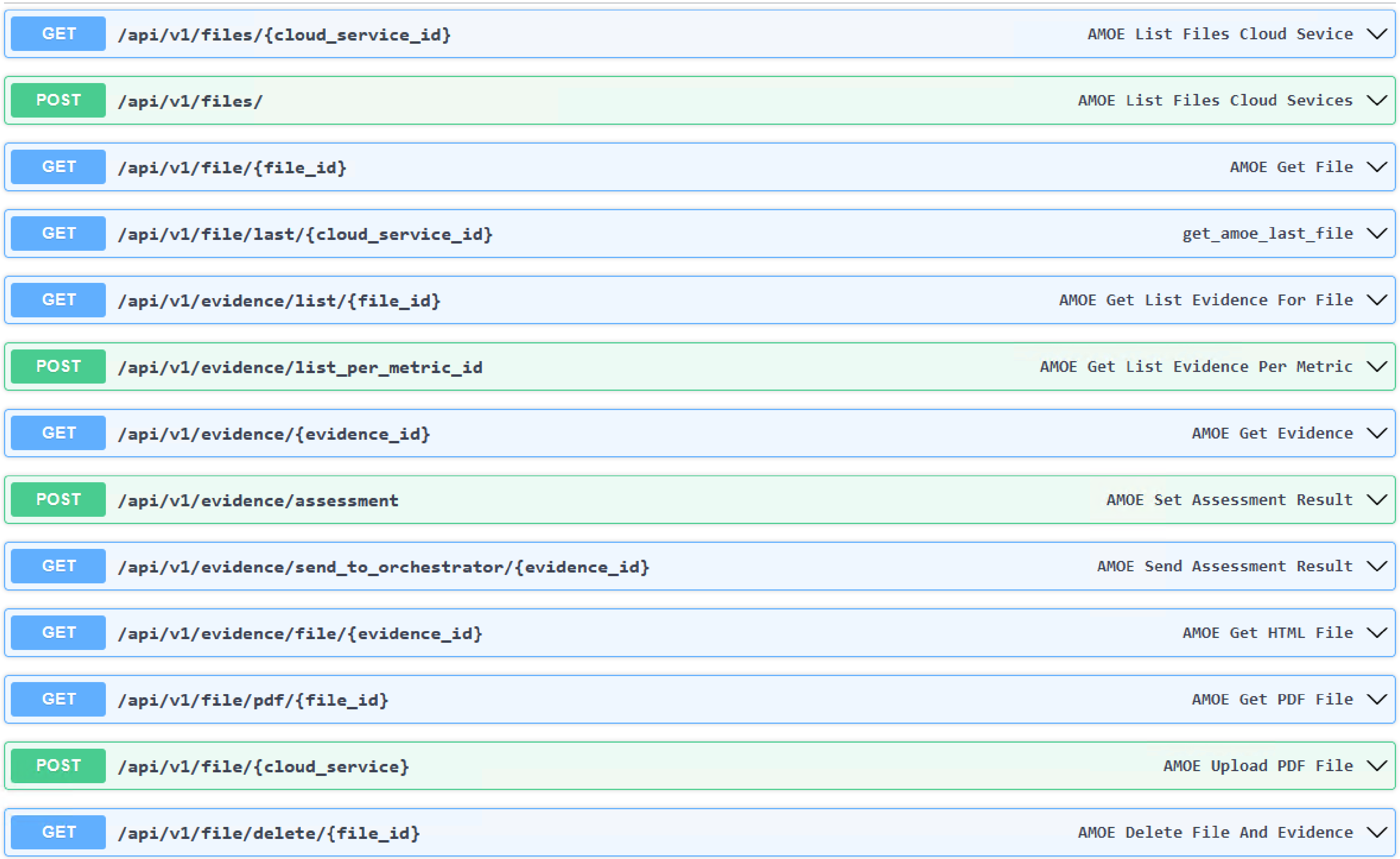
Metric Name	Control	Description	Keywords	Type	Operator	Target Value	Target Resource Type
MalwareProtectionEnabled	OPS-05.3H	This metric is used to assess if the antimalware solution is enabled on the respective resource.	-	Technical	==	true	VirtualMachine
PasswordPolicyQ2	IAM-08.1H	What is the passwords maximum age according to the password policy?	password, age, maximum	Organizational	<=	90	Policy Document

- AMOE uses organizational metrics
- Operator and Target Value are used for pre-assessment
- The description/question and keywords are used for evidence extraction

Evidence extraction steps

- Transformation of the policy PDF to HTML
- Pre-processing of metrics and policy text
- AMOE uses a pre-trained question answering system to extract evidence
- AMOE processes all available organizational metrics

API



GET	/api/v1/files/{cloud_service_id}	AMOE List Files Cloud Sevice
POST	/api/v1/files/	AMOE List Files Cloud Sevices
GET	/api/v1/file/{file_id}	AMOE Get File
GET	/api/v1/file/last/{cloud_service_id}	get_amoe_last_file
GET	/api/v1/evidence/list/{file_id}	AMOE Get List Evidence For File
POST	/api/v1/evidence/list_per_metric_id	AMOE Get List Evidence Per Metric
GET	/api/v1/evidence/{evidence_id}	AMOE Get Evidence
POST	/api/v1/evidence/assessment	AMOE Set Assessment Result
GET	/api/v1/evidence/send_to_orchestrator/{evidence_id}	AMOE Send Assessment Result
GET	/api/v1/evidence/file/{evidence_id}	AMOE Get HTML File
GET	/api/v1/file/pdf/{file_id}	AMOE Get PDF File
POST	/api/v1/file/{cloud_service}	AMOE Upload PDF File
GET	/api/v1/file/delete/{file_id}	AMOE Delete File And Evidence

Assessment and Management of Organisational Evidence (AMOE)

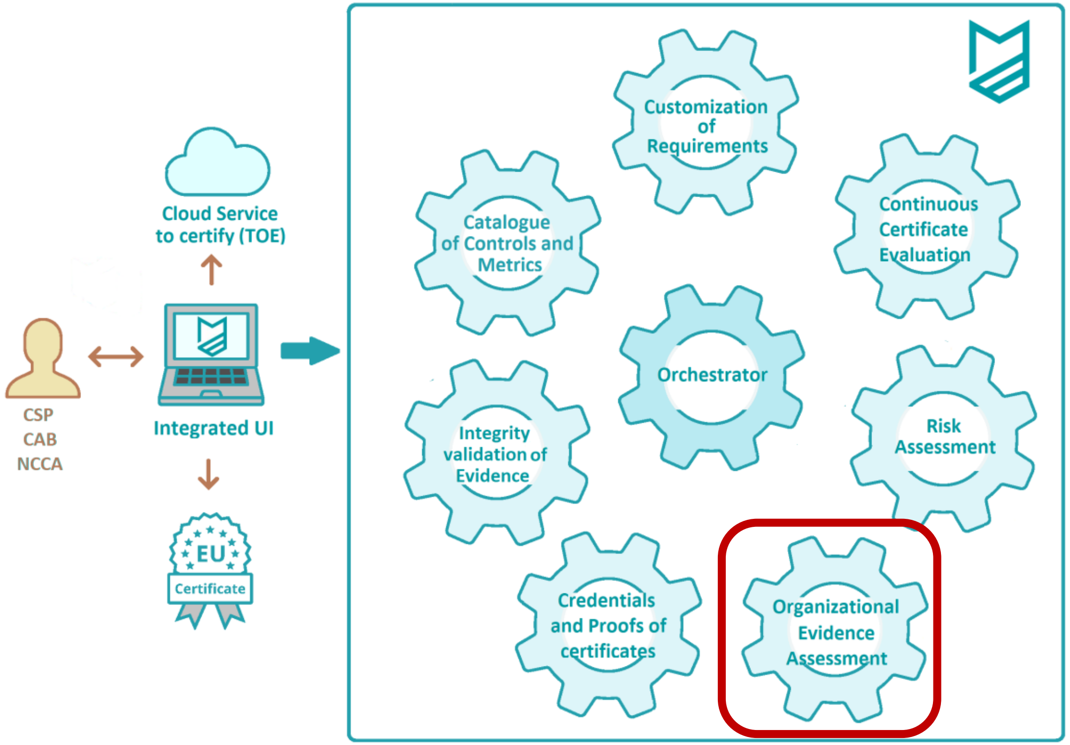
MEDINA

- DEMO -

Assessment and Management of Organisational Evidence (AMOE)

- Installation
  - Deployment
  - Technical Specifications

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

MEDINA

- Install for local deployment
  - Clone the repository:

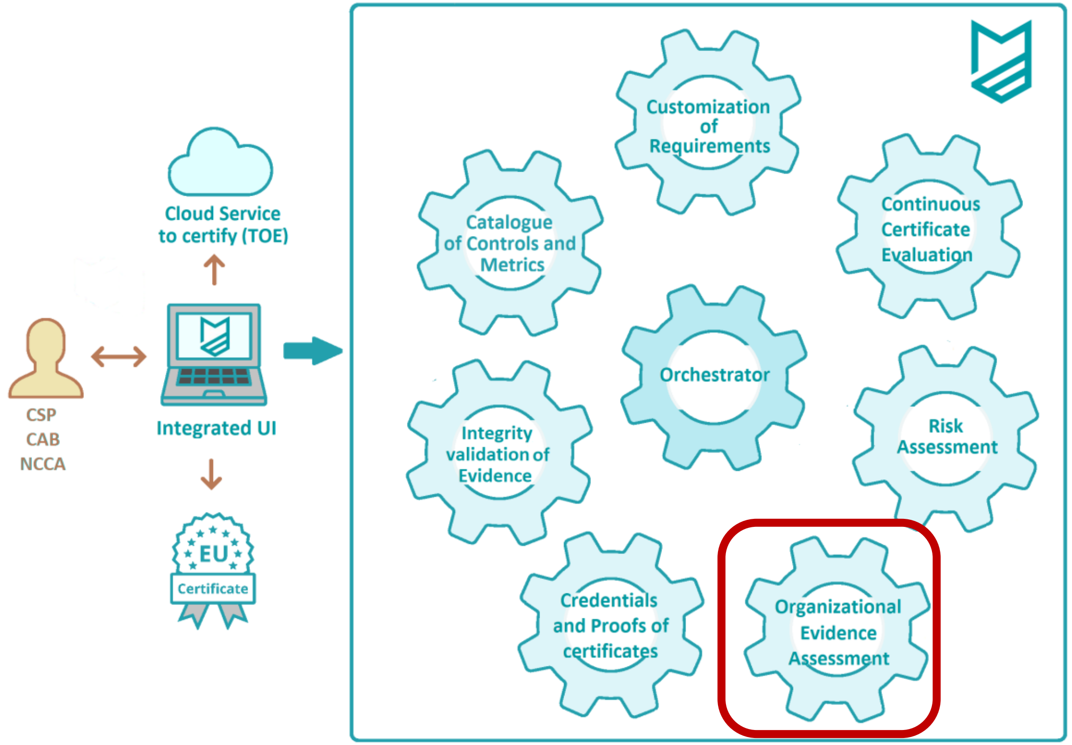
    git clone https://git.code.tecnalia.com/medina/public/amoe
  - Deploy and start Redis and MongoDB (e.g. docker container)
  - Configure DB + Keycloak + other MEDINA components in config.py
  - Build and run docker container or run ‘python app.py’

- Technical specifications
  - Python/Quart based architecture
  - Redis for session management, MongoDB for application data
  - Docker/Kubernetes for installation

Assessment and Management of Organisational Evidence (AMOE)

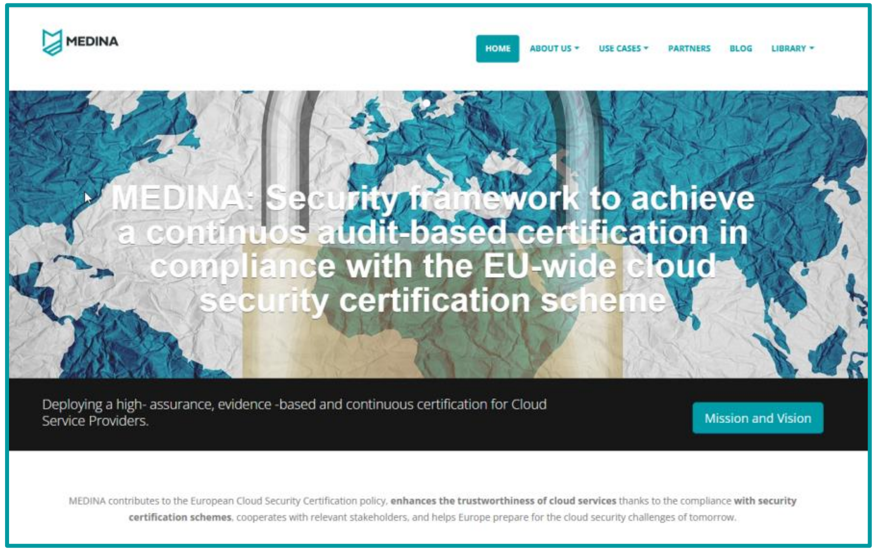
- Further information

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** *https://medina-project.eu/public-deliverables*
- Framework demonstrator is available in the MEDINA **YouTube channel** *https://www.youtube.com/@MedinaprojectEU*
- MEDINA Community in **Zenodo** *https://zenodo.org/communities/medina*
- Source code in the public **GitLab** *https://git.code.tecnalia.com/medina/public*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

🌐 www.medina-project.eu

@MedinaprojectEU

in MEDINA Project - Continuous cloud security certification

▶ @MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer
AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

NIXU cybersecurity.

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

MEDINA

Codyze

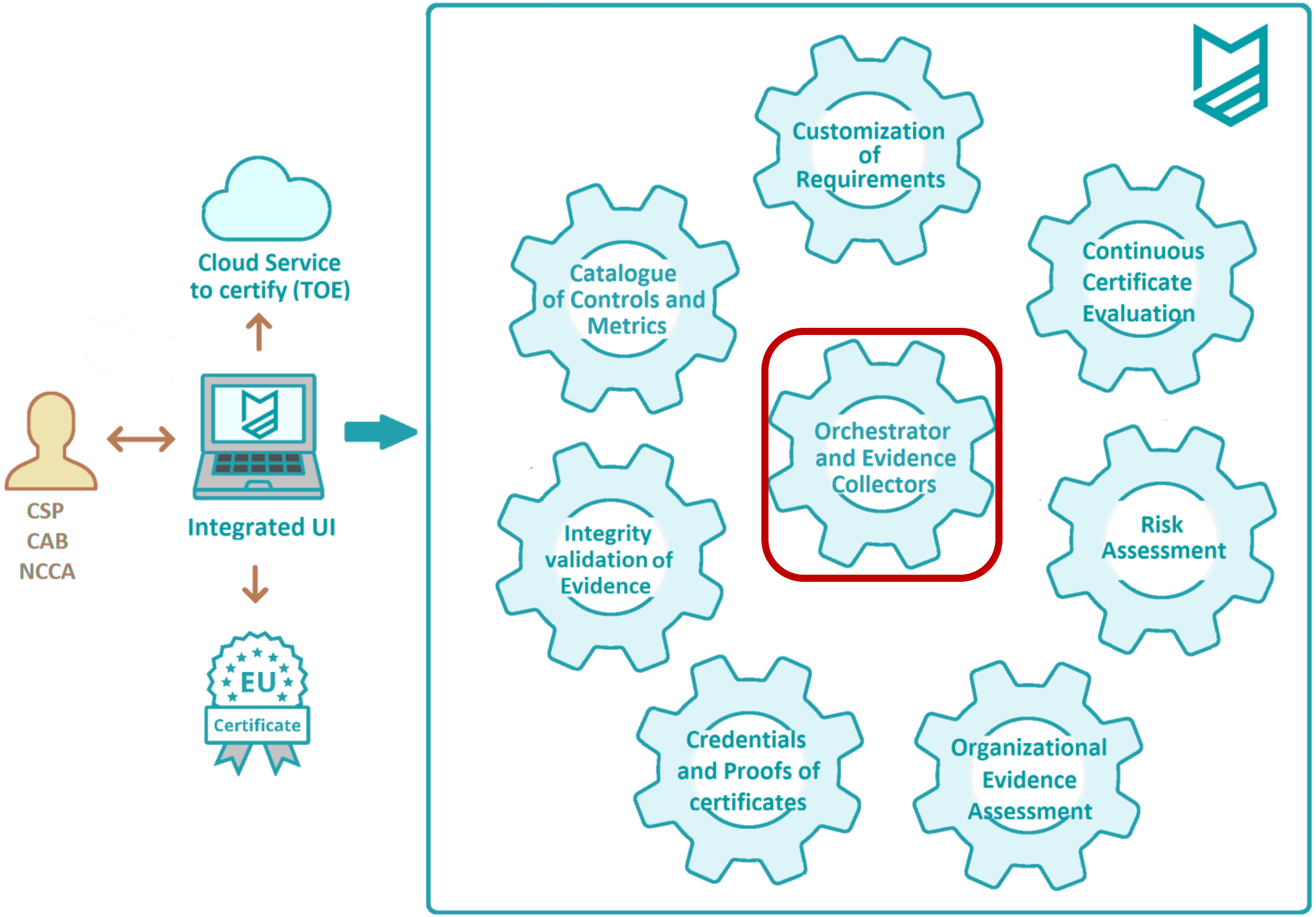
Florian Wendland, Fraunhofer AISEC

October 2023

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

Chapters

- Overview
- How to use it
- Installation
- Further information

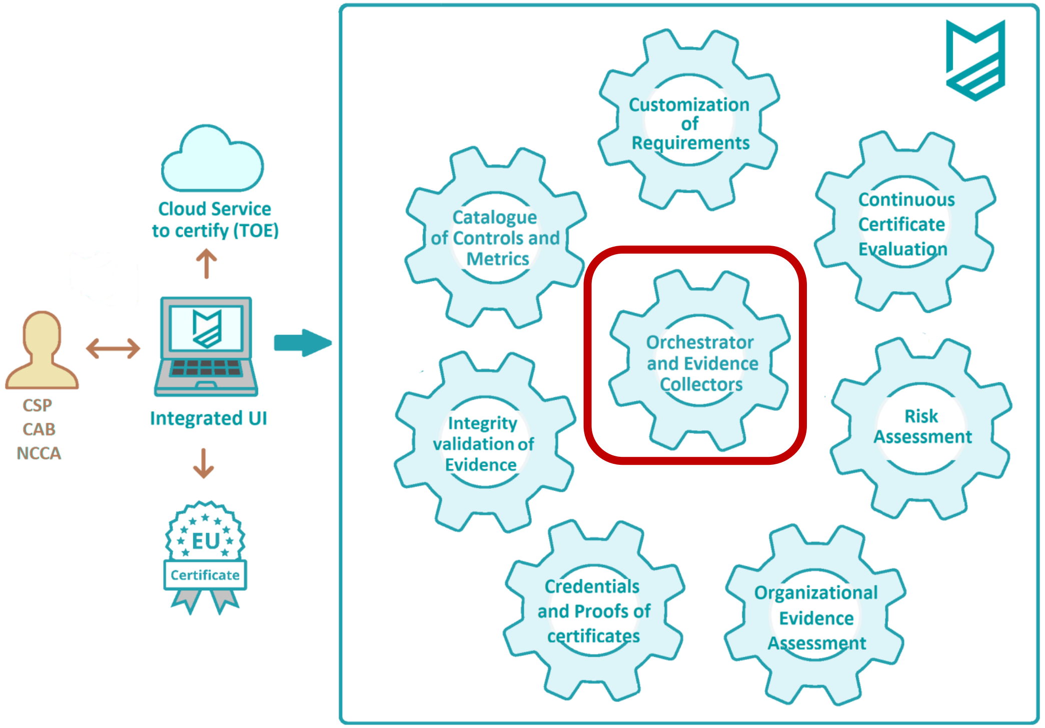


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Codyze

- Overview
  - Purpose
  - Role in MEDINA Architecture

MEDINA

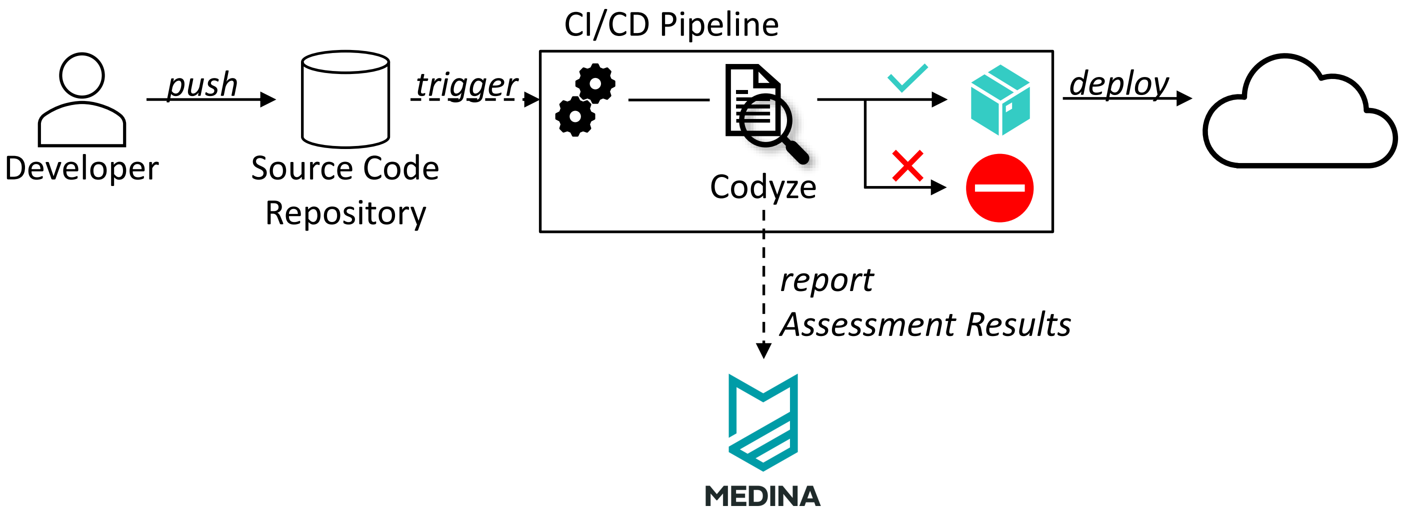

CSP
CAB
NCCA
Cloud Service to certify (TOE)
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Codyze

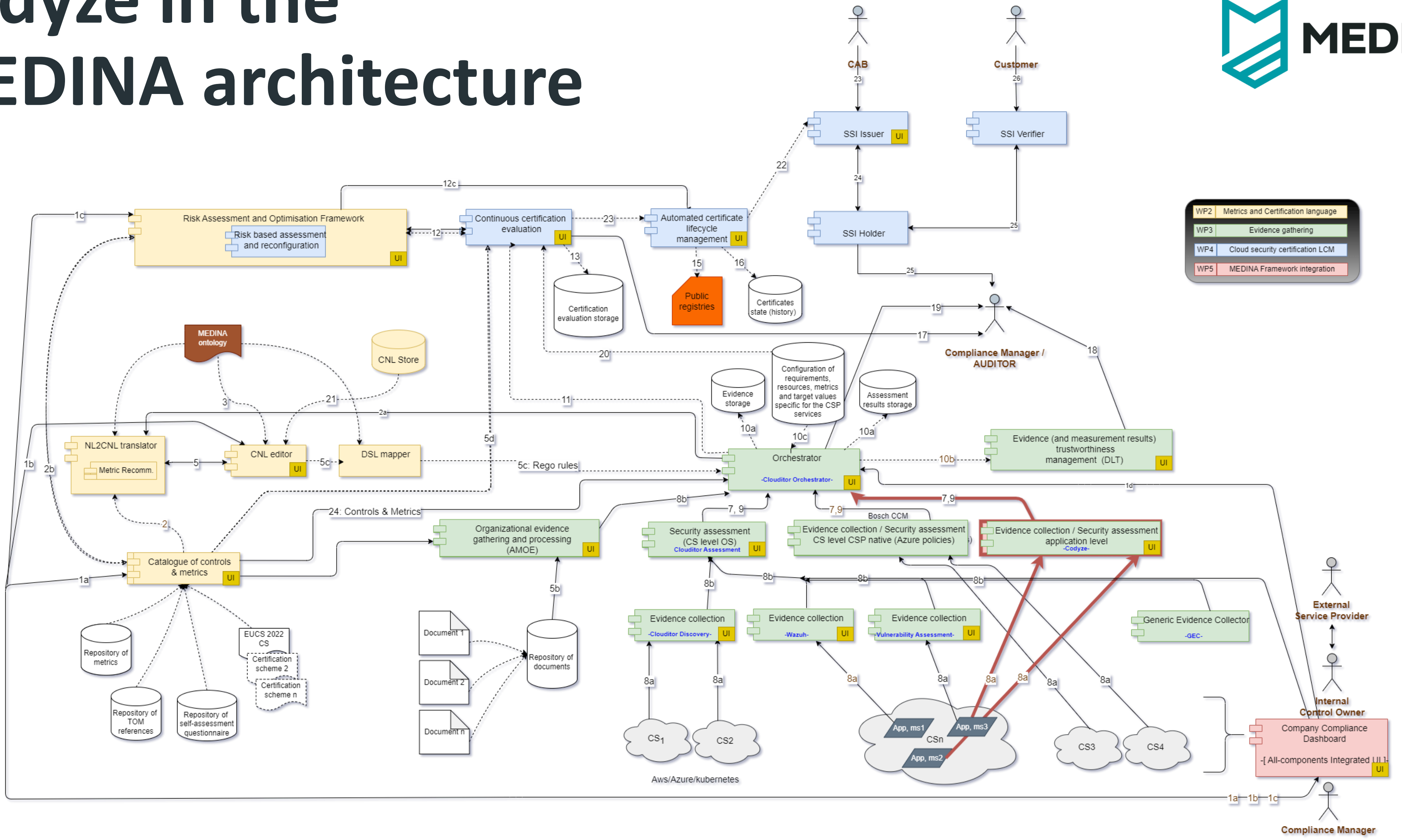
- Compliance assessment tool during software development
- Identifies non-compliant features in source code and source code repositories
- Enforces
  - Proper uses of TLS and data encryption in source code
  - Provenance on submissions to source code repository
- Contribute to more secure development processes
  - Highlight insecure implementations early during development
  - Provide mitigations to developers
  - Prevent deployment of non-compliant software products

Codyze

- CI/CD integration
  - Compliance assurance gate



Codyze in the MEDINA architecture


CAB
23
Customer
26
SSI Issuer
UI
SSI Verifier
24
SSI Holder
25
22
12c
1c
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
12
Continuous certification evaluation
UI
23
Automated certificate lifecycle management
UI
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
Compliance Manager / AUDITOR
18
20
MEDINA ontology
CNL Store
3
21
11
2a
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
1b
2b
NL2CNL translator
Metric Recomm.
5
CNL editor
UI
5c
DSL mapper
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
UI
10b
Evidence (and measurement results) trustworthiness management (DLT)
UI
1d
2
24: Controls & Metrics
8b
7, 9
7,9
Bosch CCM
7,9
Organizational evidence gathering and processing (AMOE)
UI
Security assessment (CS level OS)
Clouditor Assessment
UI
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
UI
Catalogue of controls & metrics
UI
1a
5b
8b
8b
8b
8b
Evidence collection
-Clouditor Discovery-
UI
Evidence collection
-Wazuh-
UI
Evidence collection
-Vulnerability Assessment-
UI
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
8a
8a
8a
8a
8a
8a
8a
8a
CS1
CS2
App, ms1
App, ms3
App, ms2
CSn
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
UI
1a
1b
1c
Compliance Manager

WP2	Metrics and Certification language
WP3	Evidence gathering
WP4	Cloud security certification LCM
WP5	MEDINA Framework integration

Interactions with other components

Orchestrator

- Sends assessment results regarding analyzed software

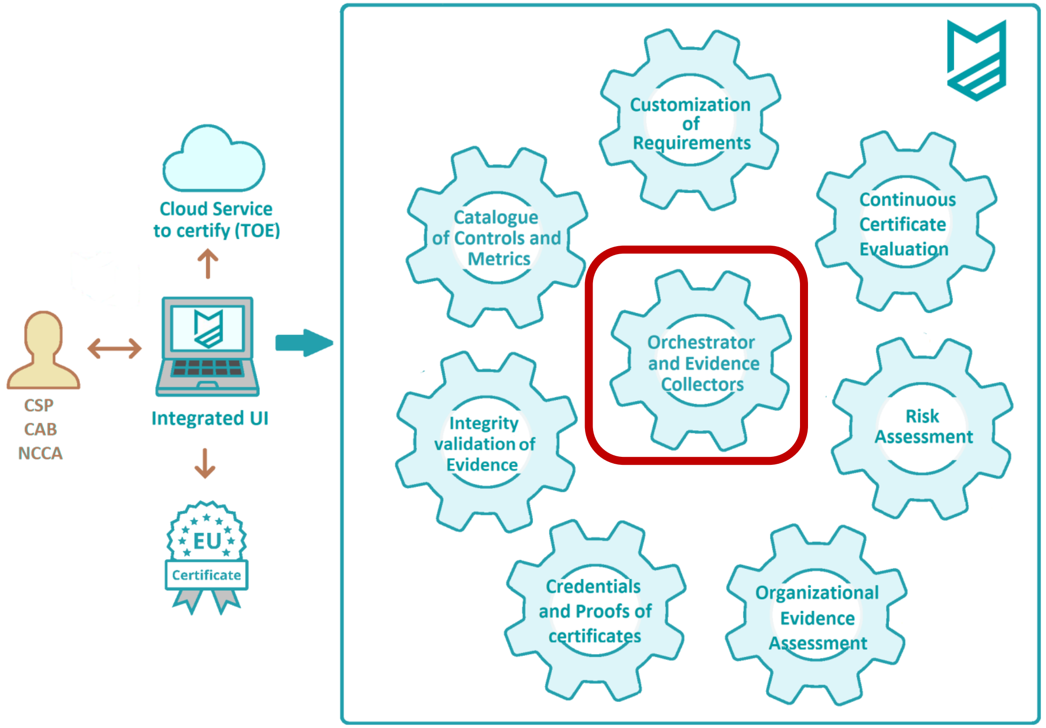
CI/CD pipeline for cloud services

- Scans new code submissions and assess compliance automatically

Codyze

- How to use it
  - Functionalities
  - Demo

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Codyze Functionalities

- Static analysis of source code (C, C++ and Java)
- Behavior of APIs bound to calls of functions and arguments
  - Verify function calls with secure argument values
  - Verify proper order of function calls
- Specifies correct usage of APIs using DSL (*MARK*)
  - *Entities* define functions and parameters
  - *Rules* enforce argument values and call order

Codyze Functionalities

DSL example

SSLServerSocket.mark

```
entity SSLServerSocket {
    var protocols;

    op enabledProtocols {
        javax.net.ssl.SSLServerSocket.setEnabledProtocols(
            protocols : java.lang.String[]
        );
    }

    ...
}
```

rules.mark

```
rule TlsVersion {
    using
        SSLServerSocket as socket
    ensure
        _subset(socket.protocols, ["TLSv1.2", "TLSv1.3"])
    fail
}
```

Codyze Functionalities

Human-readable messages

findingDescription.json

```
{
  "TlsVersion": {
    "fullDescription": {
      "text": "TLS version isn't sufficiently restricted and may allow the use of deprecated version. Ensure the use of TLS versions 1.2 or 1.3."
    },
    "shortDescription": {
      "text": "Insufficient restriction of TLS to version 1.2 or 1.3."
    },
    "fixes": [
      {
        "description": {
          "text": "Use TLS version 1.2 or 1.3."
        }
      }
    ]
  },
  ...
}
```

Codyze Functionalities

MEDINA

- Mapping of findings to MEDINA metrics

mapping.yaml

```
metrics:
  - name: "TLSVersion"
    rules:
      - "TlsVersion"
    configuration:
        default: true
        operator: ">"
        type: STRING
        target:
          - "1.2"
```

Codyze Functionalities

- Rule sets
  - Directory based
  - Content
    - Definitions for entities and rules in its DSL as **.mark* files
    - Human-readable messages through *findingDescription.json*
    - Mapping to MEDINA metrics through *mapping.yaml*
  - Pre-defined sets
    - TLS with Java JSSE
    - Encryption with Java JCA/JCE
  - Custom additions possible

Codyze Functionalities

Provenance of code submissions

- Validate submissions against authorized developers
- Checks commit messages for sign offs and signed commits

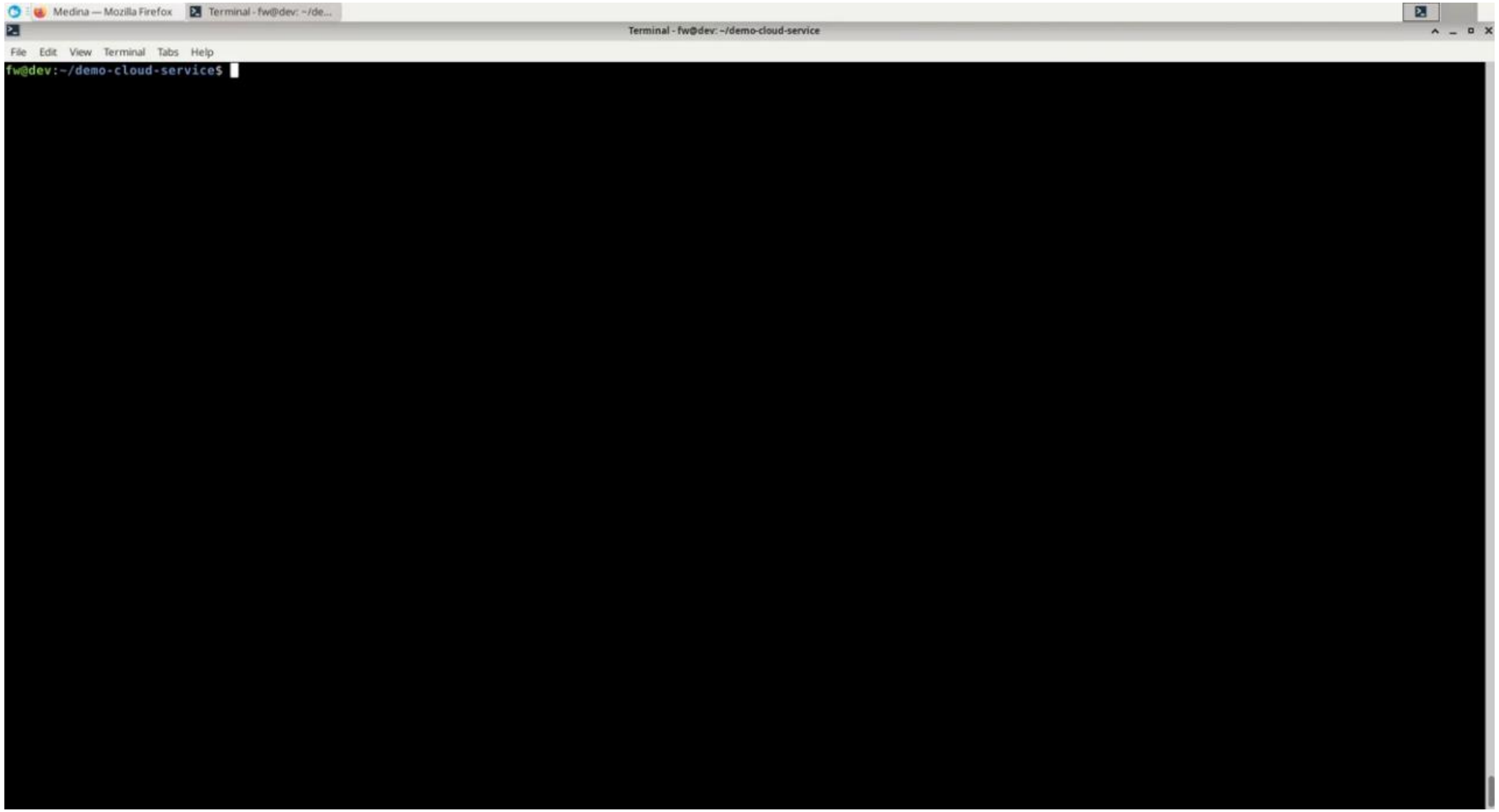
codyze-medina-metrics.yaml

```
metrics:
  - name: "CodeSignoff"
    target:
      - "<Name>"
      - "<Name>"
  - name: "SignedCommits"
    target:
      - "<16-Digit Key-Id>„
  - name: "SignedSignoff"
    target:
      - name: "<Name>"
        email: "<E-Mail>"
        pub-key-id: "<16-Digit Base-64 Signing-Key-Id>"
   - name: "ApprovedCommitAuthor"
    target:
      - "<Name>"
```

Codyze Functionalities

- Reports
  - SARIF output for integration into development platform
  - Assessment results submitted to Orchestrator

Codyze Demo

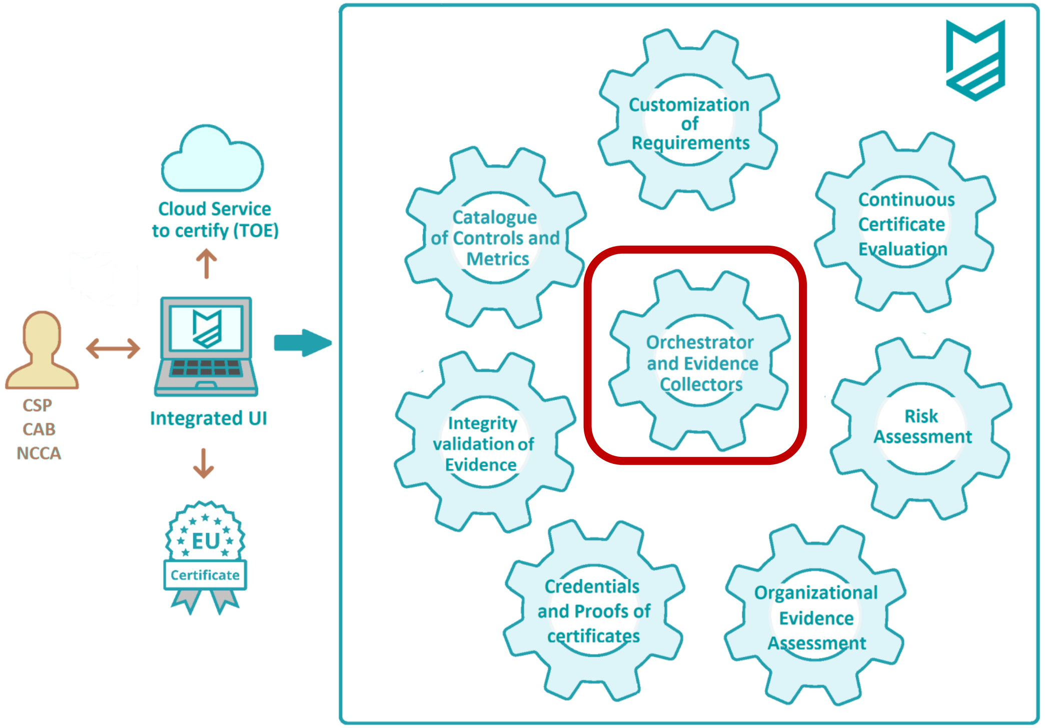

Medina — Mozilla Firefox
Terminal - fw@dev: ~/de...
Terminal - fw@dev: ~/demo-cloud-service
File
Edit
View
Terminal
Tabs
Help

```
fw@dev:~/demo-cloud-service$ 
```

Codyze

- Installation
  - Deployment
  - Technical Specifications

MEDINA



CSP
CAB
NCCA
Cloud Service to certify (TOE)
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Installation

- Get distribution
  - Archive with prebuilt binaries for Java VM
  - Container image file
  - Build either from source using Gradle wrapper
- Integration
  - Add step for Codyze into CI/CD pipeline
  - Configure source code project using templates
    - *codyze-medina.yaml*
    - *codyze-medina-metrics.yaml*
  - Possible integration of SARIF report

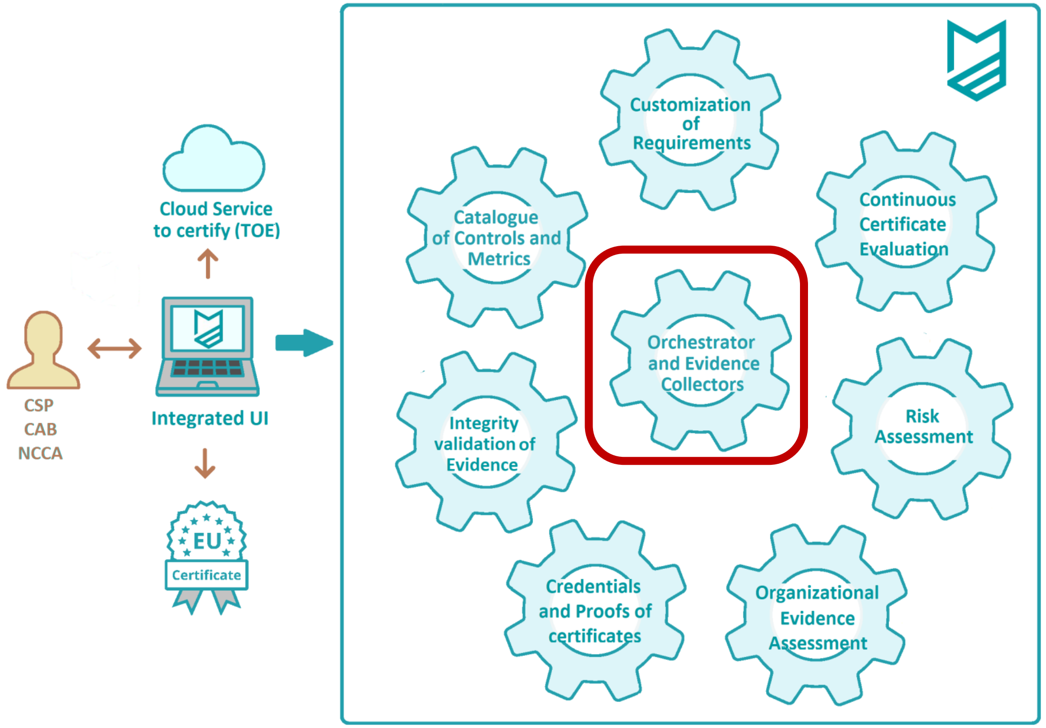
Technical Specification

- Kotlin
- Gradle build system
- DSL in Eclipse Xtext
- Predefined rulesets in DSL

Codyze

- Further information

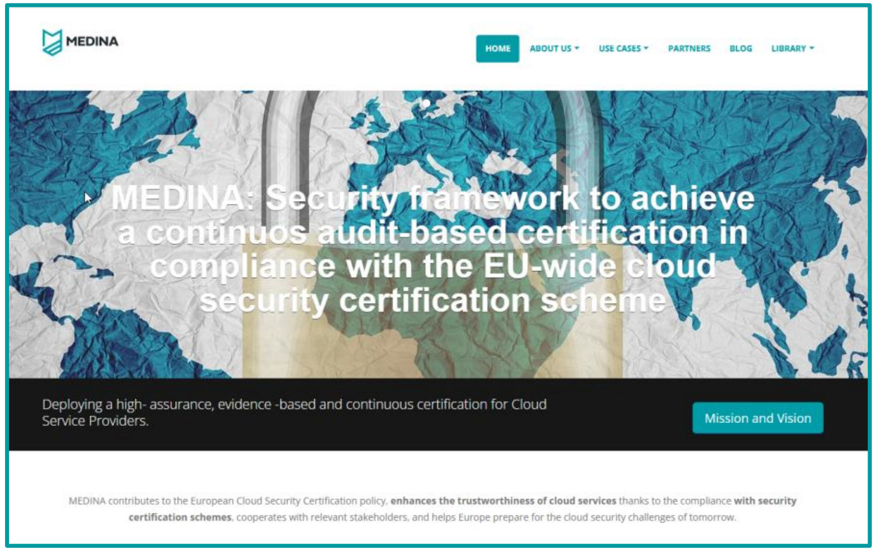
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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

MEDINA

Wazuh and VAT Evidence Collection

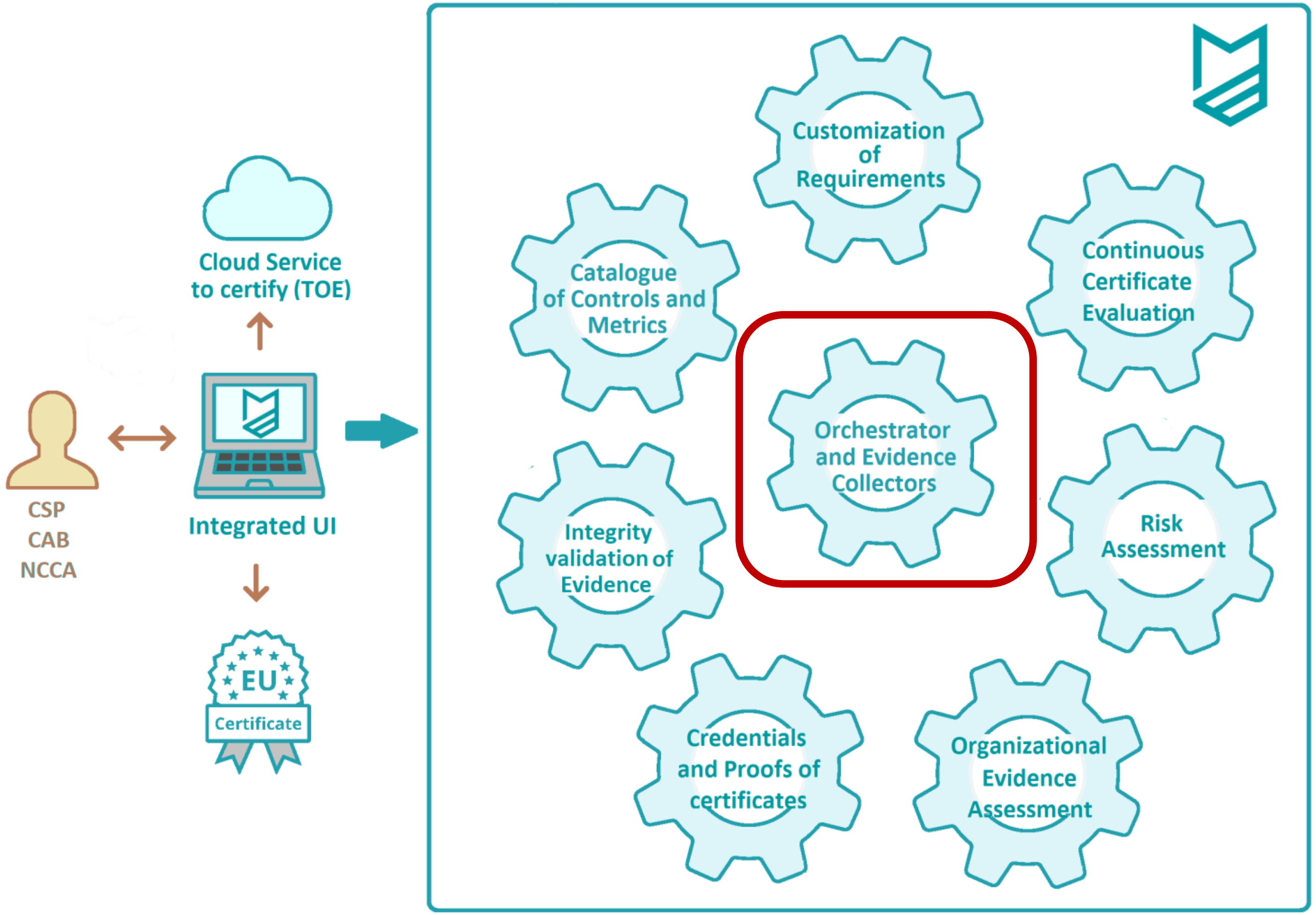
Hrvoje Ratkajec (PhD), XLAB

September 2023

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

Chapters

- Overview
- How to use it
- Installation
- Further information

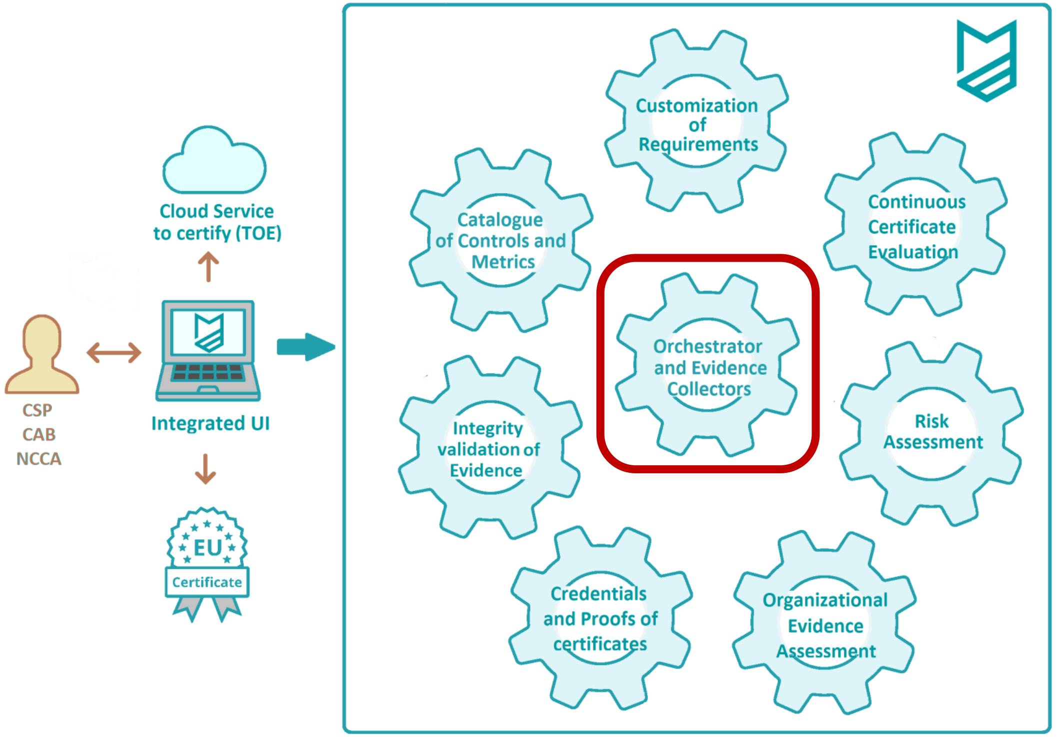


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Wazuh and VAT Evidence Collection

- Overview
  - Purpose
  - Role in MEDINA Architecture

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Wazuh

- An open-source security monitoring tool for threat detection, integrity monitoring, incident response and basic compliance monitoring
- The role in MEDINA: threat detection
- Connects to MEDINA through Wazuh and VAT Evidence Collector

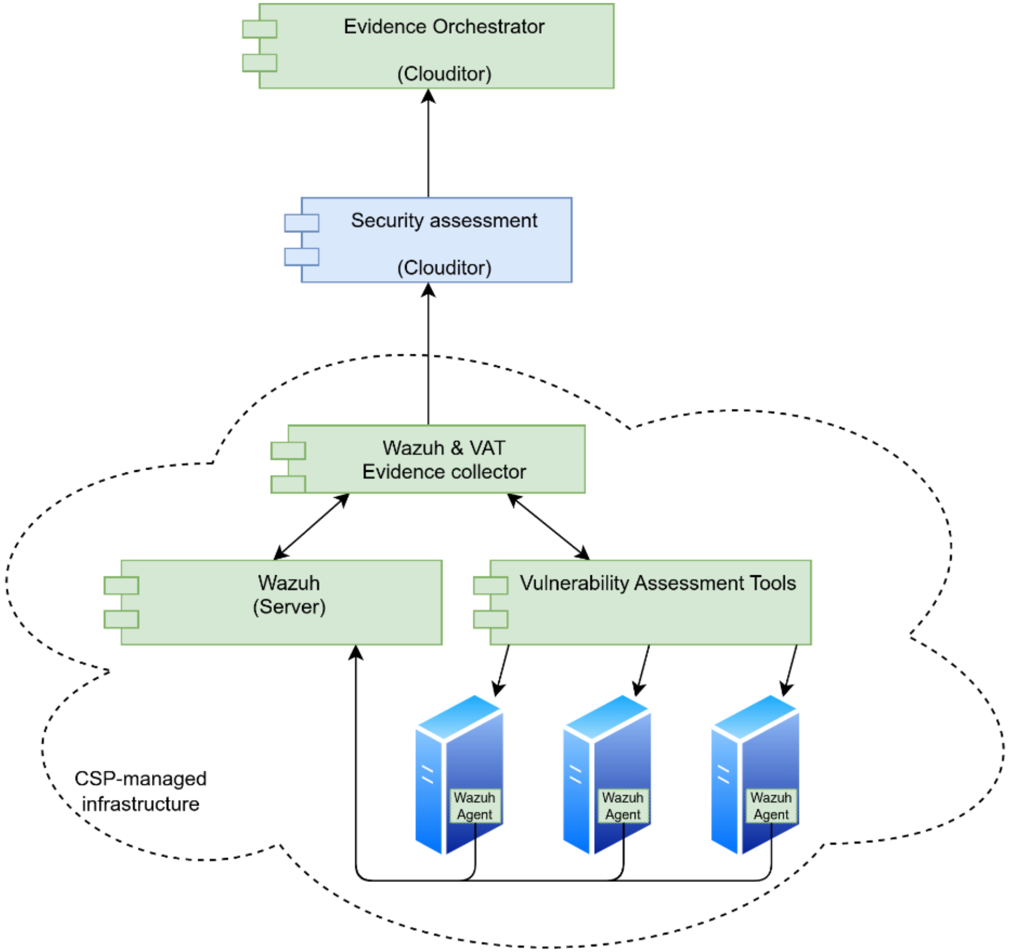
VAT

MEDINA

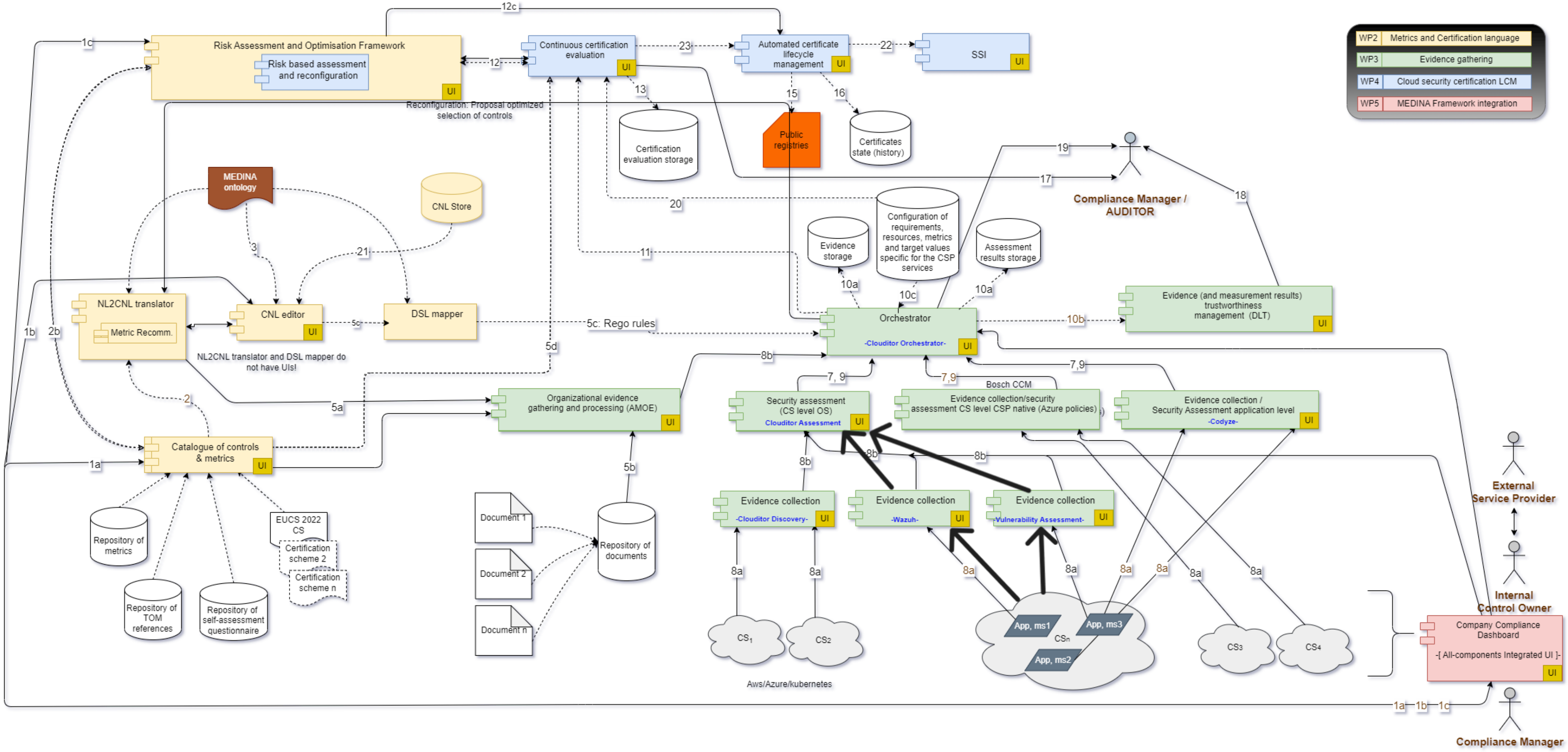
- Vulnerability Assessment Tools (VAT) act as a vulnerability scanning and detection framework, comprised of:
  - two web vulnerability scanners (W3af and OWASP ZAP)
  - a network discovery and auditing tool Nmap
  - a framework for including user-defined custom scripts for detecting specific issues or simply notifying about unavailability of particular services
- The role in MEDINA: vulnerability detection
- Connects to MEDINA through Wazuh and VAT Evidence Collector

Wazuh and VAT Evidence Collector

- Collects data from Wazuh
- Creates scans and fetches scan results from VAT
- Creates evidence based on data gathered from Wazuh and VAT
- Forwards evidence to the Security Assessment component (Clouditor)



Wazuh and VAT in MEDINA architecture


WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
Reconfiguration: Proposal optimized selection of controls
Continuous certification evaluation
Automated certificate lifecycle management
SSI
12c
1c
12
23
22
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
20
MEDINA ontology
CNL Store
3
21
11
Configuration of requirements, resources, metrics and target values specific for the CSP services
Evidence storage
Assessment results storage
10a
10c
10a
Evidence (and measurement results) trustworthiness management (DLT)
10b
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5c
5c: Rego rules
5d
1b
2b
NL2CNL translator and DSL mapper do not have UIs!
Orchestrator
-Clouditor Orchestrator-
8b
7, 9
7,9
Bosch CCM
2
5a
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection/security assessment CS level CSP native (Azure policies)
Evidence collection / Security Assessment application level
-Codyze-
Catalogue of controls & metrics
1a
5b
8b
External Service Provider
Internal Control Owner
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Repository of TOM references
Repository of self-assessment questionnaire
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
8a
CS1
CS2
App, ms1
App, ms3
App, ms2
CSn
CS3
CS4
Aws/Azure/kubernetes
Company Compliance Dashboard
-[All-components Integrated UI]-
1a 1b 1c
Compliance Manager

Interactions with other components

Security Assessment

- Wazuh and VAT Evidence Collector forwards evidence from Wazuh and VAT

Orchestrator

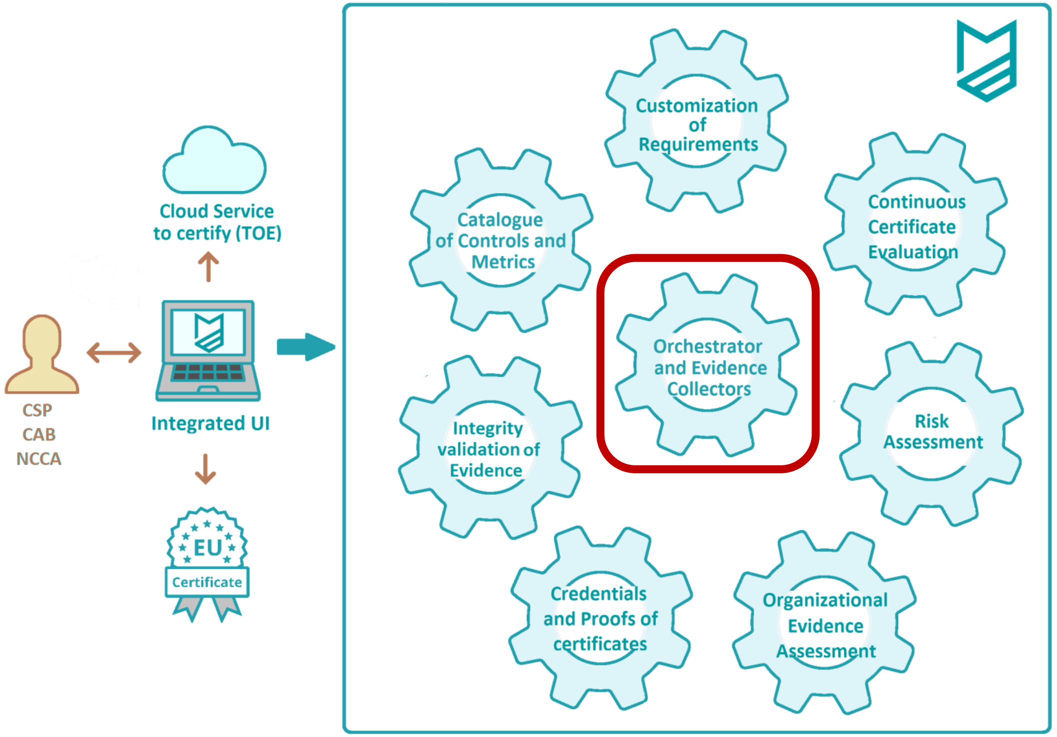
- Wazuh and VAT Evidence Collector authenticates with the Orchestrator
- Wazuh and VAT Evidence Collector gets a cloud service ID for Wazuh and VAT

Wazuh and VAT Evidence Collection

➤ How to use it

- Functionalities

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Wazuh

- Composed of Wazuh agents and server
- Wazuh agents:
  - deployed on the individual monitored machines in the cloud service provider`s infrastructure
  - communicate information about the detected anomalies to the server using Rsyslog
- Wazuh server:
  - consists of Wazuh manager along with the ELK (ElasticSearch, Logstash, Kibana) stack for gathering, storing, and display of data
  - custom integrations are possible to send alerts from Wazuh to any external component

VAT

- VAT uses several microservices. The main are:
  - Scan Configurator: web user interface to configure and trigger vulnerability scans, set schedules, review tasks results, as well as create custom scripts
  - Vulnerability Scanning Registry: collection of integrated scanning tools (W3af, OWASP ZAP and Nmap)
  - Catalogue of custom scripts for scanning and monitoring
  - VAT Service Orchestrator: scheduling and orchestration of scans as well as communication with other components

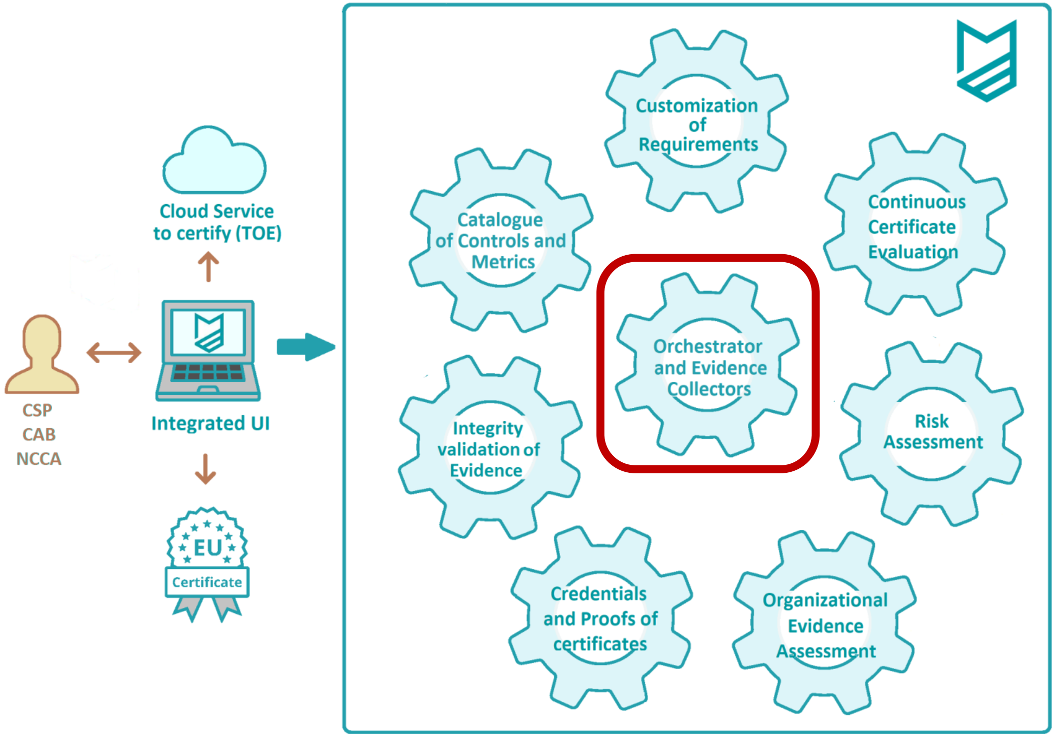
Wazuh and VAT Evidence Collector

- Wazuh Evidence Collector: collects data from Wazuh
- VAT Evidence Collector: creates VAT scans and gathers data from scans
- Clouditor Interface: forwards evidence to the Security Assessment (Clouditor) and is in charge of Clouditor Authentication and other communication with Orchestrator

Wazuh and VAT Evidence Collection

- Installation
  - Deployment
  - Technical Specifications

MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Wazuh installation

- The Wazuh deployment package contains all needed deployment and configuration scripts for installing Wazuh, Wazuh and VAT Evidence Collector and Clouditor connection:
  - Clone the repository:

    git clone https://git.code.tecnalia.com/medina/public/wazuh-deploy

    git clone https://git.code.tecnalia.com/medina/public/wazuh-vat-evidence-collector
  - provision the Wazuh server, Wazuh agents, Clouditor, and Evidence Collector virtual machines by running:

    make create provision
  - Wazuh is available at https://192.168.33.10:5601

- Technical specifications:
  - Wazuh: Ansible deployment scripts, YAML definitions, configuration as well as specific MEDINA configurations of Wazuh rules (XML, JSON).
  - Wazuh and VAT Evidence Collector: developed in Python and packaged as a Docker container.

VAT installation

- VAT is packed as Docker images. Deployment scripts are provided using Vagrant and Ansible in the “vat-deploy” repository:
  - Clone the repository:

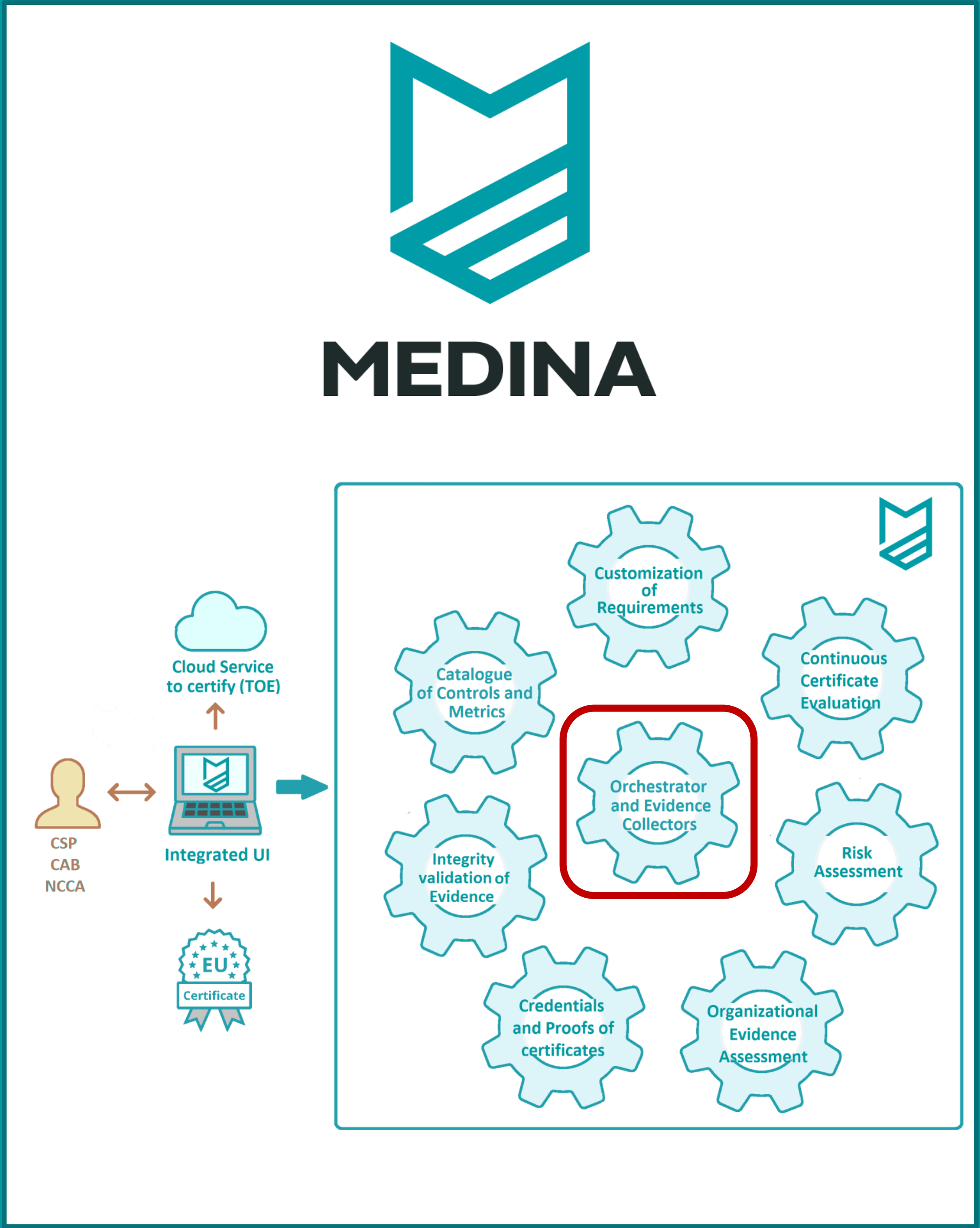
    git clone https://git.code.tecnalia.com/medina/public/vat-deploy
  - Run:

    make create provision

- Technical specifications:
  - The backend components are mostly written in Node.js, except Scheduler which is written in Go
  - MongoDB is used for the Task Storage, and OpenStack Swift for the Object Storage and storage of custom scanning scripts
  - Scan Configurator frontend is built with the Angular web framework
  - The Generic Scanning Suite is built as a single Docker image with Ubuntu as base image with required scanning modules installed (OWASP ZAP, w3af, Nmap)
  - The Result Aggregator is written in Python and outputs a JSON file containing outputs of all the scanning modules used

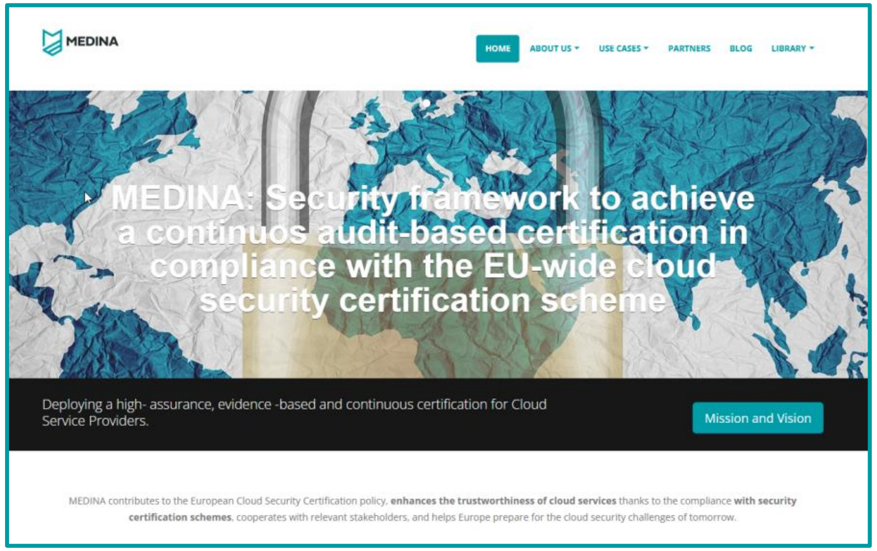
Wazuh and VAT Evidence Collection

- Further information


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator and Evidence Collectors
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** *https://medina-project.eu/public-deliverables*
- Framework demonstrator is available in the MEDINA **YouTube channel** *https://www.youtube.com/@MedinaprojectEU*
- MEDINA Community in **Zenodo** *https://zenodo.org/communities/medina*
- Source code in the public **GitLab** *https://git.code.tecnalia.com/medina/public*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft

XLAB

NIXU cybersecurity.

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

MEDINA

Integrity Validation of Evidence

TECNALIA

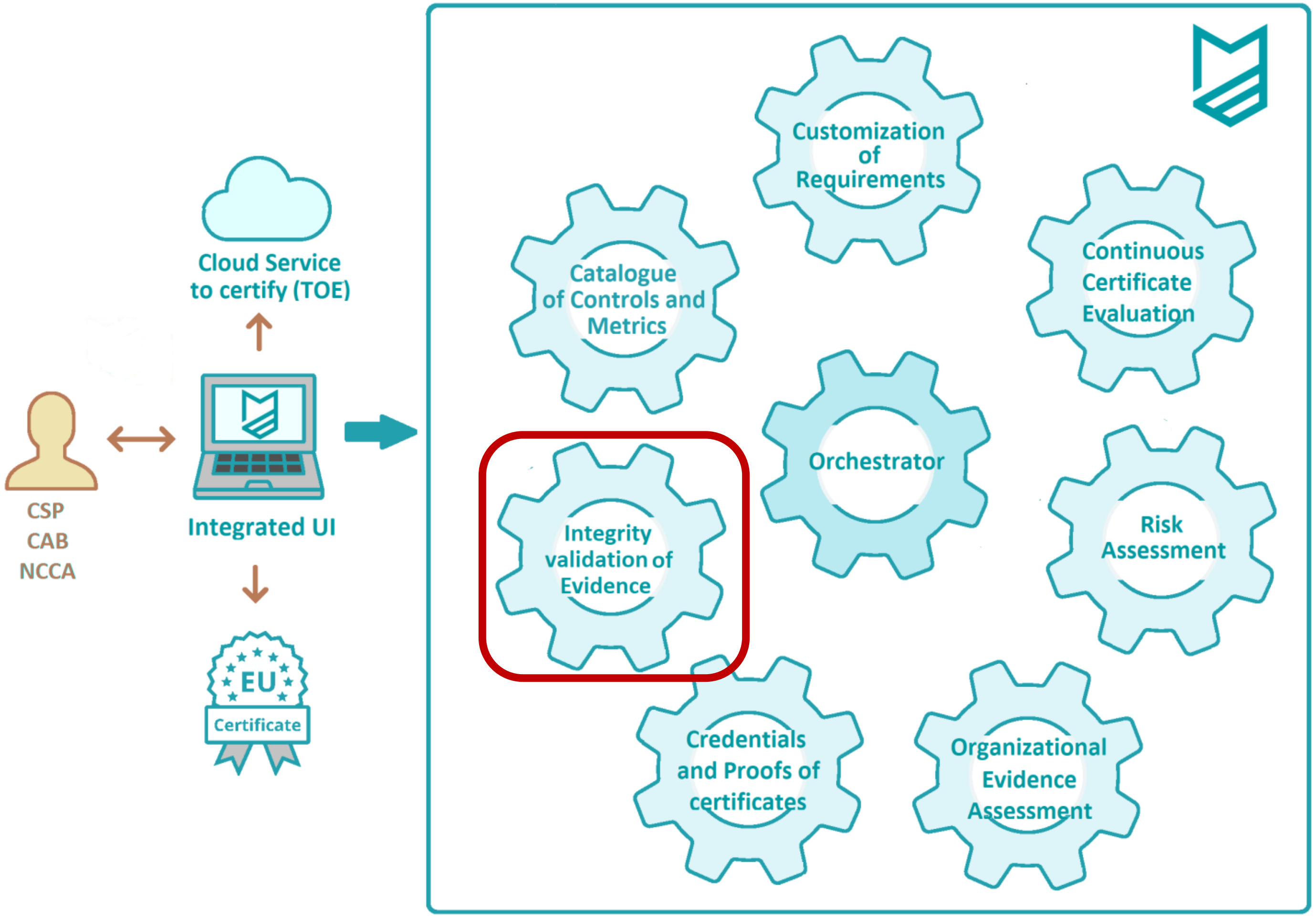
September 2023

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

Chapters

MEDINA

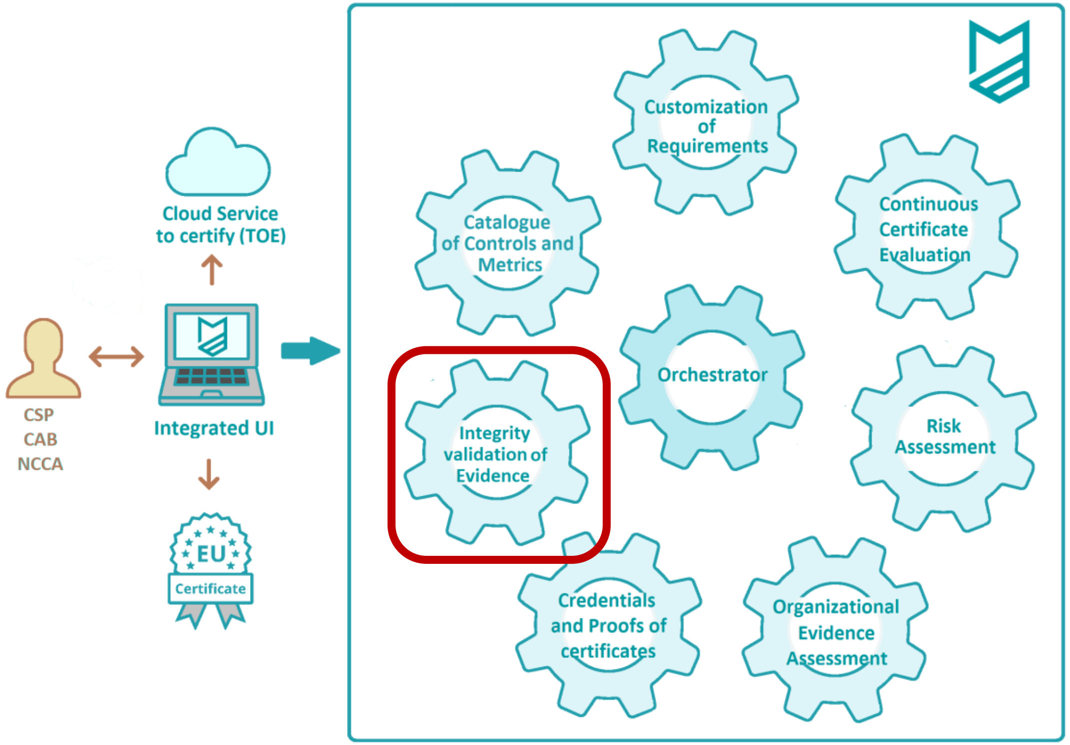
- Overview
- How to use it
- Installation
- Further information


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Integrity Validation of Evidence

- ➤ Overview
  - - Purpose
  - - Role in MEDINA Architecture

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Integrity Validation of Evidence

MEDINA Evidence Trustworthiness System component

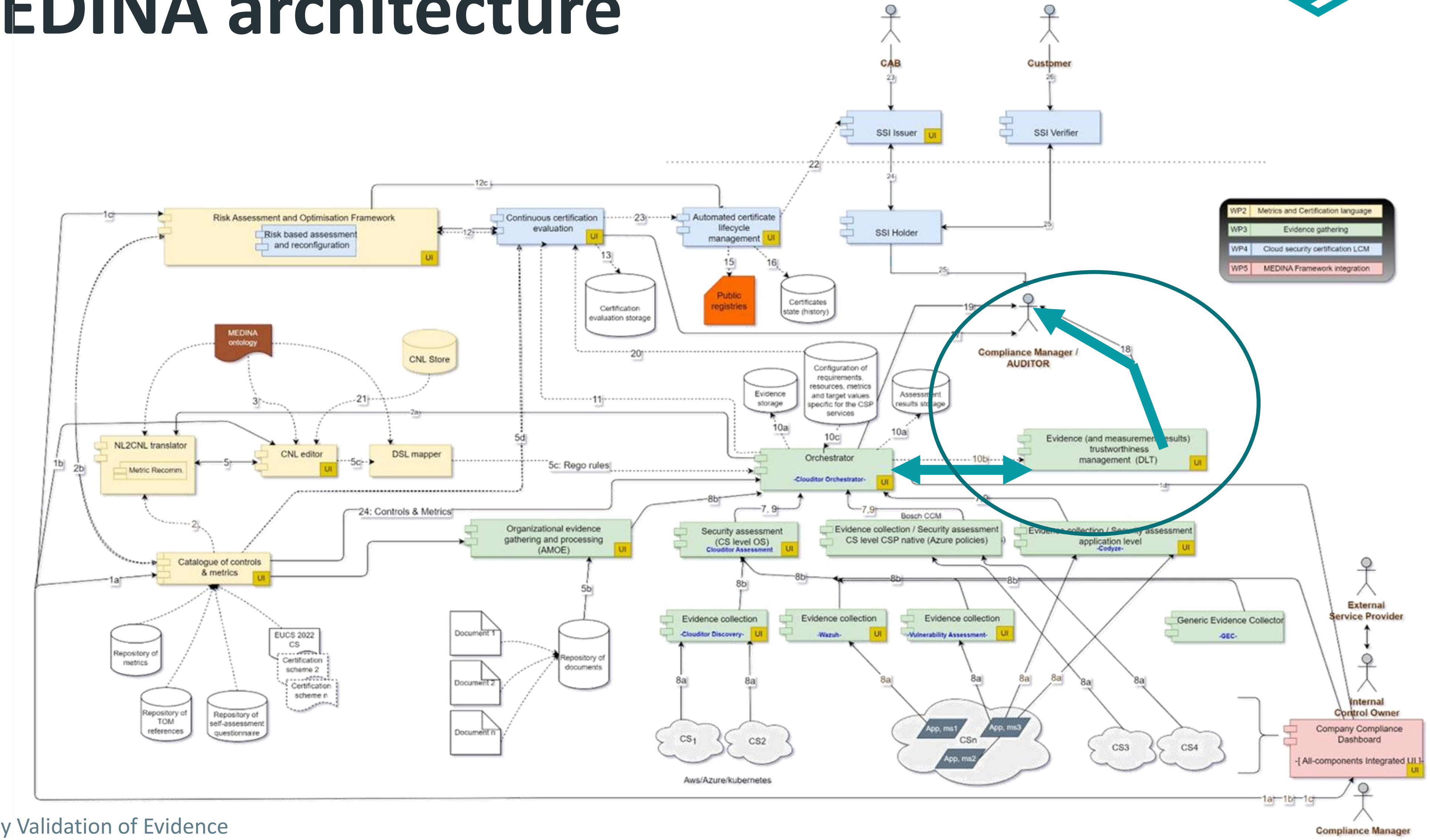
- Maintains an **improved audit trail** of evidence and assessment results.
- Provides a **manual and automatic way of verification** of evidence and assessment results integrity.
- Uses **Blockchain technology** as secure backbone, providing:
  - a record of information on a verifiable way (**verification**)
  - a record of information on a permanent way (**traceability**)
  - guarantees resistance to modification of stored data (**integrity**).

Integrity Validation of Evidence

- The component is enhanced with some extra features:

  1. User-friendly graphical interfaces
     - Manual verification
     - Automatic verification
  2. Security by design (Blockchain as secure storage)
  3. Easy to integrate (REST API in the Blockchain client)
  4. Information confidentiality is guaranteed through the use of hashes
  5. Easy to be extended in terms of information to be recorded

Integrity Validation of Evidence in the MEDINA architecture


CAB
Customer
SSI Issuer
SSI Verifier
SSI Holder
UI
22
23
24
25
26
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
Continuous certification evaluation
Automated certificate lifecycle management
12c
12
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
MEDINA ontology
CNL Store
19
20
21
11
18
Compliance Manager / AUDITOR
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
10b
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5c: Rego rules
5d
Orchestrator
-Clouditor Orchestrator-
Evidence (and measurement results) trustworthiness management (DLT)
1d
24: Controls & Metrics
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Bosch CCM
Evidence collection / Security assessment application level
-Codyze-
7, 9
8b
Catalogue of controls & metrics
1a
1b
1c
2a
2b
3
5b
Repository of metrics
Repository of TOM references
Repository of self-assessment questionnaire
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
Generic Evidence Collector
-GEC-
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
External Service Provider
Internal Control Owner
Company Compliance Dashboard
-[All-components Integrated UI]-
Compliance Manager

Interactions with other components

Orchestrator

- Provides the evidence and assessment results information to be recorded.
- Provides the current evidence and assessment result value to be validated.

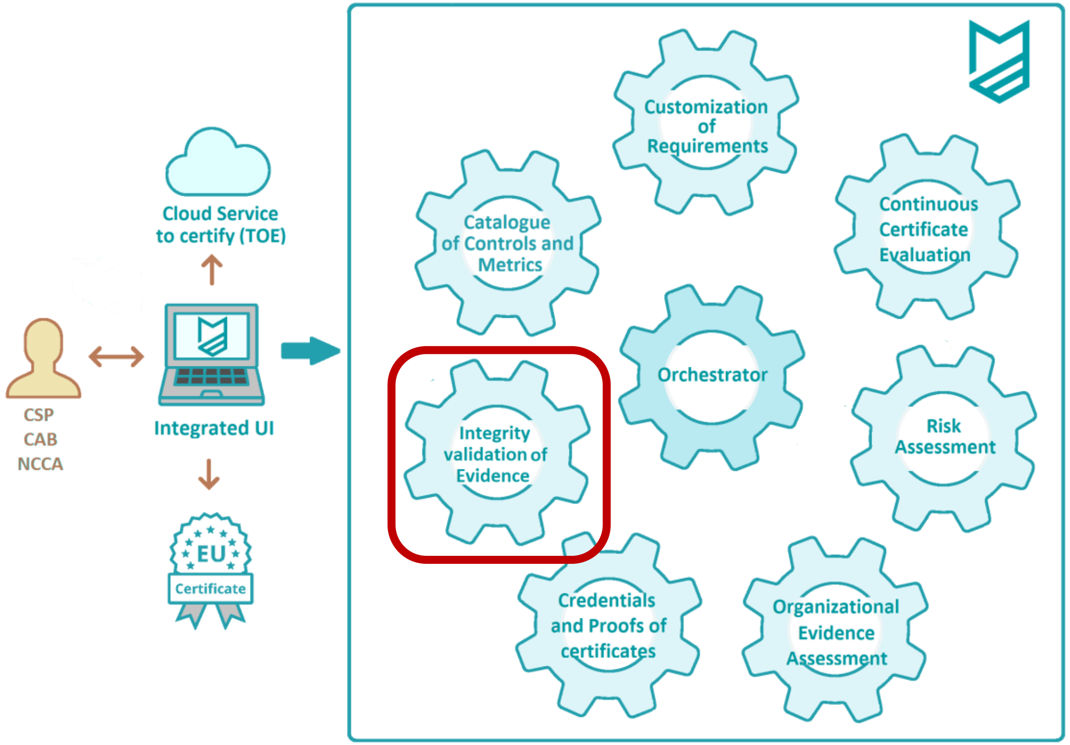
Compliance Manager/Auditor

- Consults the integrity of the evidence or assessment results in a manual or automatic way.

Integrity Validation of Evidence

- How to use it
  - Functionalities
  - Demo

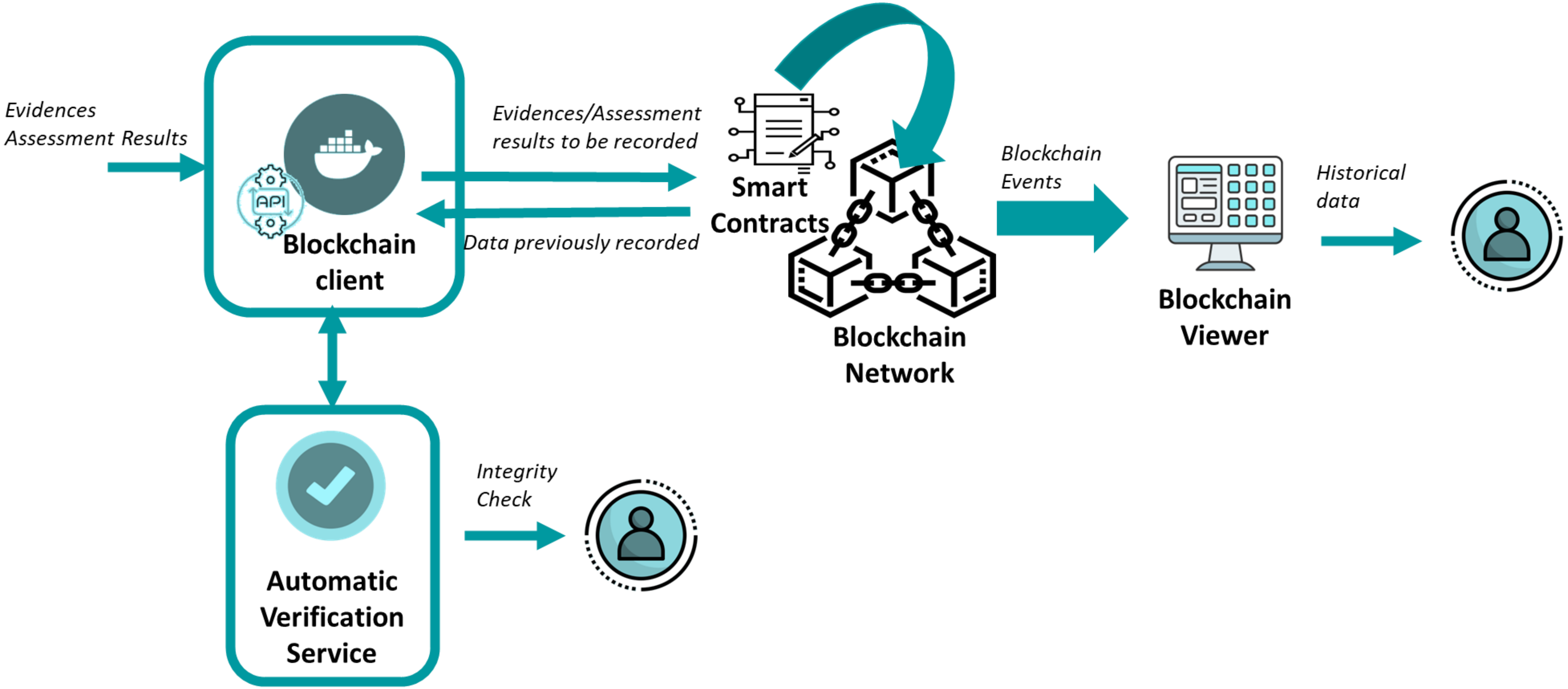
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Functionalities

Components



Evidences Assessment Results

Blockchain client

Evidences/Assessment results to be recorded

Data previously recorded

Smart Contracts

Blockchain Network

Blockchain Events

Blockchain Viewer

Historical data

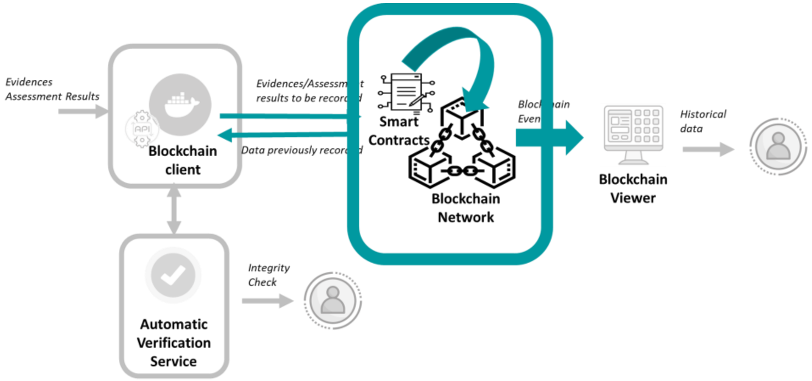
Automatic Verification Service

Integrity Check

Functionalities

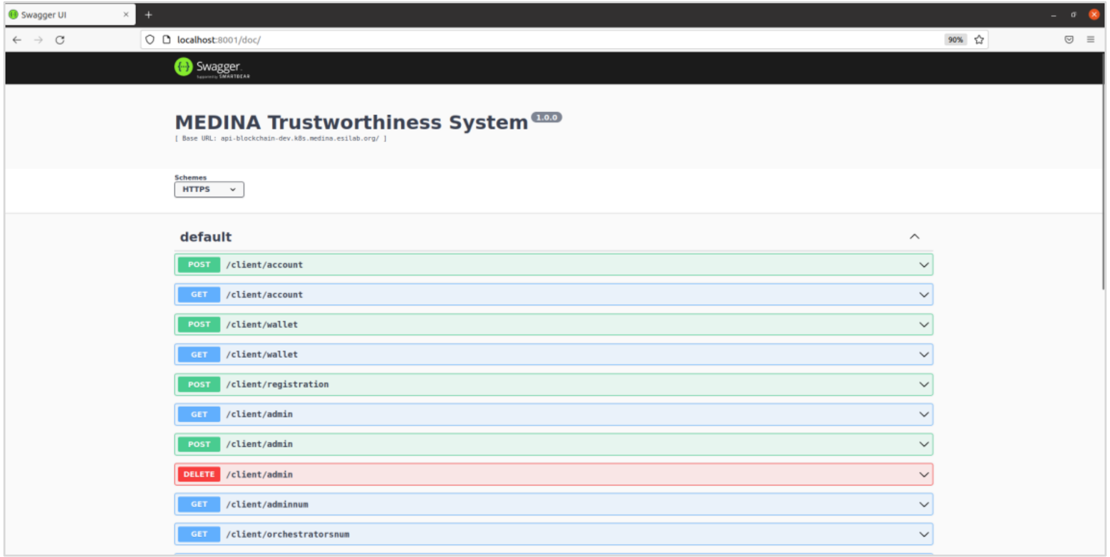
- A **common Blockchain network** has been deployed for different CSPs.
  - A common distributed database that continuously maintains a growing list of cryptographically linked records.
- Smart Contracts have been designed for the **evidence and assessment results audit trail** functionality.
  - Computation programs stored on a blockchain that automatically run when predetermined conditions are met.

Quorum



Functionalities

- Each CSP needs a **Blockchain client** to make the use of Blockchain transparent to users.
  - Internally deals with all technical details of using Blockchain.
  - Exposes a REST API for easy interaction.



Swagger UI

localhost:8001/doc/

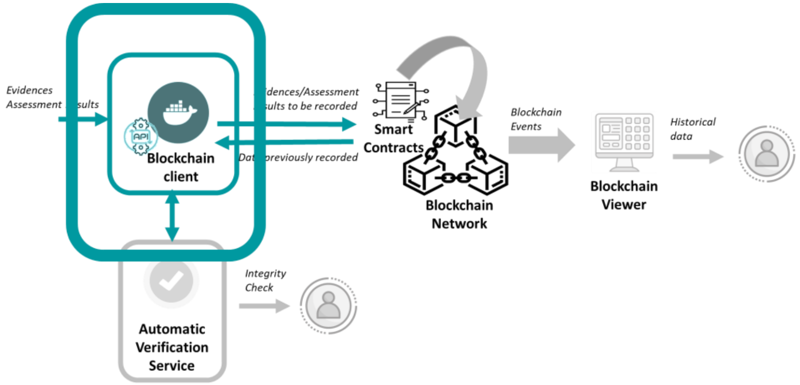
MEDINA Trustworthiness System 1.0.0

[Base URL: api-blockchain-dev.k8s.medina.esilab.org/]

Schemes: HTTPS

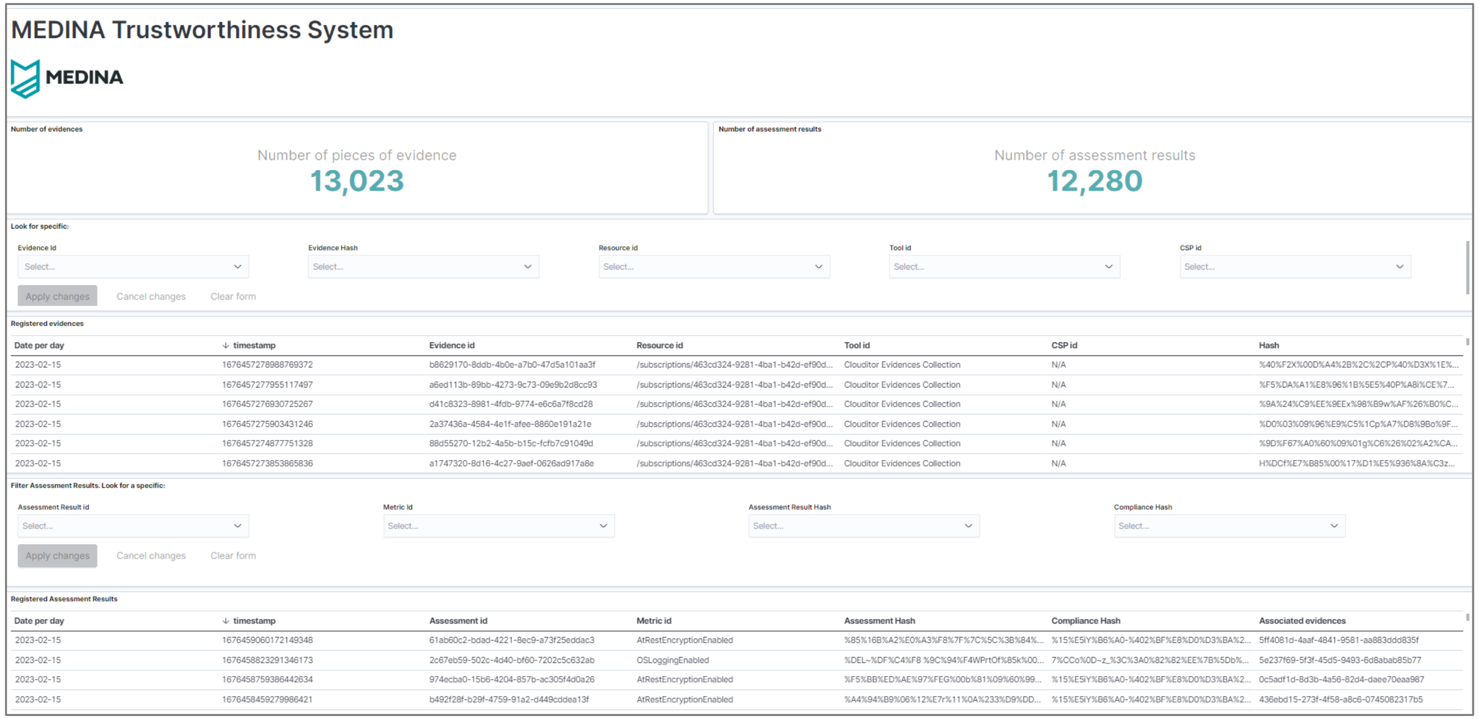
default

```
POST    /client/account
GET     /client/account
POST    /client/wallet
GET     /client/wallet
POST    /client/registration
GET     /client/admin
POST    /client/admin
DELETE  /client/admin
GET     /client/adminnum
GET     /client/orchestratorsnum
```



Functionalities

- A **common Blockchain viewer** has been designed for gathering and showing **all the information** saved on the Blockchain for **different CSPs** (and be able to easily verify it) in a **manual way**.



MEDINA Trustworthiness System

MEDINA

Number of evidences

Number of pieces of evidence
13,023

Number of assessment results

Number of assessment results
12,280

Look for specific:

Evidence Id: Select...
Evidence Hash: Select...
Resource id: Select...
Tool id: Select...
CSP id: Select...

Apply changes | Cancel changes | Clear form

Registered evidences

Date per day	↓ timestamp	Evidence id	Resource id	Tool id	CSP id	Hash
2023-02-15	1676457278988769372	b8629170-8ddb-4b0e-a7b0-47d5a101aa3f	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%40%F2X%00D%A4%2B%2C%2CP%40%D3X%1E%...
2023-02-15	1676457277955117497	a6ed113b-89bb-4273-9c73-09e9b2d8cc93	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%F5%DA%A1%E8%96%1B%5E5%40P%A8i%CE%7...
2023-02-15	1676457276930725267	d41c8323-8981-4fdb-9774-e6c6a7f8cd28	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%9A%24%C9%EE%9EEx%98%B9w%AF%26%B0%C...
2023-02-15	1676457275903431246	2a37436a-4584-4e1f-afee-8860e191a21e	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%D0%03%09%96%E9%C5%1Cp%A7%D8%9Bo%9F...
2023-02-15	1676457274877751328	88d55270-12b2-4a5b-b15c-fcfb7c91049d	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%9D%F67%A0%60%09%01g%C6%26%02%A2%CA...
2023-02-15	1676457273853865836	a1747320-8d16-4c27-9aef-0626ad917a8e	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	H%DCf%E7%B85%00%17%D1%E5%936%8A%C3z...

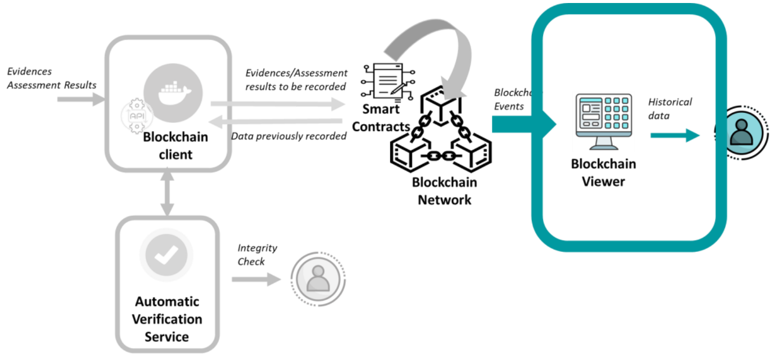
Filter Assessment Results. Look for a specific:

Assessment Result id: Select...
Metric Id: Select...
Assessment Result Hash: Select...
Compliance Hash: Select...

Apply changes | Cancel changes | Clear form

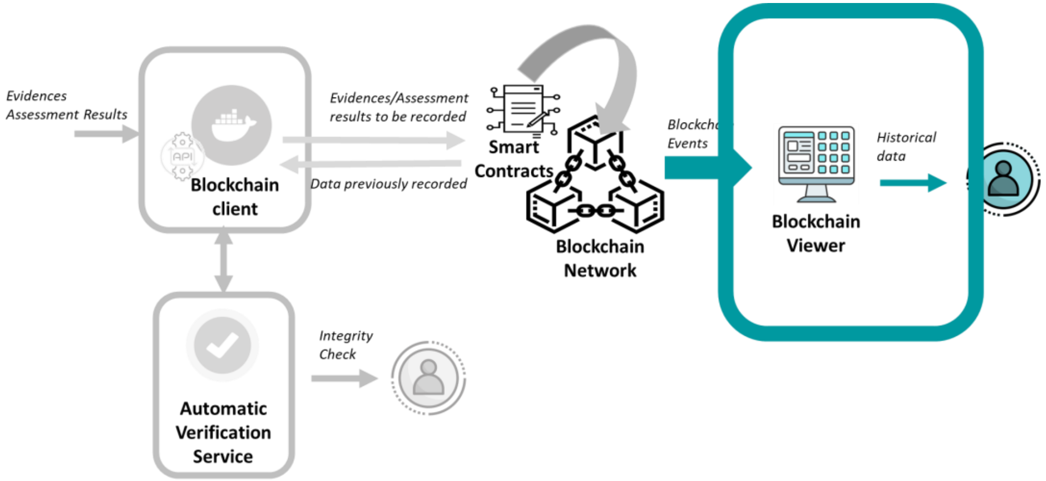
Registered Assessment Results

Date per day	↓ timestamp	Assessment id	Metric id	Assessment Hash	Compliance Hash	Associated evidences
2023-02-15	1676459060172149348	61ab60c2-bdad-4221-8ec9-a73f25eddac3	AtRestEncryptionEnabled	%85%16B%A2%E0%A3%F8%7F%7C%5C%3B%84%...	%15%E5iY%B6%A0-%402%BF%E8%D0%D3%BA%2...	5ff4081d-4aaf-4841-9581-aa883ddd835f
2023-02-15	1676458823291346173	2c67eb59-502c-4d40-bf60-7202c5c632ab	OSLoggingEnabled	%DEL~%DF%C4%F8 %9C%94%F4WPrtOf%85k%00...	7%CCo%0D~z_%3C%3A0%82%82%EE%7B%5Db%...	5e237f69-5f3f-45d5-9493-6d8abab85b77
2023-02-15	1676458759386442634	974ecba0-15b6-4204-857b-ac305f4d0a26	AtRestEncryptionEnabled	%F5%BB%ED%AE%97%FEG%00b%81%09%60%99...	%15%E5iY%B6%A0-%402%BF%E8%D0%D3%BA%2...	0c5adf1d-8d3b-4a56-82d4-daee70eaa987
2023-02-15	1676458459279986421	b492f28f-b29f-4759-91a2-d449cddea13f	AtRestEncryptionEnabled	%A4%94%B9%06%12%E7r%11%0A%233%D9%DD...	%15%E5iY%B6%A0-%402%BF%E8%D0%D3%BA%2...	436ebd15-273f-4f58-a8c6-0745082317b5



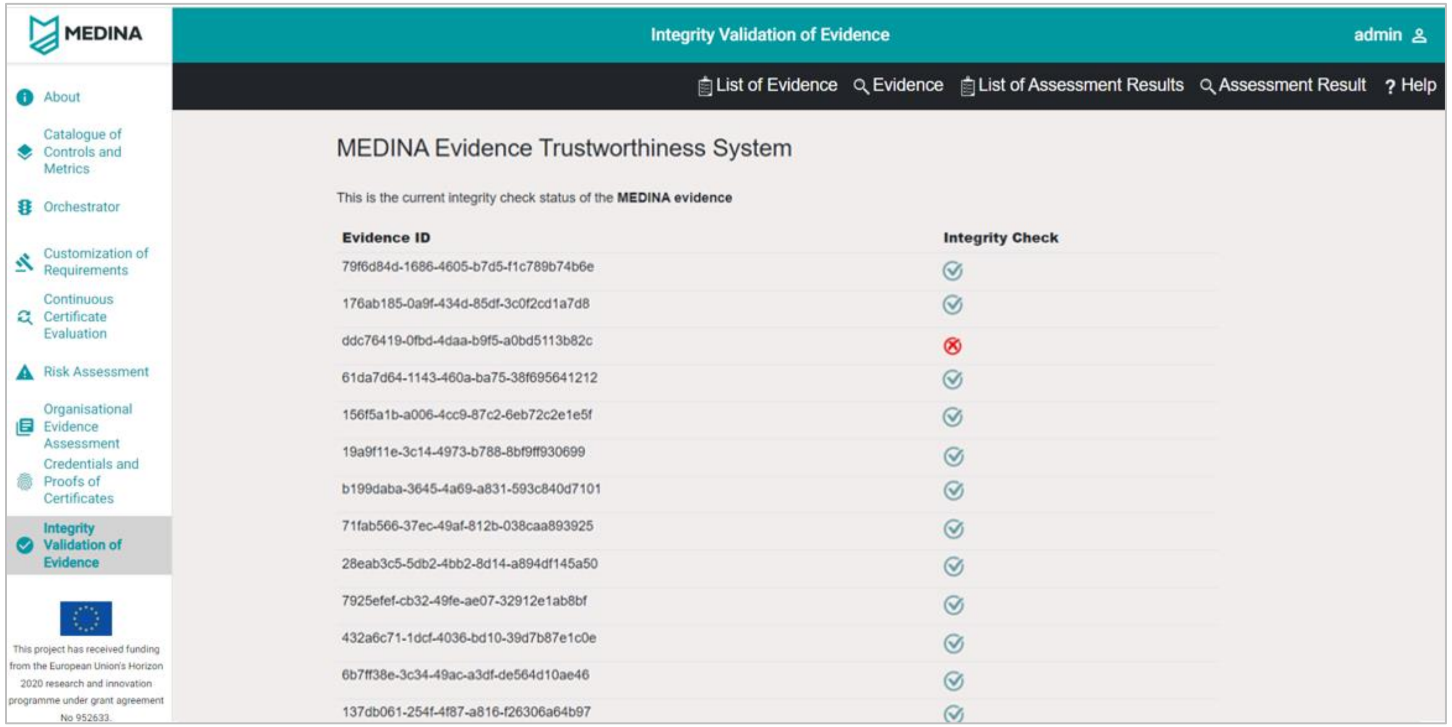
Integrity Validation of Evidence – Manual verification

- DEMO -



Functionalities

- **Automatic verification** service allows an automatic check of the integrity of CSP’s evidence and assessment results.

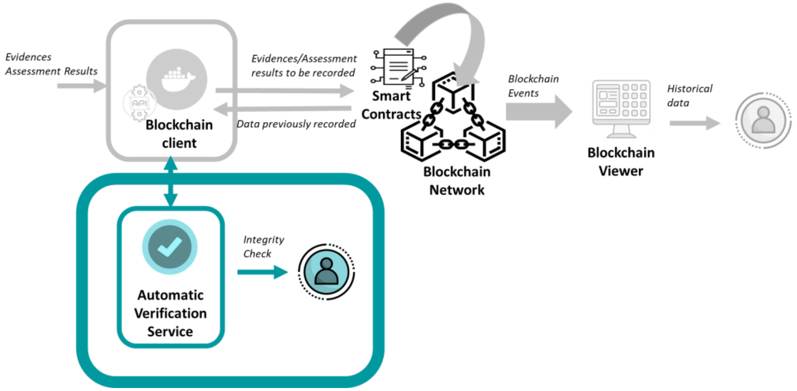

MEDINA
Integrity Validation of Evidence
admin
List of Evidence
Evidence
List of Assessment Results
Assessment Result
? Help
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Continuous Certificate Evaluation
Risk Assessment
Organisational Evidence Assessment
Credentials and Proofs of Certificates
Integrity Validation of Evidence

MEDINA Evidence Trustworthiness System

This is the current integrity check status of the **MEDINA evidence**

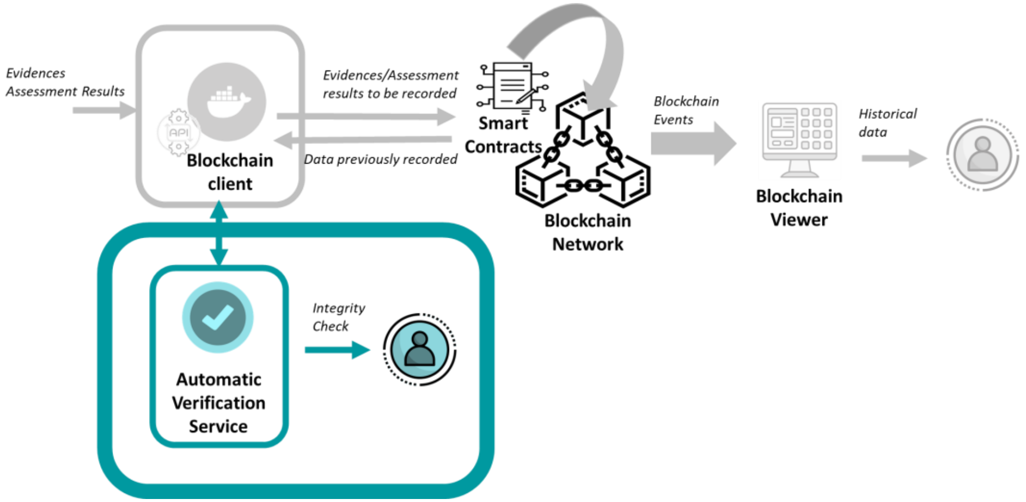
Evidence ID	Integrity Check
79f6d84d-1686-4605-b7d5-f1c789b74b6e	✓
176ab185-0a9f-434d-85df-3c0f2cd1a7d8	✓
ddc76419-0fbd-4daa-b9f5-a0bd5113b82c	☒
61da7d64-1143-460a-ba75-38f695641212	✓
156f5a1b-a006-4cc9-87c2-6eb72c2e1e5f	✓
19a9f11e-3c14-4973-b788-8bf9ff930699	✓
b199daba-3645-4a69-a831-593c840d7101	✓
71fab566-37ec-49af-812b-038caa893925	✓
28eab3c5-5db2-4bb2-8d14-a894df145a50	✓
7925efef-cb32-49fe-ae07-32912e1ab8bf	✓
432a6c71-1dcf-4036-bd10-39d7b87e1c0e	✓
6b7ff38e-3c34-49ac-a3df-de564d10ae46	✓
137db061-254f-4f87-a816-f26306a64b97	✓

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



Integrity Validation of Evidence – Automatic verification

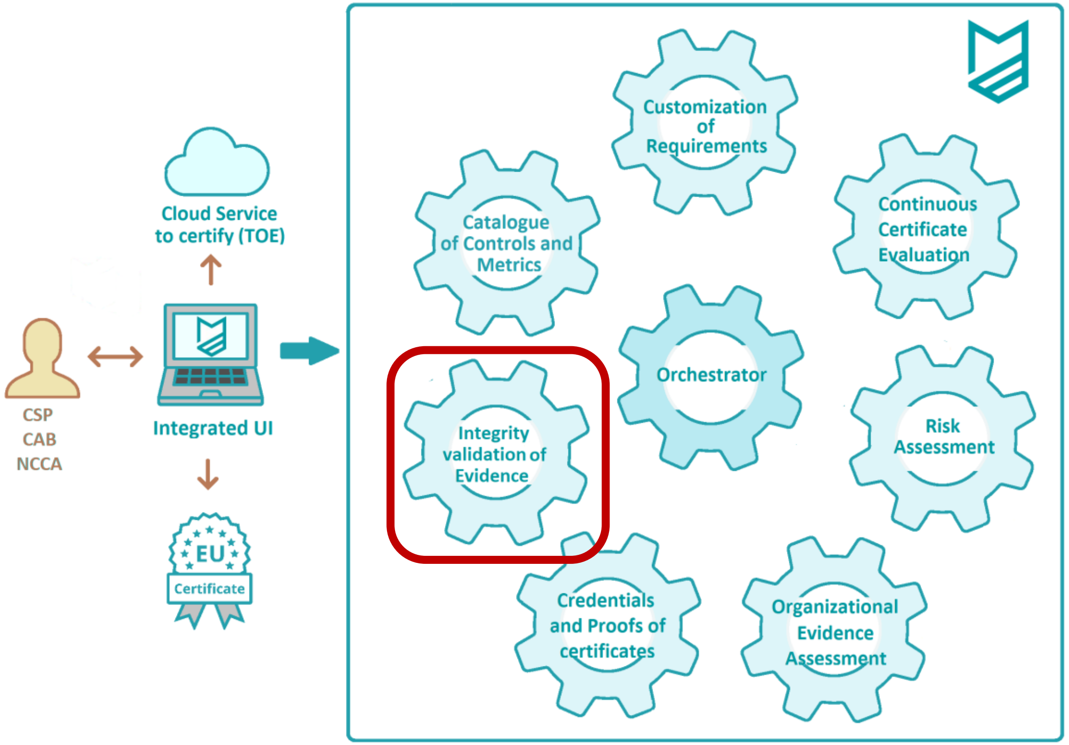
- DEMO -



Integrity Validation of Evidence

- Installation
  - - Deployment
  - - Technical Specifications

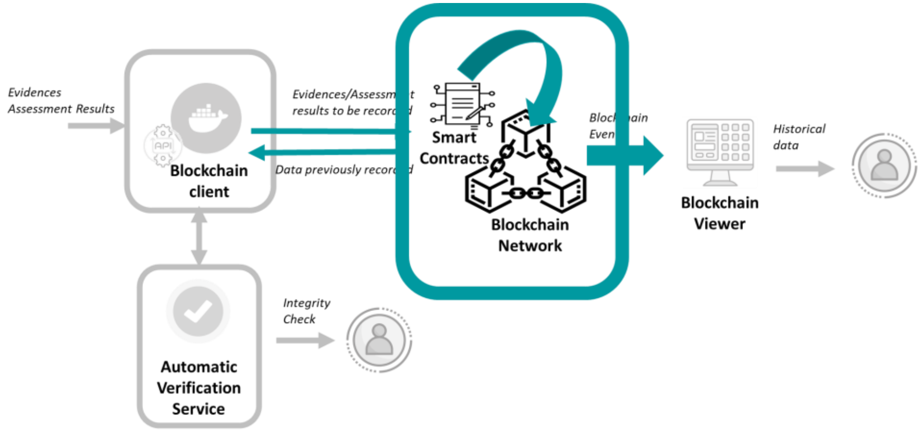
MEDINA



Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Deployment

- The **Blockchain network** is **provided as a service** from TECNALIA.
  - The **Smart Contracts** are already deployed on the TECNALIA´s Blockchain network.
- **The Blockchain network is automatically accesible through the Blockchain client.**



Deployment

The Blockchain client can be locally deployed:

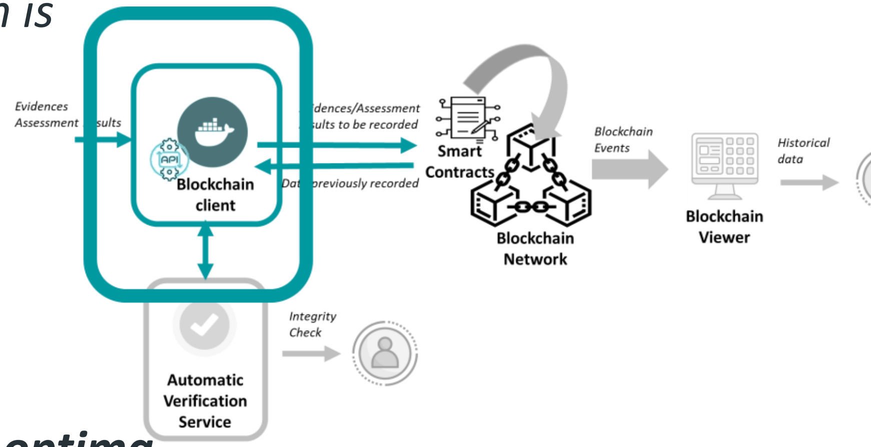
- Login MEDINA artifact:

  -
    ```
    sudo docker login optima-medina-docker-dev.artifact.tecnalia.com
    ```
    (and enter your username and password; registration in Orein is needed in advance)
- Pull the Docker image:

  -
    ```
    sudo docker pull optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/blockchain:latest
    ```
- Run the Docker image:

  -
    ```
    sudo docker run -d -p 8001:8001 –name medina_blockchain optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/blockchain:latest
    ```
- The Blockchain client will be available at:

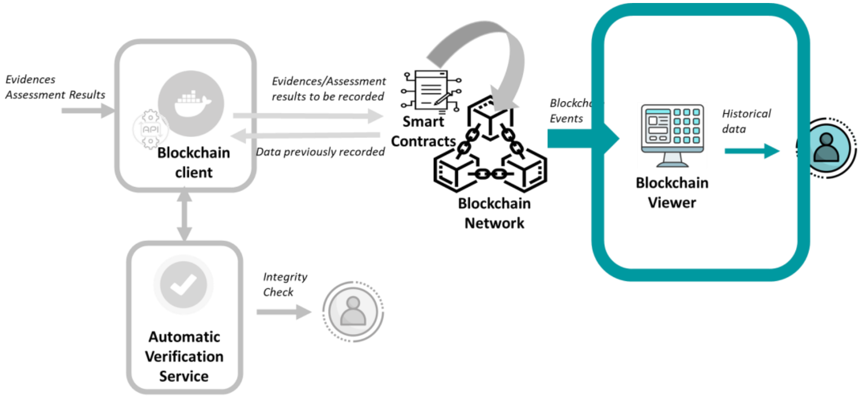
  https://localhost:8001/



Deployment

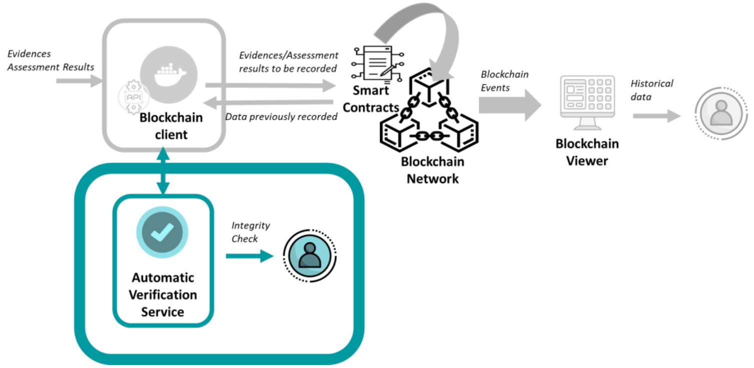
- The **Blockchain Viewer** is **provided as a service** from TECNALIA.
- The Blockchain Viewer is accesible at:

  https://kibana.medina.bclab.dev



Deployment

- **Automatic verification (backend/frontend) service can be locally deployed**:
  - Login MEDINA artifact:
    - ***sudo docker login optima-medina-docker-dev.artifact.tecnalia.com*** *(and enter your username and password; registration in Orein is needed in advance)*
  - Pull the Docker image:
    - ***sudo docker pull optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/backend:latest***
    - ***sudo docker pull optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/frontend:latest***
  - Run the Docker image:
    - ***sudo docker run -d -p 8002:8002 –name medina_backend optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/backend:latest***
    - ***sudo docker run -d -p 8003:8003 –name medina_backend optima-medina-docker-dev.artifact.tecnalia.com/wp3/t35/frontend:latest***
  - The automatic verification service will be available at https://localhost:8003/



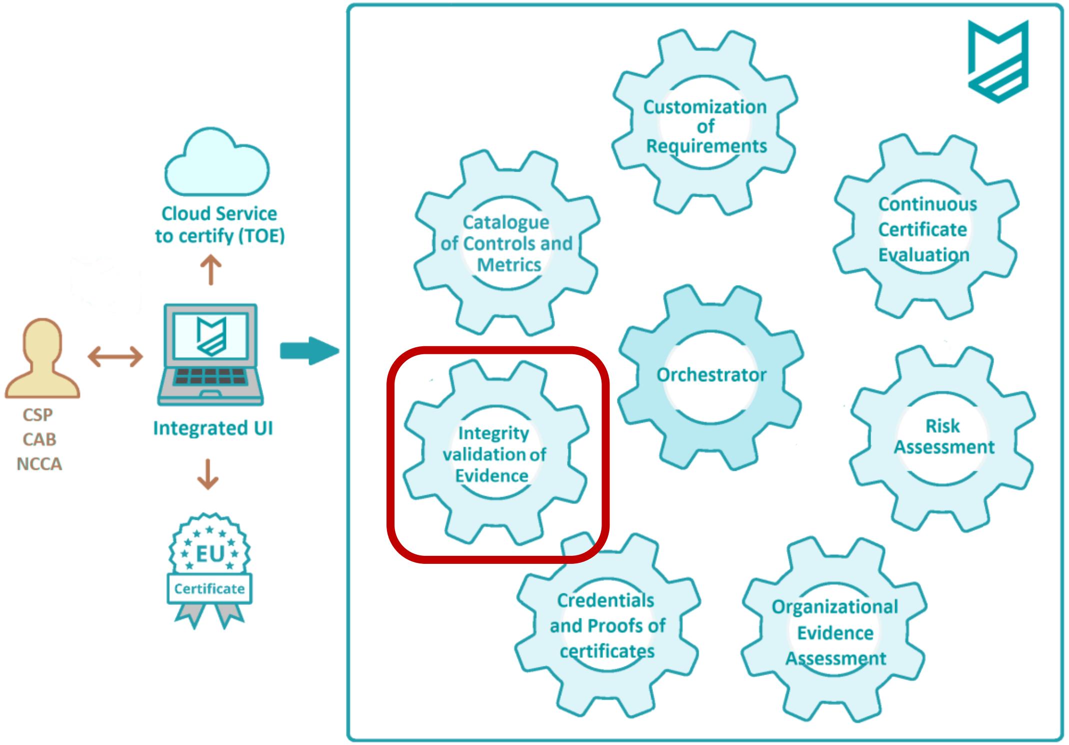
Installation

- Technical specifications
  - Hyperledger Quorum as Blockchain technology.
  - Solidity-based Smart Contracts.
  - Elastic ELK for Blockchain viewer.
  - React and Nodejs for backend/frontend.
  - Javascript for Blockchain client.
  - Docker for installation.

Integrity Validation of Evidence

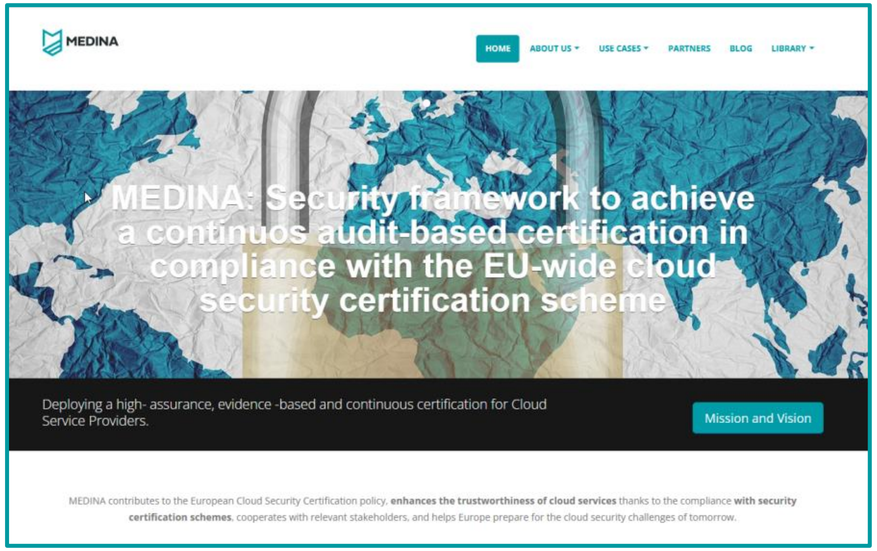
- ➤ Further information

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer
AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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

MEDINA

Continuous Certification Evaluation
Risk Assessment and Optimisation Framework
Automated Life Cycle Manager

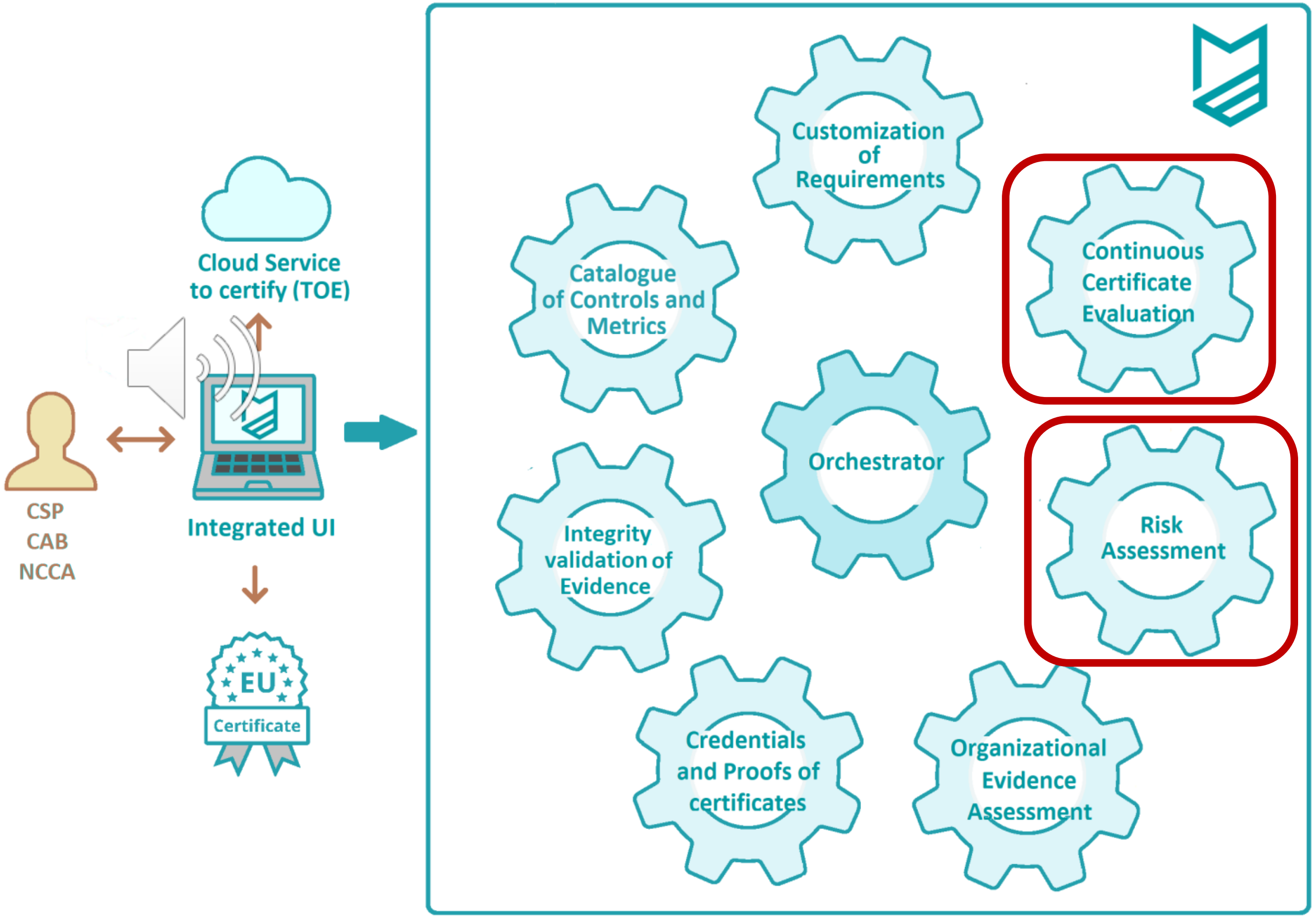
XLAB, CNR, Fraunhofer AISEC

September 2023

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

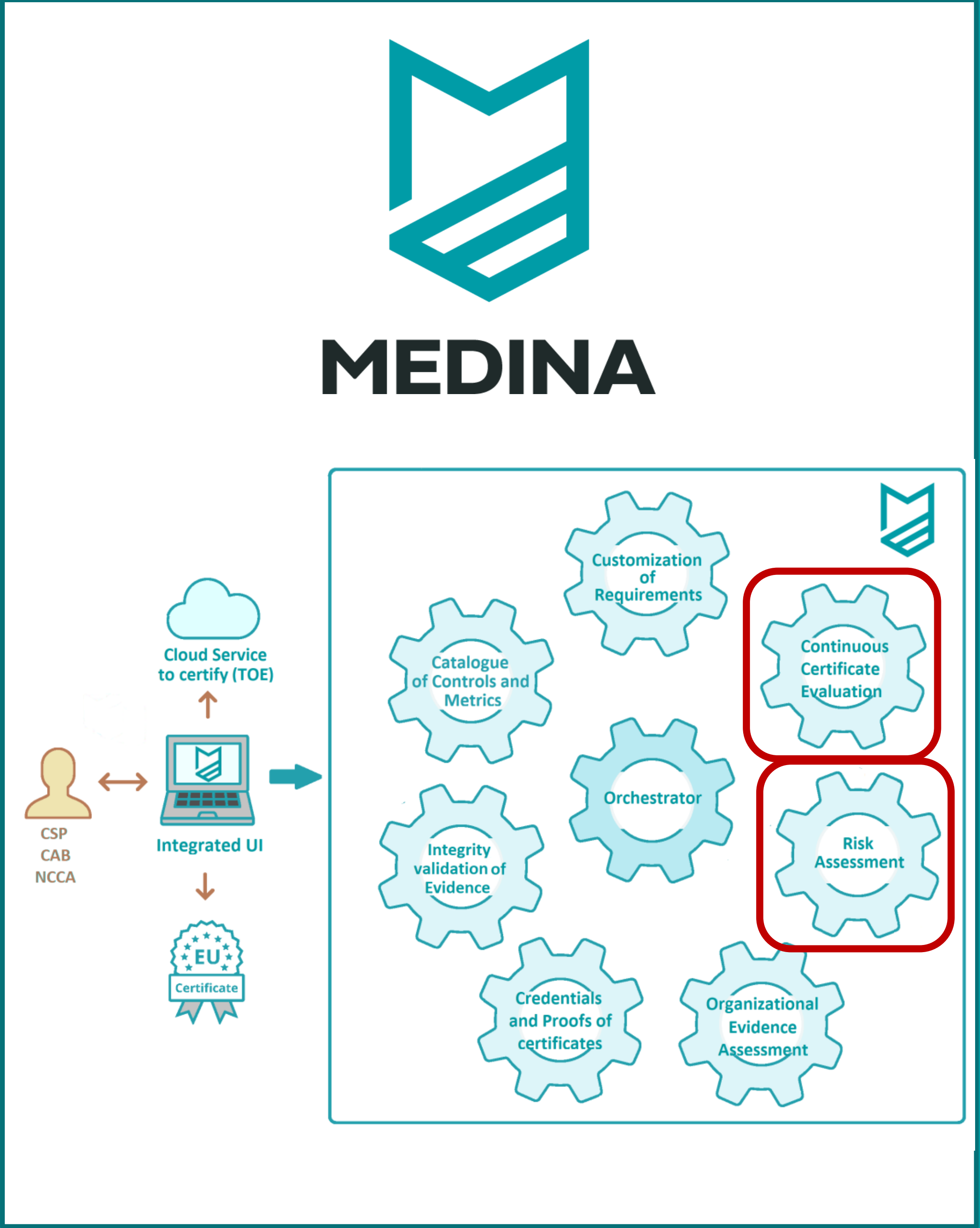
Chapters

- Overview
- How to use it
- Installation
- Further information


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

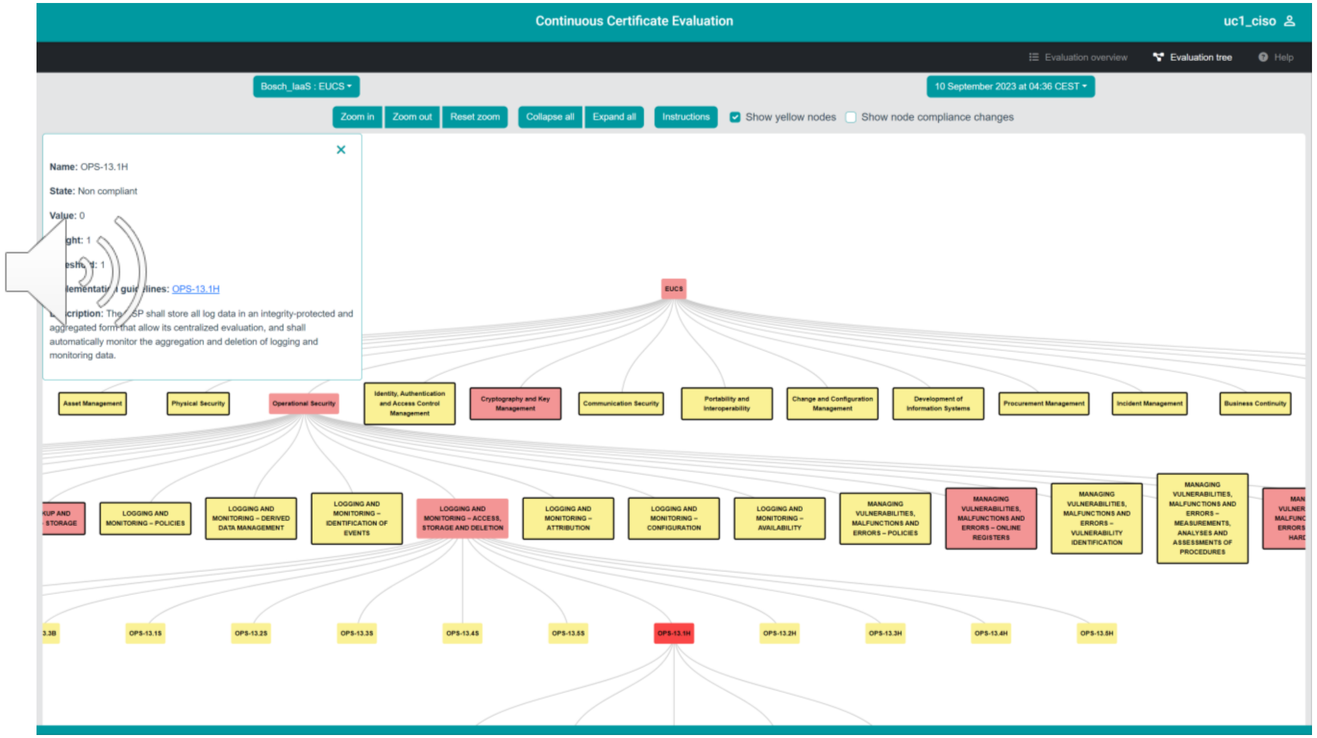
CCE
RAOF
LCM

- Overview
  - Purpose
  - Role in MEDINA Architecture


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Continuous Certification Evaluation (CCE)

- Purpose:
  - Collects assessment results and builds an evaluation tree for the Target of Evaluation (ToE) representing the aggregated assessment results on higher levels of the certification scheme (e.g. EUCS)
- Modes of use:
  - Has a navigable user interface (UI) that allows the user to interact with the evaluation tree
- Use in MEDINA:
  - Receives structure of the used certification scheme from the Catalogue of Controls and Metrics
  - Receives all configurations (inc. assessment results) related to ToE from the Orchestrator
  - Send the evaluation tree for further risk assessment to RAOF
  - Sends operational effectiveness measures to Life-Cycle Manager


Continuous Certificate Evaluation
uc1_ciso
Evaluation overview
Evaluation tree
Help
Bosch_IaaS : EUCS
10 September 2023 at 04:36 CEST
Zoom in
Zoom out
Reset zoom
Collapse all
Expand all
Instructions
Show yellow nodes
Show node compliance changes
EUCS
Asset Management
Physical Security
Operational Security
Identity, Authentication and Access Control Management
Cryptography and Key Management
Communication Security
Portability and Interoperability
Change and Configuration Management
Development of Information Systems
Procurement Management
Incident Management
Business Continuity
KUP AND STORAGE
LOGGING AND MONITORING – POLICIES
LOGGING AND MONITORING – DERIVED DATA MANAGEMENT
LOGGING AND MONITORING – IDENTIFICATION OF EVENTS
LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION
LOGGING AND MONITORING – ATTRIBUTION
LOGGING AND MONITORING – CONFIGURATION
LOGGING AND MONITORING – AVAILABILITY
MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES
MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS
MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION
MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS OF PROCEDURES
MAN VULNER MALFUNC ERRORS HARD
3.3B
OPS-13.1S
OPS-13.2S
OPS-13.3S
OPS-13.4S
OPS-13.5S
OPS-13.1H
OPS-13.2H
OPS-13.3H
OPS-13.4H
OPS-13.5H

×

Name: OPS-13.1H

State: Non compliant

Value: 0

ght: 1

esh d: 1

lementati guid lines: OPS-13.1H

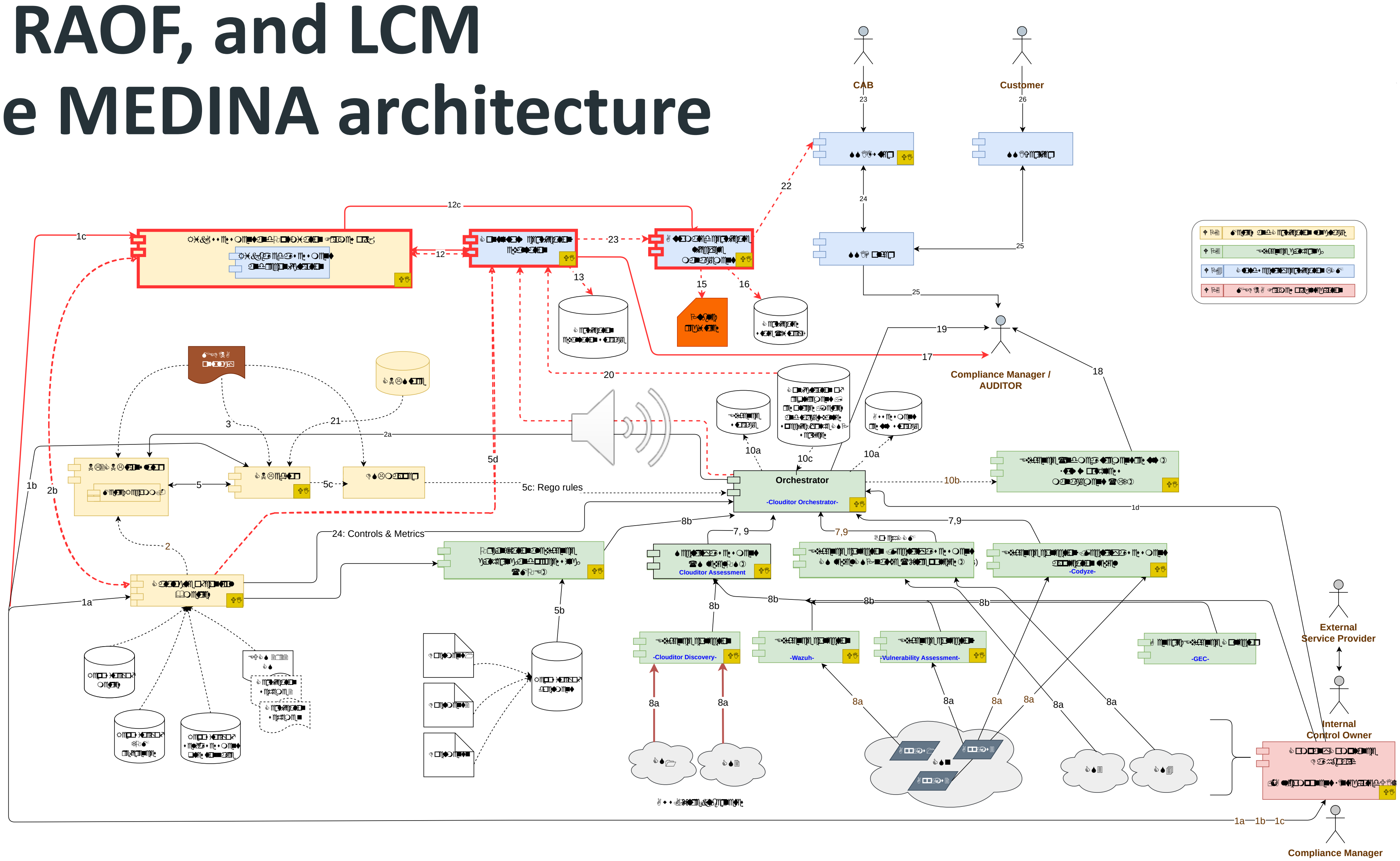
cription: The SP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data.

Risk Assessment and Optimisation Framework (RAOF)

- Purpose:
  - Dynamically analyse and evaluate detected non-conformities with estimated cyber risk.
- Two modes:
  - Static – manual usage through GUI (see a dedicated demo)
  - Dynamic – automatic usage through API (this demo)
- Use in Medina
  - Receive information about non-conformities from CCE
  - Analyse non-conformities and evaluate if they are major or minor
  - Report the results to LCM

Automated Life Cycle Manager (LCM)

- Provides preliminary, automated certificate state
- Integrates multiple factors for deciding on a certificate state
  - Risk value (see RAOF)
  - Operational effectiveness (calculated by CCE)
  - Timing rules (based on EUCS)
- Integrates with Orchestrator to store and modify certificates and their status
- Integrates with SSI for human validation



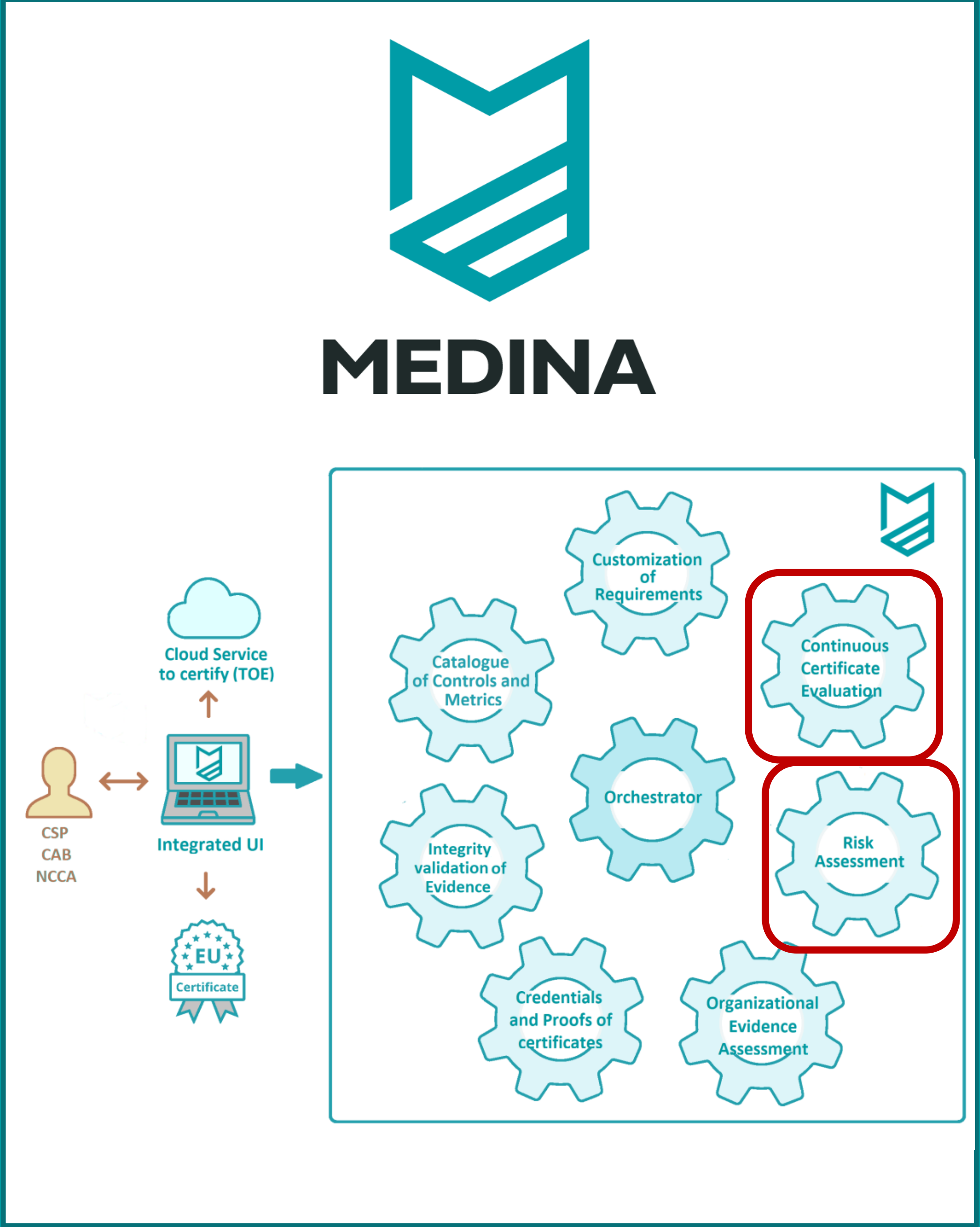
CCE, RAOF, and LCM in the MEDINA architecture

Interactions with other components

- Catalogue of Controls and Metrics
- Orchestrator
  - Obtain assessment results
- SSI System
  - Forward certificate updates
- User
  - View aggregated cloud service compliance view
  - Configure risk assessment parameters
  - View certificate status

CCE
RAOF
LCM

- How to use them
  - Functionalities
  - Demo


MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

CCE

- Functionalities:
  - Aggregates assessment results for ToE and presents them in the form of an evaluation tree
  - Supports multiple ToE
  - Holds evaluation history for every ToE
- Input:
  - Structure of the certification scheme
    - Provided by Catalogue of Controls and Metrics
  - All configurations related to ToE (chosen controls/requirements, a list of monitored resources and assessment results)
    - Provided by Orchestrator
- Processing:
  - Aggregation of assessment results
  - Calculation of compliance of each tree node
- Output:
  - Interactive visualization of the evaluation tree with compliance status

RAOF

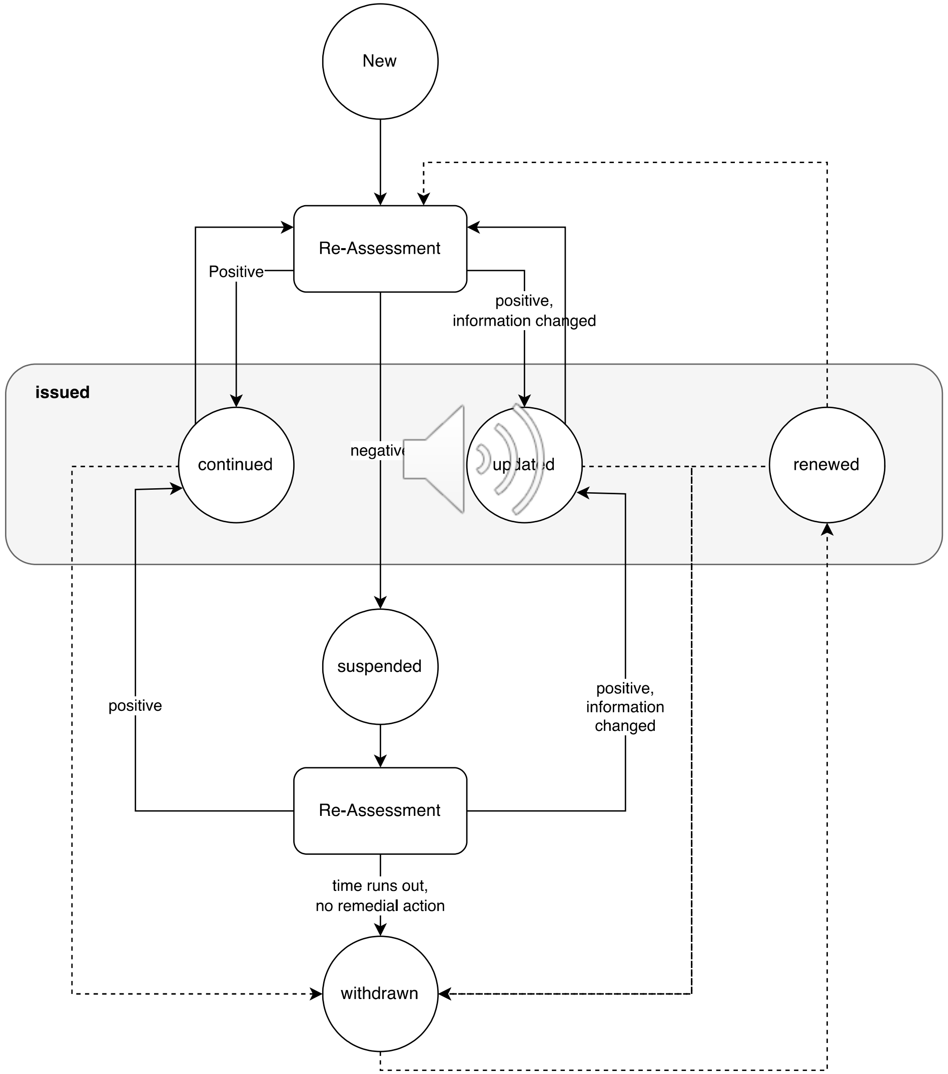
MEDINA

- Functionalities:
  - A background risk-based analysis and evaluation of non-conformities
- Input:
  - Asset and impact values
    - Provided before continuous monitoring, through GUI
  - Status of requirements
    - Provided by CCE, based on the monitoring results
- Processing:
  - Automatically compute real risk value using input information
  - Compare the value with ideal risk (full conformity) to decide if non-conformity is major or minor
- Output:
  - Major or minor evaluation result (sent to LCM)

LCM

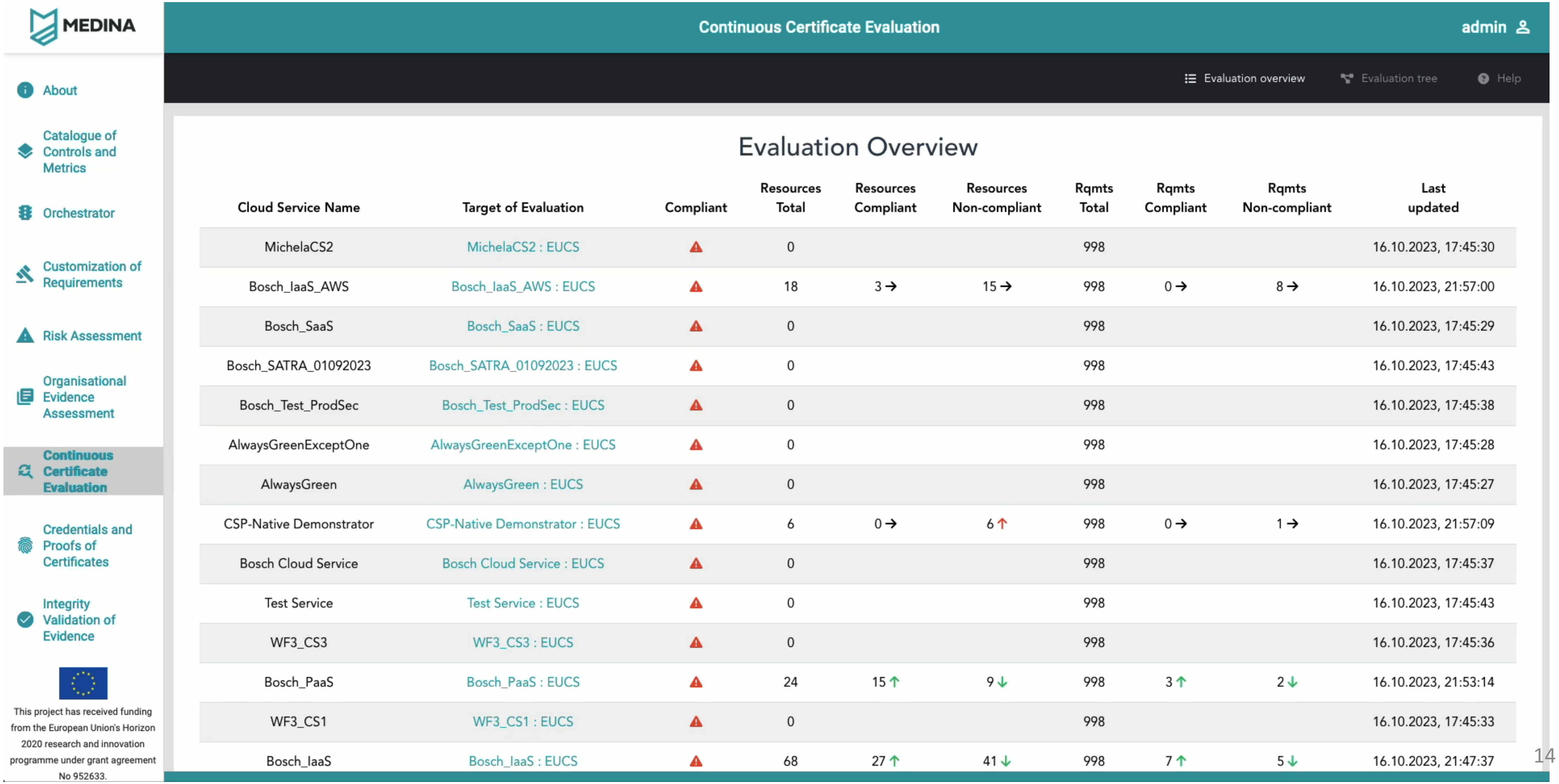
- Functionalities:
  - Automated decision making for EUCS certificates
- Input: Risk value, operational effectiveness data (updated daily for the past 3 months), timing checks
- Output:
  - Certificate status (new, continued, suspended, withdrawn, updated, renewed)

LCM: EUCS States



Integrated Demo

MEDINA


MEDINA
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation
Credentials and Proofs of Certificates
Integrity Validation of Evidence
Continuous Certificate Evaluation
admin
Evaluation overview
Evaluation tree
Help

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

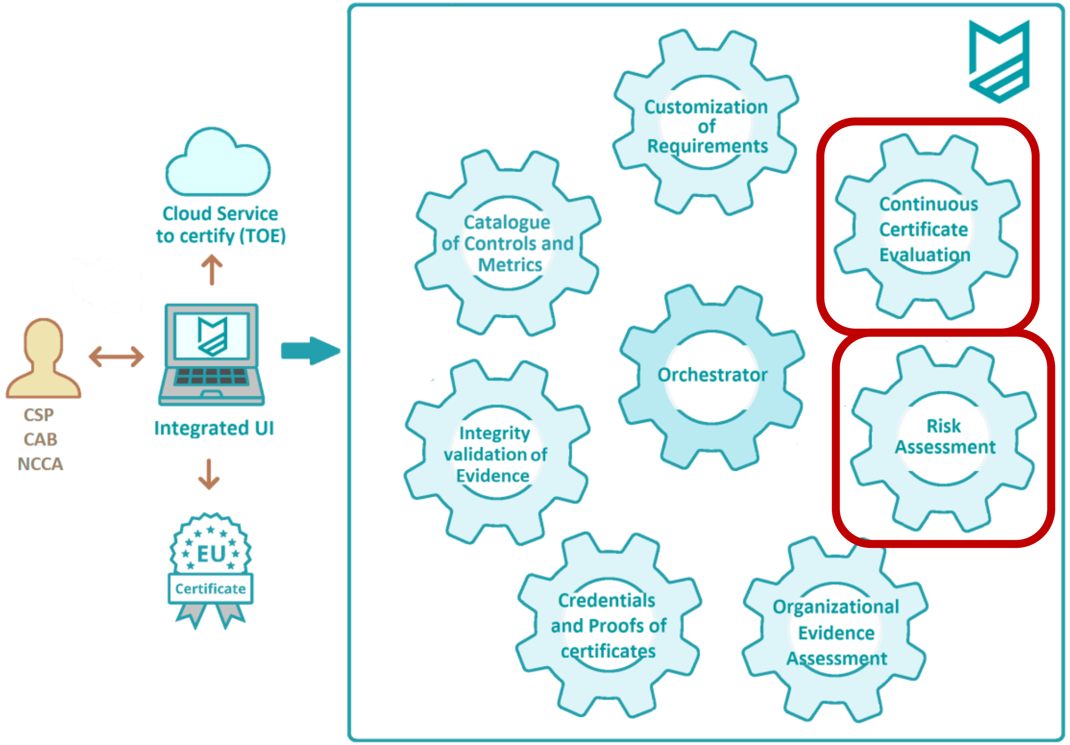
Evaluation Overview

Cloud Service Name	Target of Evaluation	Compliant	Resources Total	Resources Compliant	Resources Non-compliant	Rqmts Total	Rqmts Compliant	Rqmts Non-compliant	Last updated
MichelaCS2	MichelaCS2 : EUCS	⚠	0			998			16.10.2023, 17:45:30
Bosch_IaaS_AWS	Bosch_IaaS_AWS : EUCS	⚠	18	3 →	15 →	998	0 →	8 →	16.10.2023, 21:57:00
Bosch_SaaS	Bosch_SaaS : EUCS	⚠	0			998			16.10.2023, 17:45:29
Bosch_SATRA_01092023	Bosch_SATRA_01092023 : EUCS	⚠	0			998			16.10.2023, 17:45:43
Bosch_Test_ProdSec	Bosch_Test_ProdSec : EUCS	⚠	0			998			16.10.2023, 17:45:38
AlwaysGreenExceptOne	AlwaysGreenExceptOne : EUCS	⚠	0			998			16.10.2023, 17:45:28
AlwaysGreen	AlwaysGreen : EUCS	⚠	0			998			16.10.2023, 17:45:27
CSP-Native Demonstrator	CSP-Native Demonstrator : EUCS	⚠	6	0 →	6 ↑	998	0 →	1 →	16.10.2023, 21:57:09
Bosch Cloud Service	Bosch Cloud Service : EUCS	⚠	0			998			16.10.2023, 17:45:37
Test Service	Test Service : EUCS	⚠	0			998			16.10.2023, 17:45:43
WF3_CS3	WF3_CS3 : EUCS	⚠	0			998			16.10.2023, 17:45:36
Bosch_PaaS	Bosch_PaaS : EUCS	⚠	24	15 ↑	9 ↓	998	3 ↑	2 ↓	16.10.2023, 21:53:14
WF3_CS1	WF3_CS1 : EUCS	⚠	0			998			16.10.2023, 17:45:33
Bosch_IaaS	Bosch_IaaS : EUCS	⚠	68	27 ↑	41 ↓	998	7 ↑	5 ↓	16.10.2023, 21:47:37

CCE
RAOF
LCM

- Installation
  - Deployment
  - Technical Specifications

MEDINA



CSP
CAB
NCCA

Cloud Service to certify (TOE)

Integrated UI

EU Certificate

Customization of Requirements

Catalogue of Controls and Metrics

Continuous Certificate Evaluation

Orchestrator

Integrity validation of Evidence

Risk Assessment

Credentials and Proofs of certificates

Organizational Evidence Assessment

Installation

MEDINA

Installation and Deployment

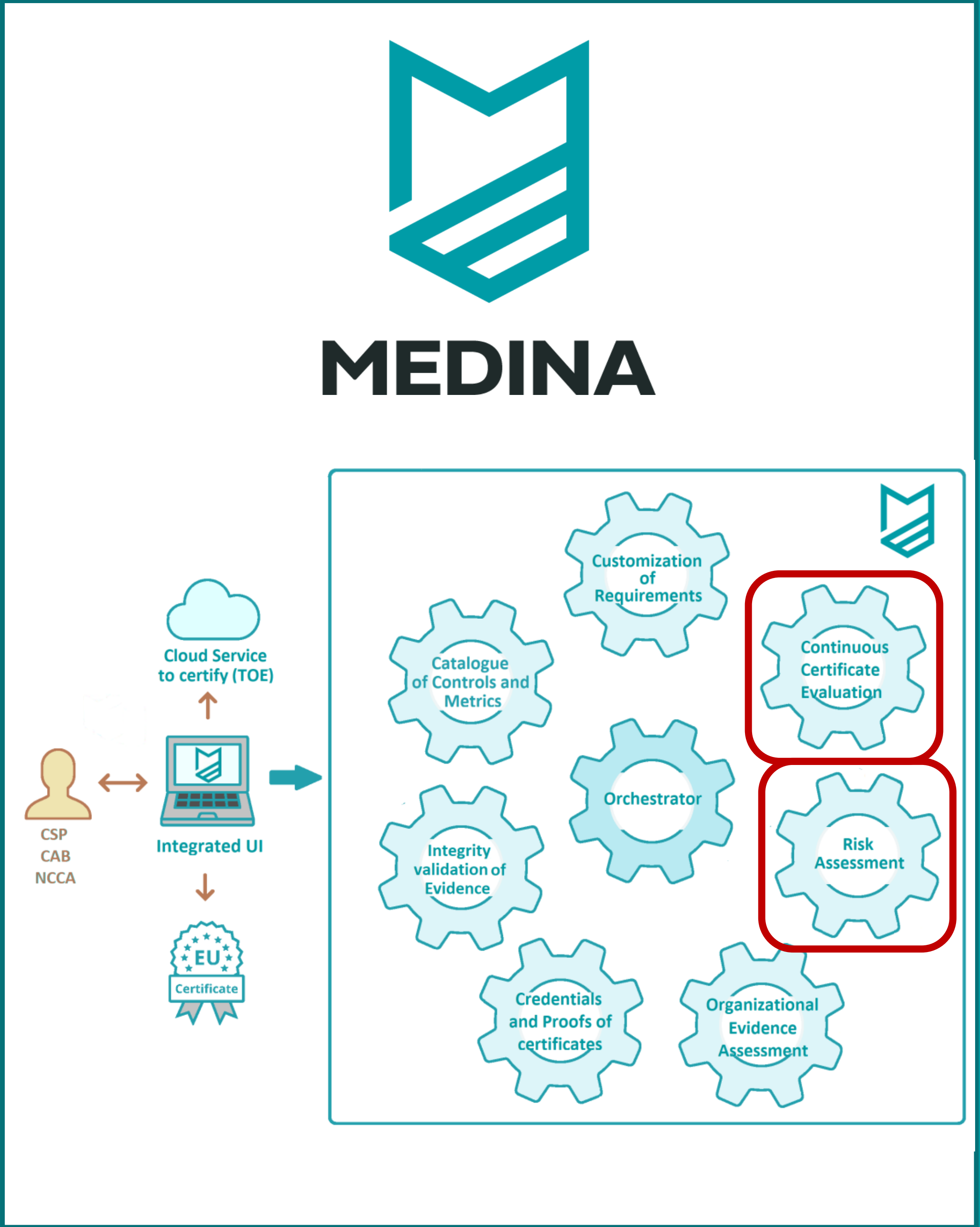
- Docker images. The configuration options for starting the containers are described in the README files:
  - https://git.code.tecnalia.com/medina/public/continuous-certification-evaluation, https://git.code.tecnalia.com/medina/public/cce-frontend
  - https://git.code.tecnalia.com/medina/public/static-risk-assessment-and-optimization-framework
  - https://git.code.tecnalia.com/medina/public/life-cycle-manager

Technical specifications

- CCE: Java & Spring Boot; Javascript / Vue Front-end; MongoDB
- RAOF: Java, Python, MySQL
- LCM: Go

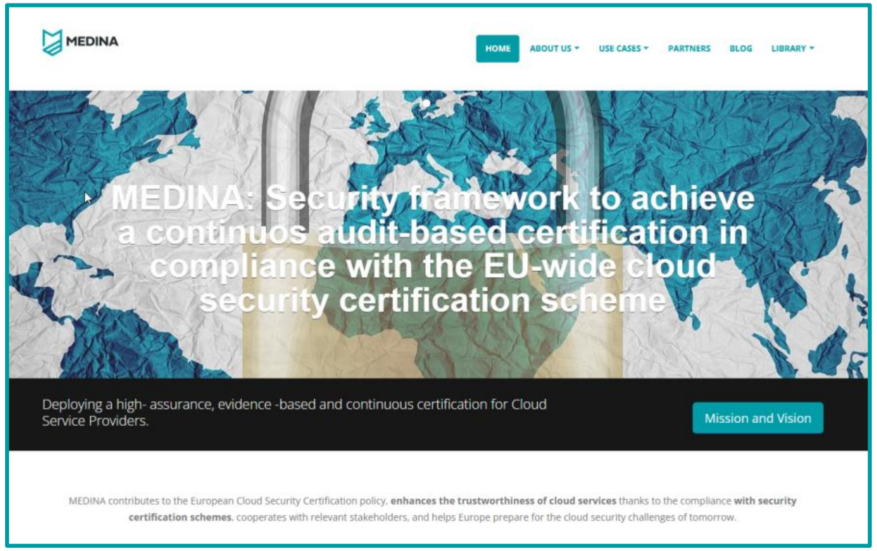
CCE
RAOF
LCM

- Further information


MEDINA
Cloud Service
to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** https://medina-project.eu/public-deliverables
- Framework demonstrator is available in the MEDINA **YouTube channel** https://www.youtube.com/@MedinaprojectEU
- MEDINA Community in **Zenodo** https://zenodo.org/communities/medina
- Source code in the public **GitLab** https://git.code.tecnalia.com/medina/public



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

NIXU cybersecurity.

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

MEDINA

Credentials and Proofs of certificates

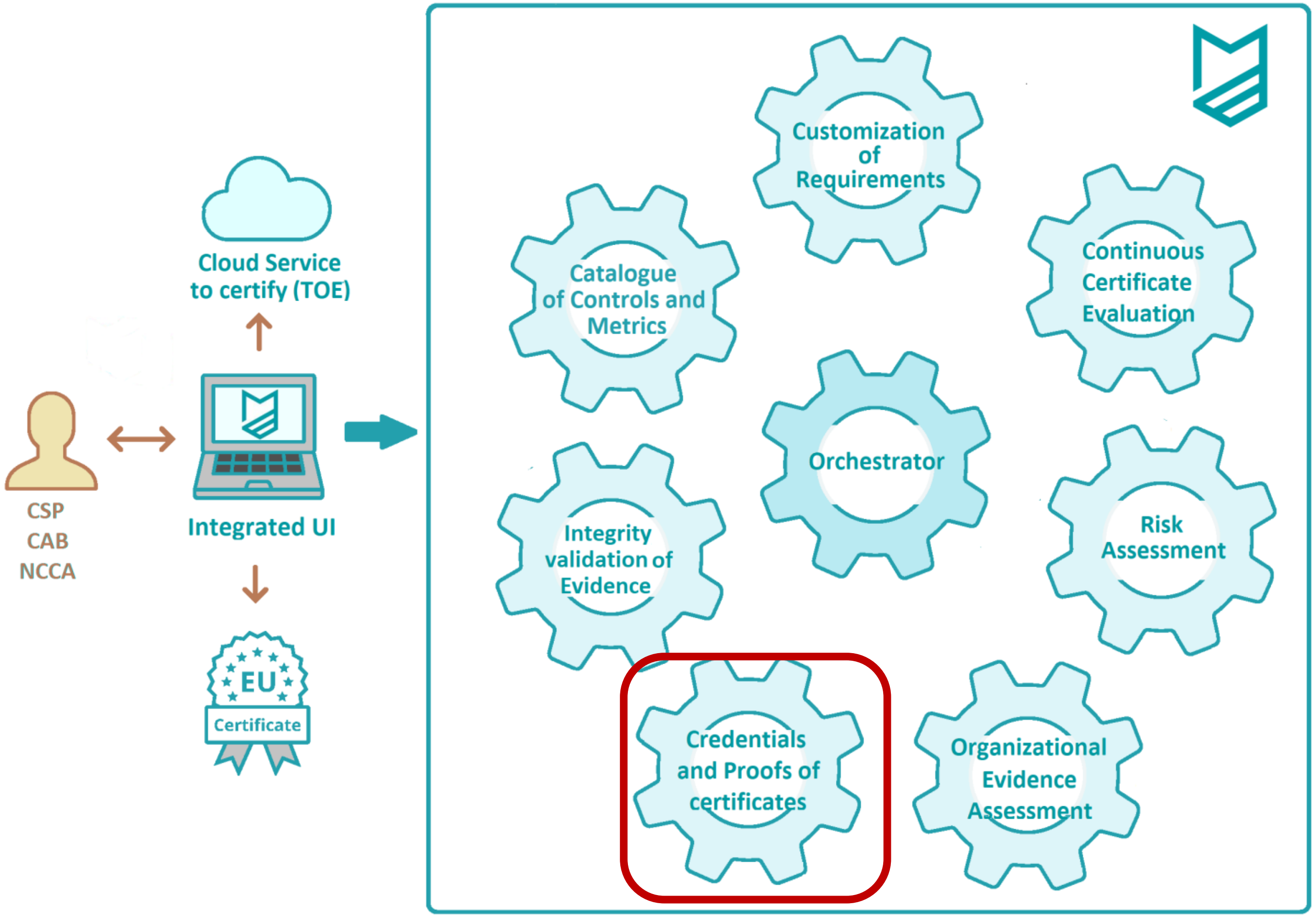
TECNALIA

September 2023

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

Chapters

- Overview
- How to use it
- Installation
- Further information

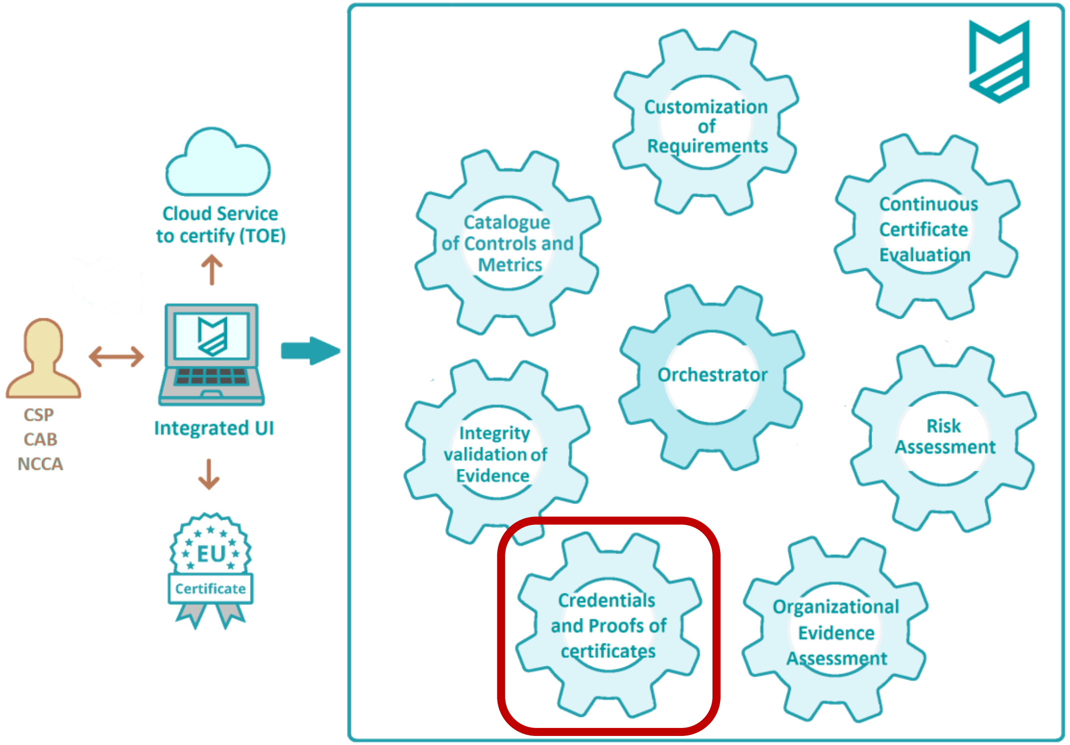


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Credentials and Proofs of certificates

- Overview
  - Purpose
  - Role in MEDINA Architecture

MEDINA

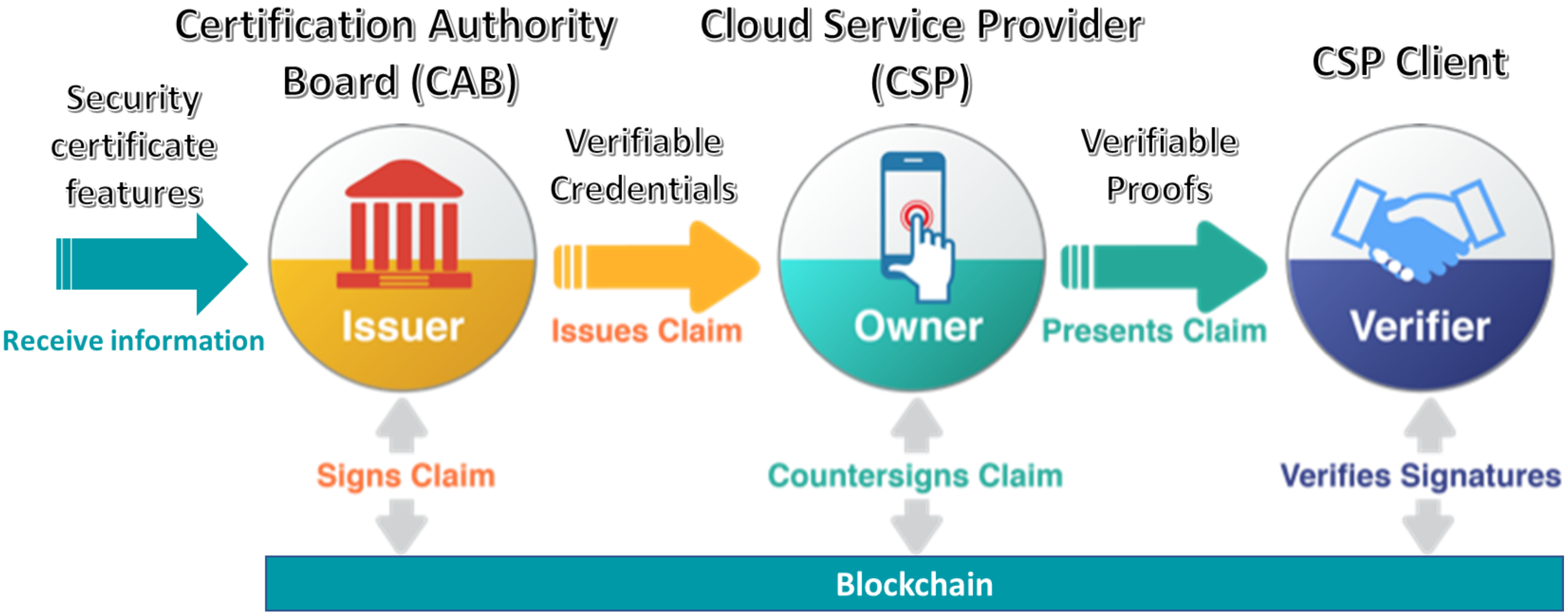

Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Credentials and Proofs of certificates

- **Self Sovereign Identity (SSI)** is a novel model for managing digital identities in which individuals have sole ownership over the ability to control their personal data.
- **Digital identities are created** through **verifiable credentials**. They are tamper-evident credentials that have authorship that can be cryptographically verified.
- **Digital identities are proved** through **verifiable proofs** based on the verifiable credentials.

Credentials and Proofs of certificates

MEDINA SSI Framework component



Credentials and Proofs of certificates

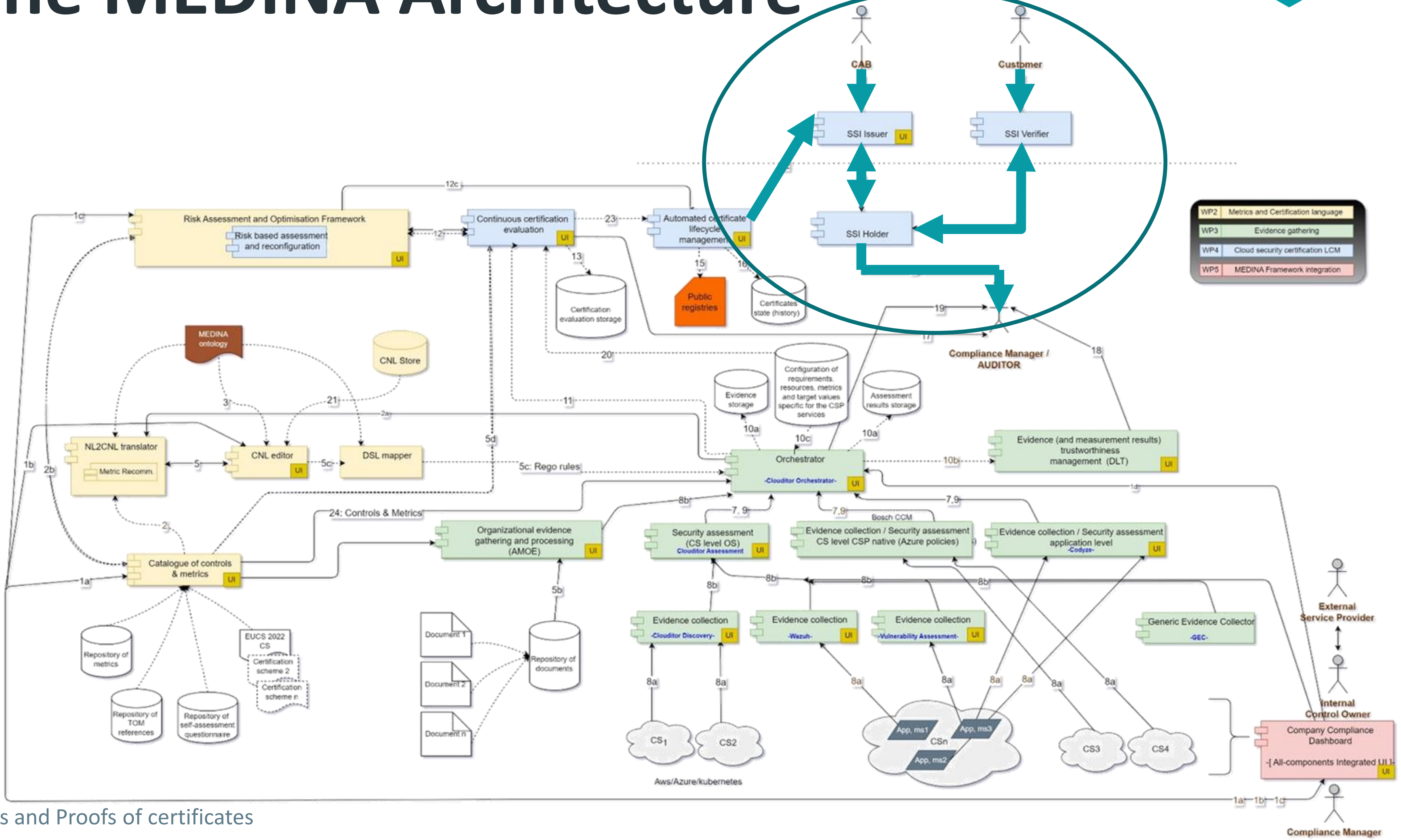
- **Issuer:** Provides the **CAB** a way to **issue verifiable credentials about the security certificates related to the CSPs.**
- **Owner:** Provides **CSPs** with the capability to **manage their own security certificates** as part of their identity through verifiable credentials.
- **Verifier:** Provides a way for **CSPs' customers** to **ask and verify proofs** of different security certificates features.

Credentials and Proofs of certificates

- The **Credentials and Proofs of certificates** is enhanced with some extra features:

  1. User-friendly graphical interface.
  2. Security by design (Blockchain as secure storage).
  3. Automatic operation for CSPs.
  4. Easy to integrate (REST API).
  5. Easy to be extended in terms of security certificates features.

Credentials and Proofs of certificates in the MEDINA Architecture


CAB
Customer
SSI Issuer
UI
SSI Verifier
SSI Holder
WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
Continuous certification evaluation
Automated certificate lifecycle management
12c
12
23
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
20
MEDINA ontology
CNL Store
3
21
2a
11
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5
5c
5d
5c: Rego rules
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
10a
10c
Orchestrator
-Clouditor Orchestrator-
10b
Evidence (and measurement results) trustworthiness management (DLT)
1d
1c
1b
2b
2
24: Controls & Metrics
8b
7, 9
7,9
Bosch CCM
Catalogue of controls & metrics
1a
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
5b
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
Generic Evidence Collector
-GEC-
External Service Provider
Internal Control Owner
8a
CS1
CS2
Aws/Azure/kubernetes
App, ms1
App, ms3
App, ms2
CSn
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
Compliance Manager

Interactions with other components

Lifecycle Manager (LCM)

- Provides the updated security certificate features (cloud service ID, certificate status).

Certification Authority Board (CAB)

- Issues security certificates to CSPs based on received features from LCM through verifiable credentials.

Compliance Manager/Auditor

- Consults the security certificate features of the CSP.

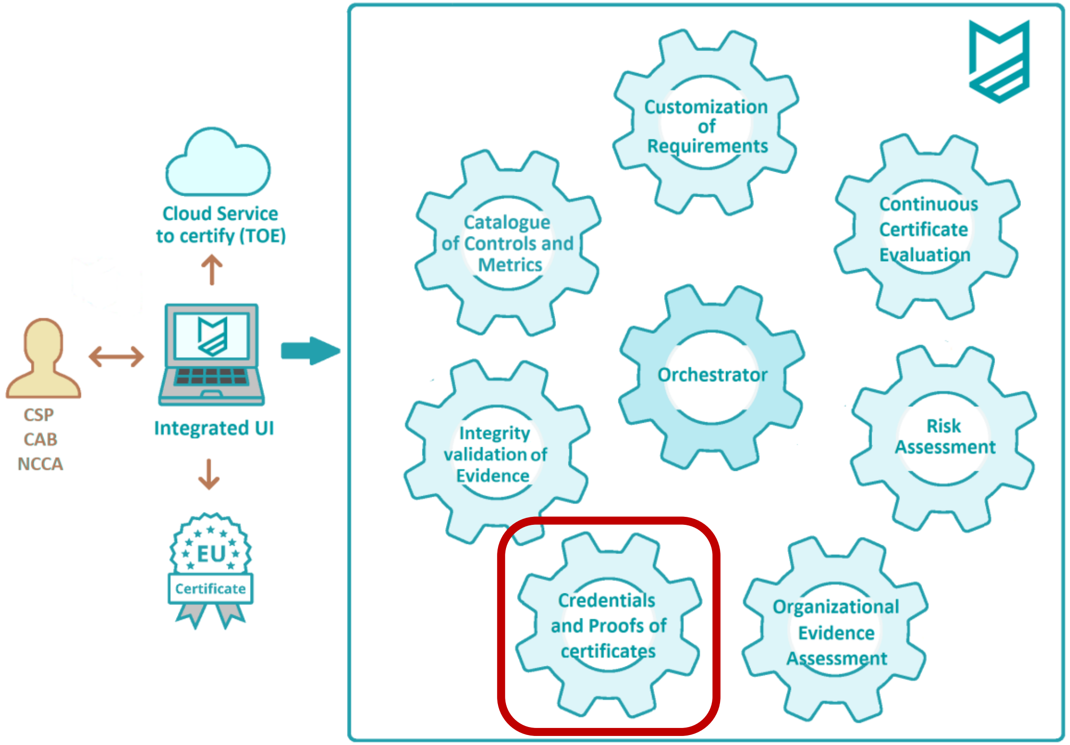
CSP Customer

- Requests the CSP Verifiable proofs of the security certificate features.
- Verifies and validates the received verifiable proofs.

Credentials and Proofs of certificates

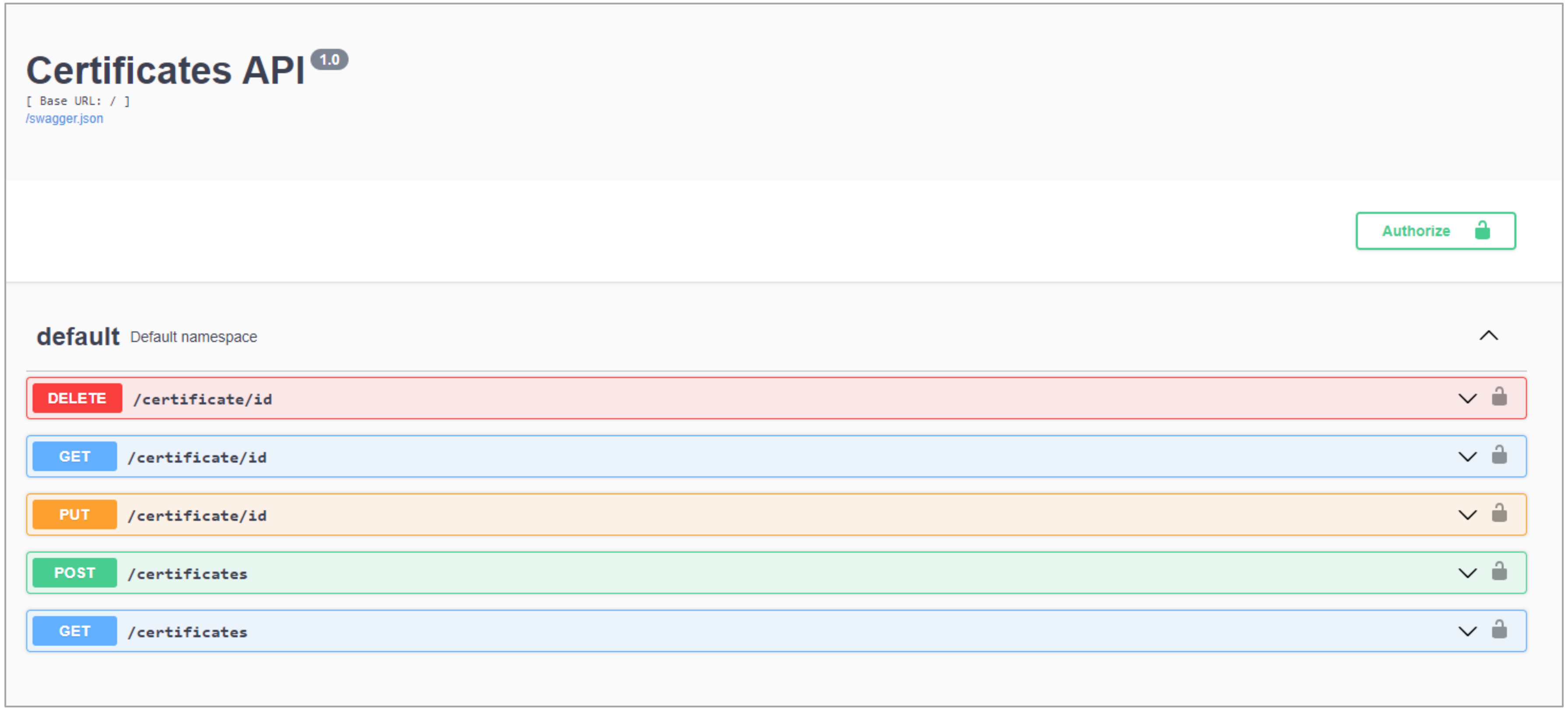
- ➤ How to use it
  - - Functionalities
  - - Demo

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Functionalities

- REST API for providing the security certificate features.



Certificates API 1.0

[Base URL: /]

/swagger.json

default Default namespace

DELETE /certificate/id

GET /certificate/id

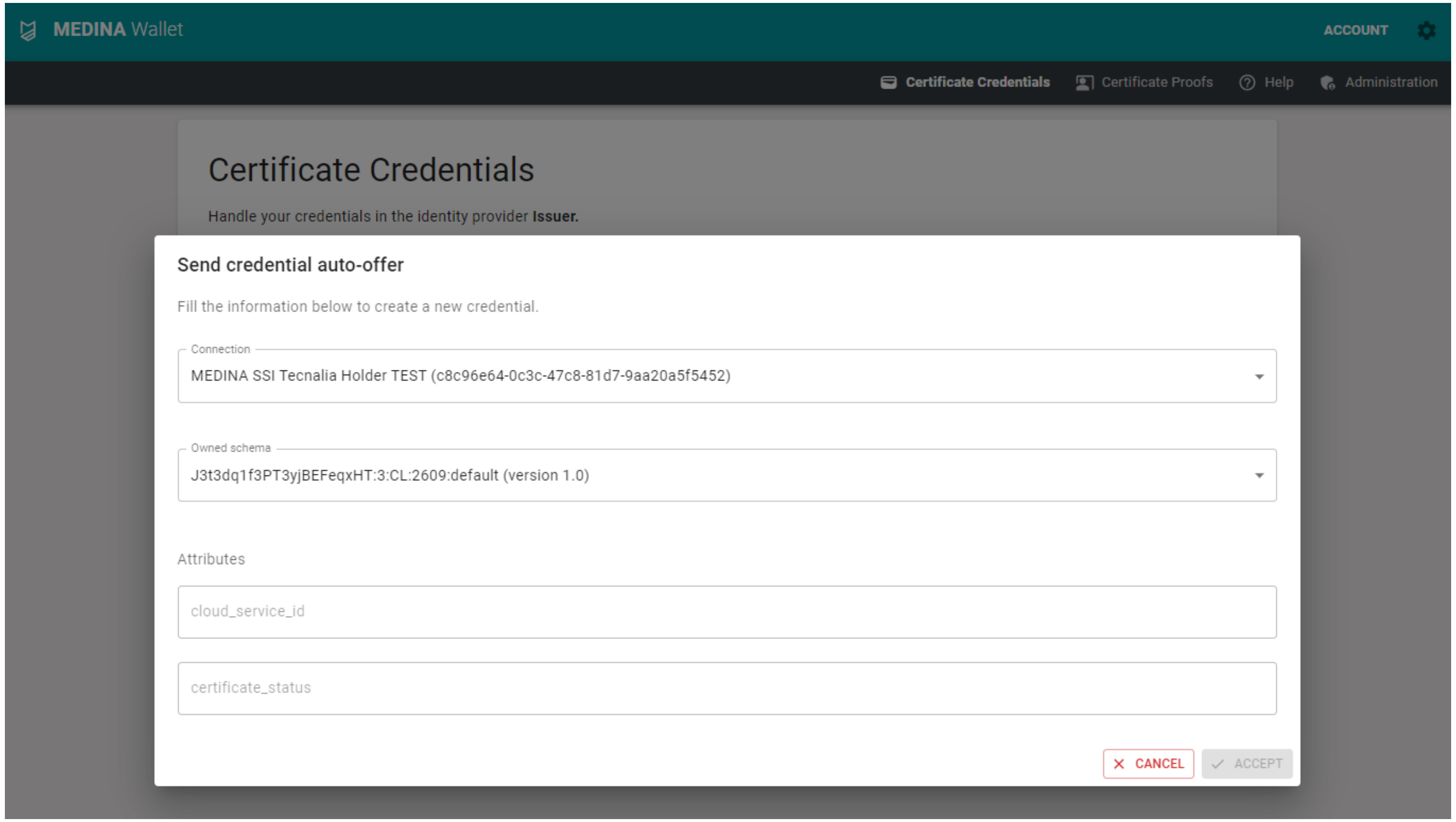
PUT /certificate/id

POST /certificates

GET /certificates

Functionalities

- Tool for appropriate entities (CABs) to issue/update/revoke and sign security certifications for the cloud providers.



Certificate Credentials

Handle your credentials in the identity provider **Issuer.**

Send credential auto-offer

Fill the information below to create a new credential.

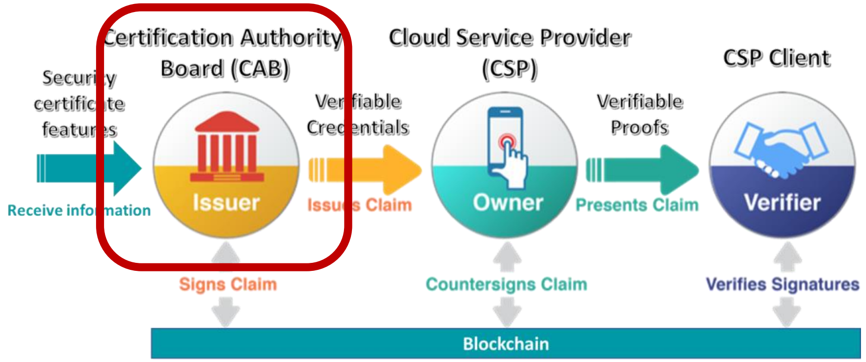
Connection: MEDINA SSI Tecnalia Holder TEST (c8c96e64-0c3c-47c8-81d7-9aa20a5f5452)

Owned schema: J3t3dq1f3PT3yjBEFeqxHT:3:CL:2609:default (version 1.0)

Attributes

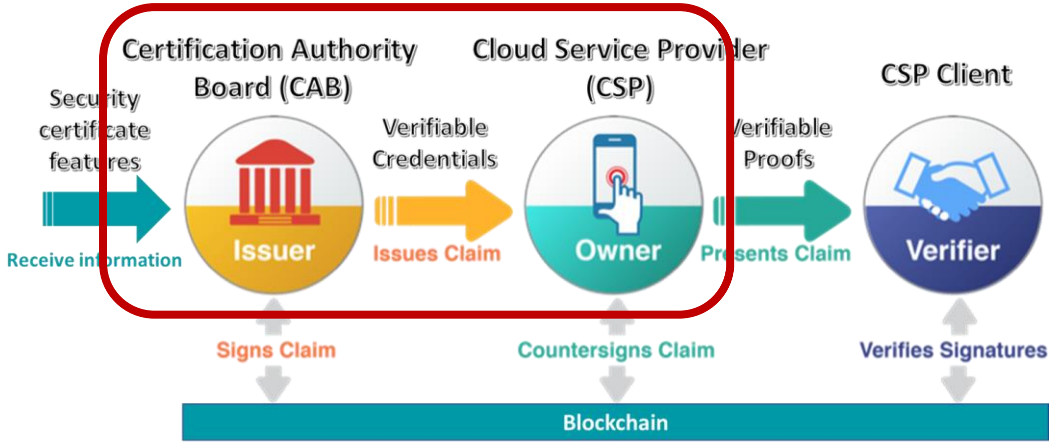
cloud_service_id

certificate_status



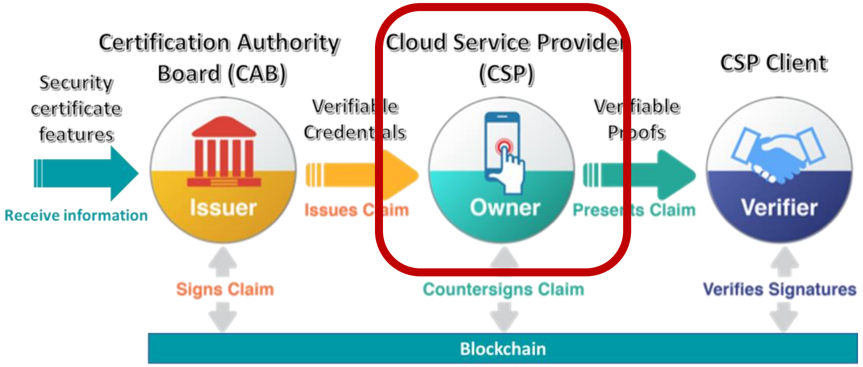
Credentials and Proofs of certificates – Certificate Issuance

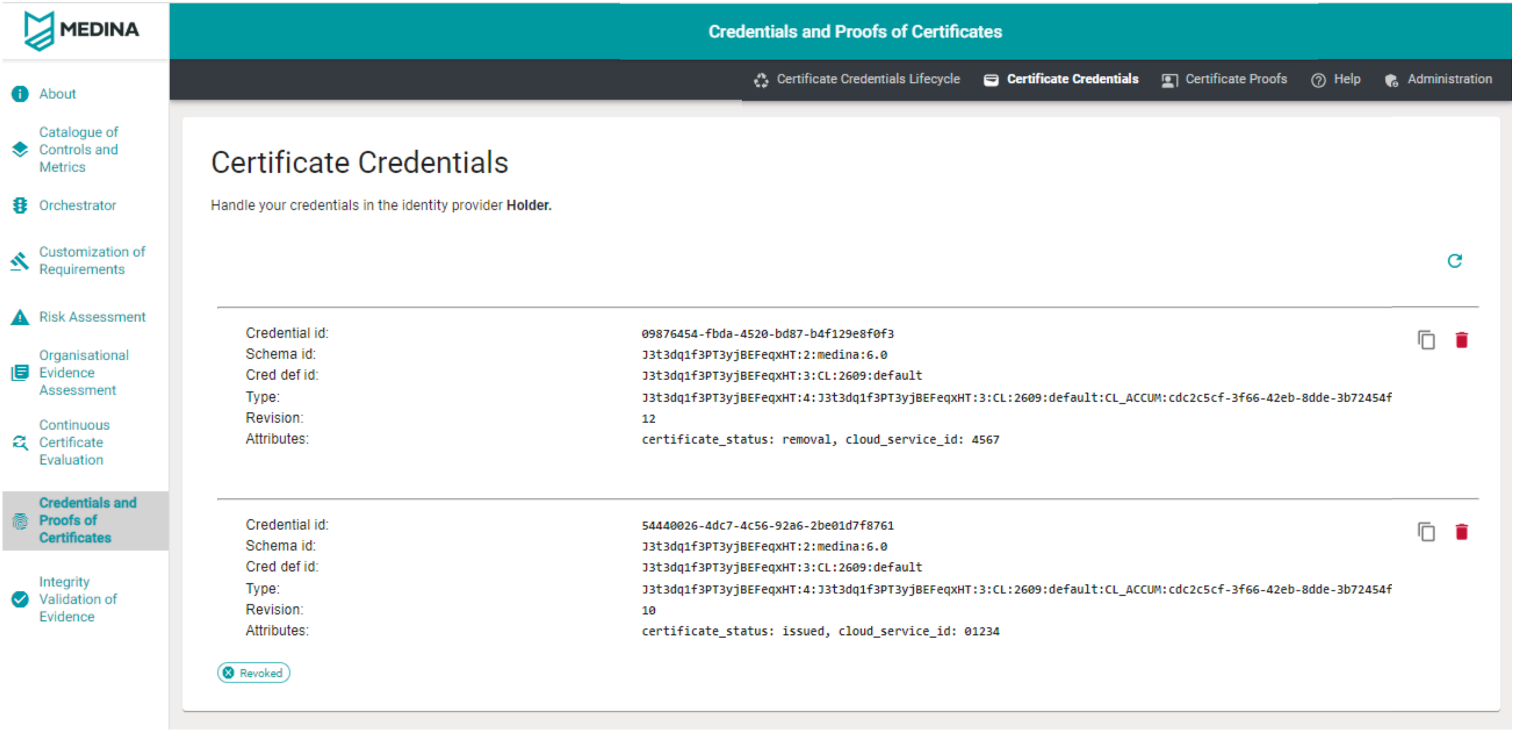
- DEMO -



Functionalities

- Tool for cloud providers to see/list received certifications and their associated state.





MEDINA
Credentials and Proofs of Certificates
Certificate Credentials Lifecycle
Certificate Credentials
Certificate Proofs
Help
Administration
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation
Credentials and Proofs of Certificates
Integrity Validation of Evidence
Revoked

Certificate Credentials

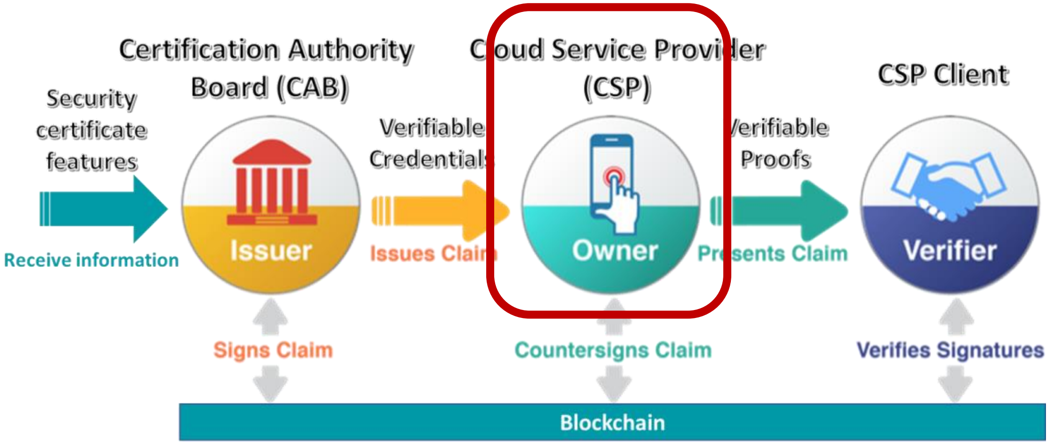
Handle your credentials in the identity provider **Holder.**

```
Credential id:   09876454-fbda-4520-bd87-b4f129e8f0f3
Schema id:       J3t3dq1f3PT3yjBEFeqxHT:2:medina:6.0
Cred def id:     J3t3dq1f3PT3yjBEFeqxHT:3:CL:2609:default
Type:            J3t3dq1f3PT3yjBEFeqxHT:4:J3t3dq1f3PT3yjBEFeqxHT:3:CL:2609:default:CL_ACCUM:cdc2c5cf-3f66-42eb-8dde-3b72454f
Revision:        12
Attributes:      certificate_status: removal, cloud_service_id: 4567
```

```
Credential id:   54440026-4dc7-4c56-92a6-2be01d7f8761
Schema id:       J3t3dq1f3PT3yjBEFeqxHT:2:medina:6.0
Cred def id:     J3t3dq1f3PT3yjBEFeqxHT:3:CL:2609:default
Type:            J3t3dq1f3PT3yjBEFeqxHT:4:J3t3dq1f3PT3yjBEFeqxHT:3:CL:2609:default:CL_ACCUM:cdc2c5cf-3f66-42eb-8dde-3b72454f
Revision:        10
Attributes:      certificate_status: issued, cloud_service_id: 01234
```

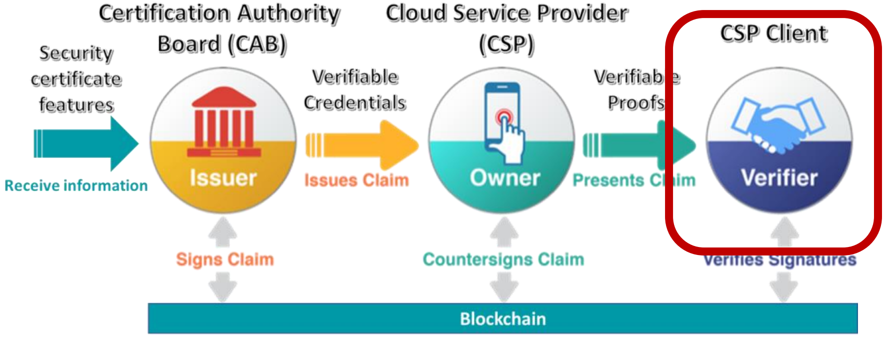
Credentials and Proofs of certificates – Certificate List

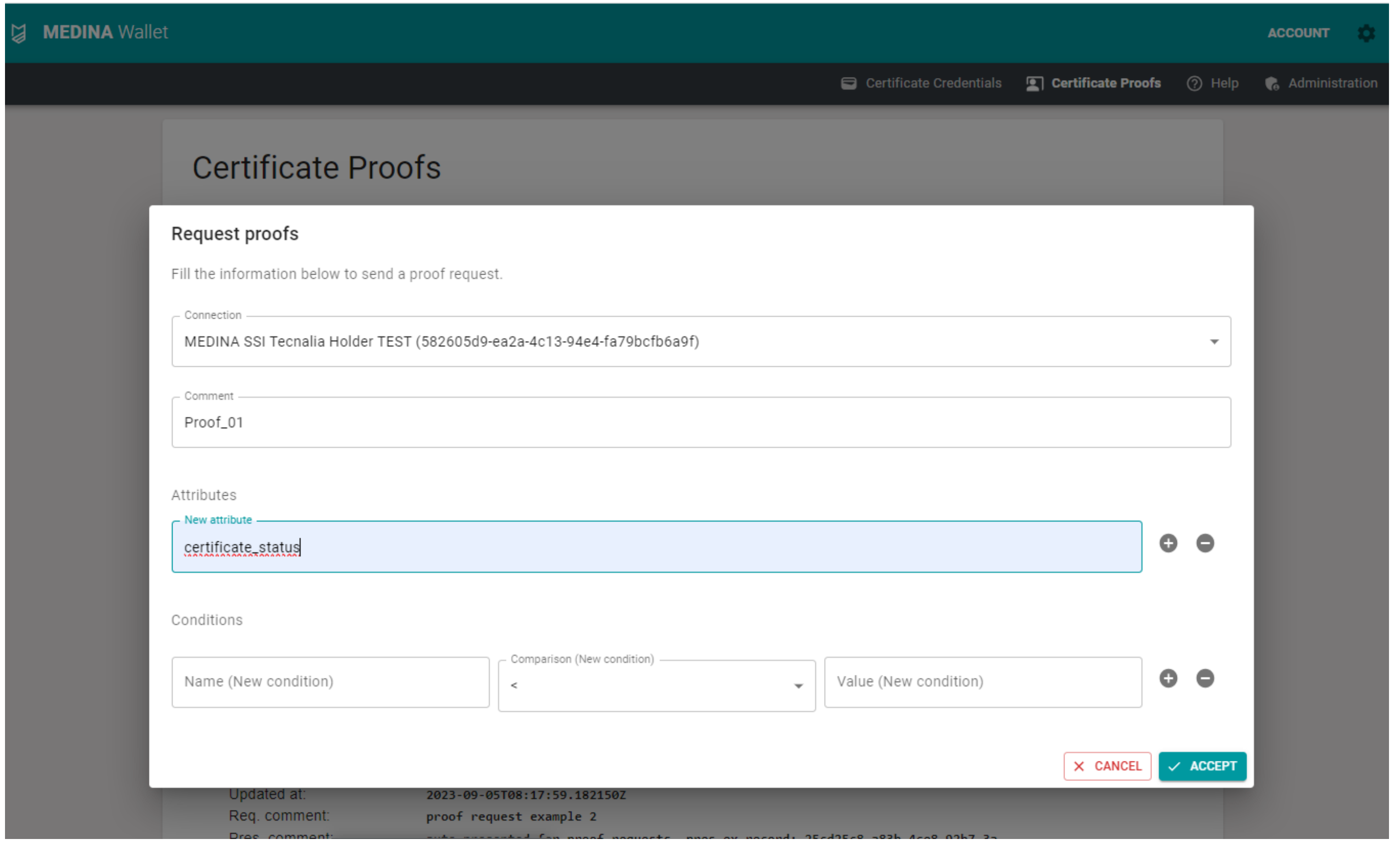
- DEMO -



Functionalities

- Tool for appropriate entities (for example, cloud providers’ clients) to ask for proofs about the state of different certifications of the cloud providers.





Certificate Proofs

Request proofs

Fill the information below to send a proof request.

Connection: MEDINA SSI Tecnalia Holder TEST (582605d9-ea2a-4c13-94e4-fa79bcfb6a9f)

Comment: Proof_01

Attributes

New attribute: certificate_status

Conditions

Name (New condition) | Comparison (New condition): < | Value (New condition)

CANCEL ACCEPT

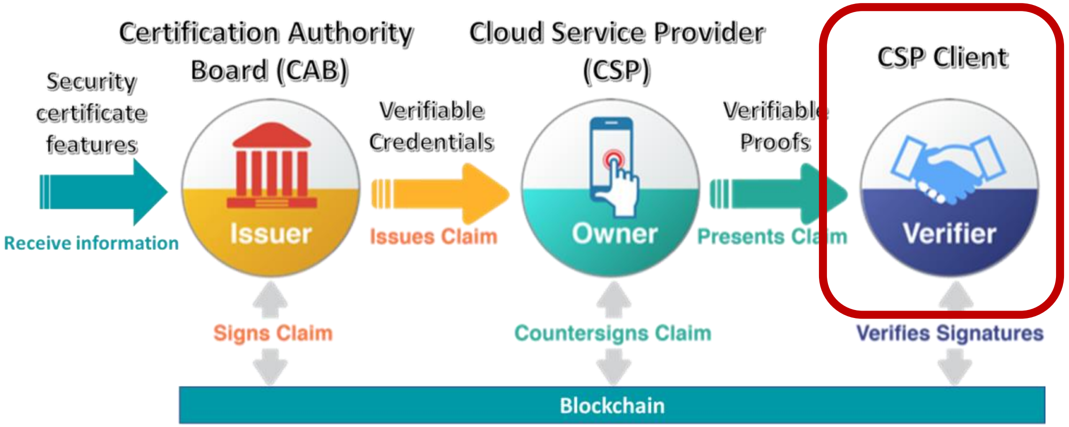
Updated at: 2023-09-05T08:17:59.182150Z

Req. comment: proof request example 2

Pres. comment: auto-presented for proof requests, pres_ex_record: 25cd25c8-a83b-4ce8-92b7-3a

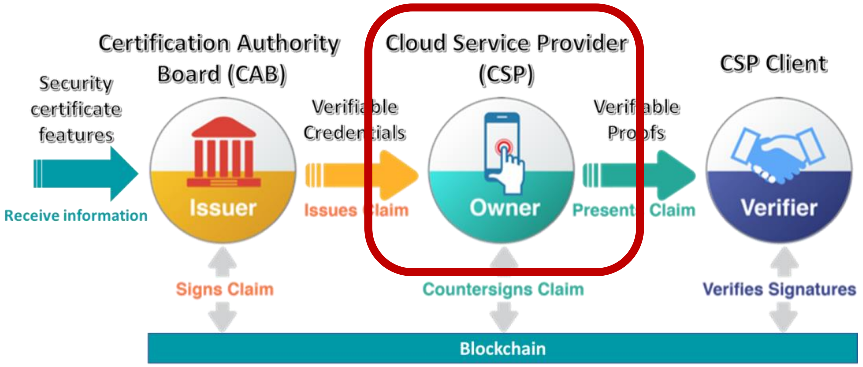
Credentials and Proofs of certificates – Certificate Proof Request

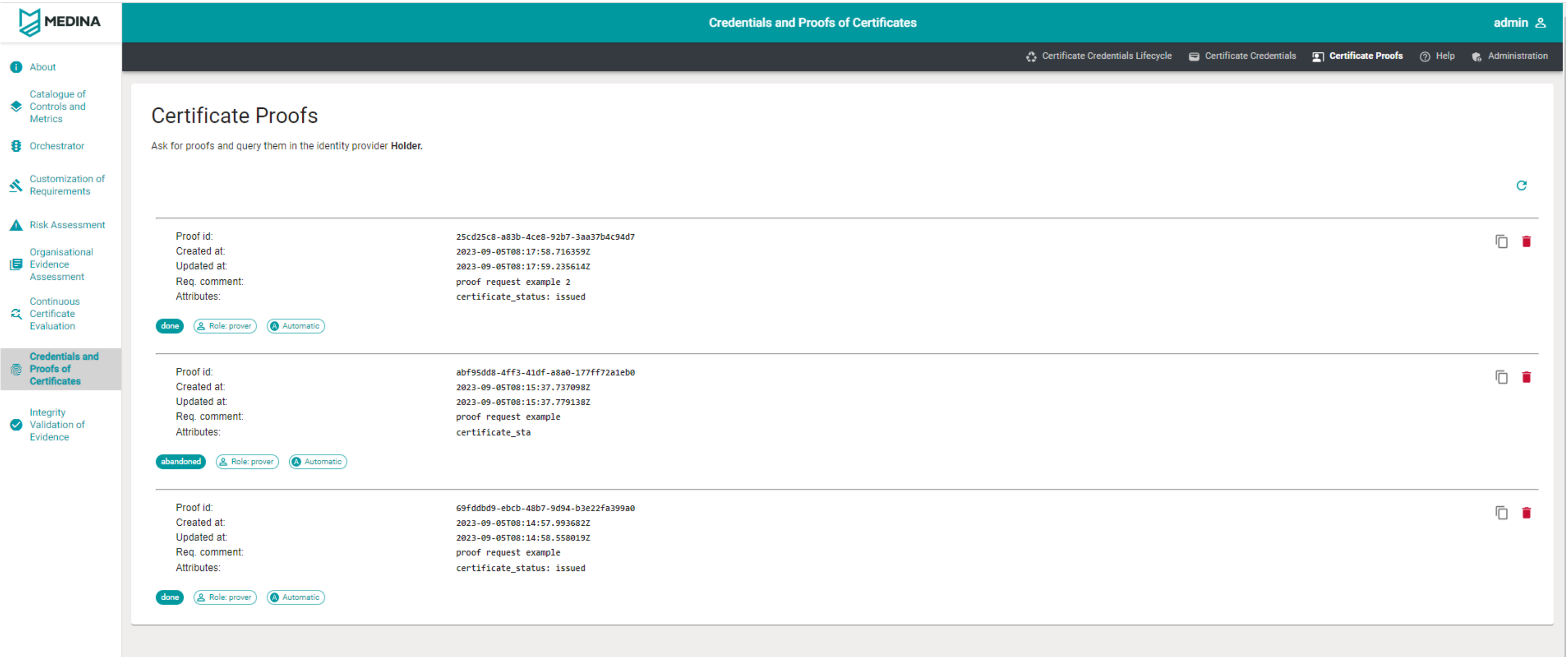
- DEMO -



Functionalities

- Tool for cloud providers to send proofs about the certificate state to their clients.





MEDINA
Credentials and Proofs of Certificates
admin
Certificate Credentials Lifecycle
Certificate Credentials
Certificate Proofs
Help
Administration
About
Catalogue of Controls and Metrics
Orchestrator
Customization of Requirements
Risk Assessment
Organisational Evidence Assessment
Continuous Certificate Evaluation
Credentials and Proofs of Certificates
Integrity Validation of Evidence

Certificate Proofs

Ask for proofs and query them in the identity provider **Holder.**

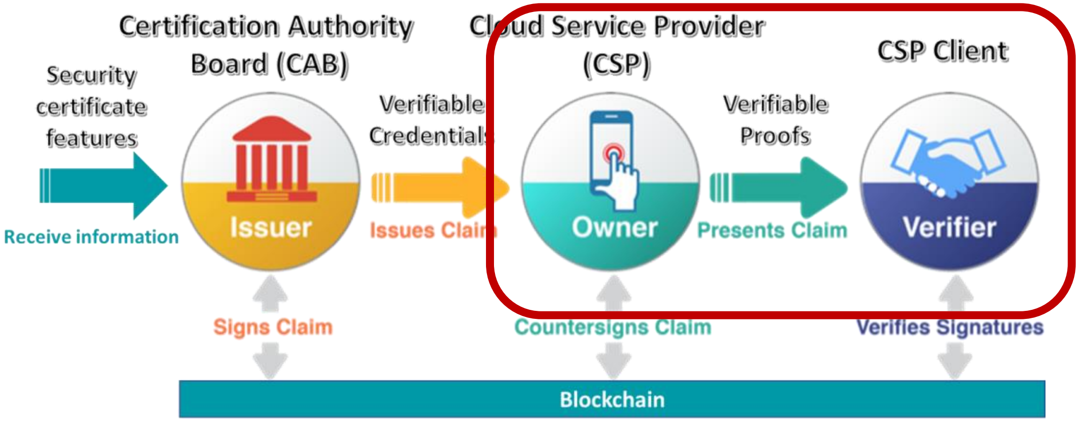
```
Proof id:        25cd25c8-a83b-4ce8-92b7-3aa37b4c94d7
Created at:      2023-09-05T08:17:58.716359Z
Updated at:      2023-09-05T08:17:59.235614Z
Req. comment:    proof request example 2
Attributes:      certificate_status: issued
done   Role: prover   Automatic

Proof id:        abf95dd8-4ff3-41df-a8a0-177ff72a1eb0
Created at:      2023-09-05T08:15:37.737098Z
Updated at:      2023-09-05T08:15:37.779138Z
Req. comment:    proof request example
Attributes:      certificate_sta
abandoned   Role: prover   Automatic

Proof id:        69fddbd9-ebcb-48b7-9d94-b3e22fa399a0
Created at:      2023-09-05T08:14:57.993682Z
Updated at:      2023-09-05T08:14:58.558019Z
Req. comment:    proof request example
Attributes:      certificate_status: issued
done   Role: prover   Automatic
```

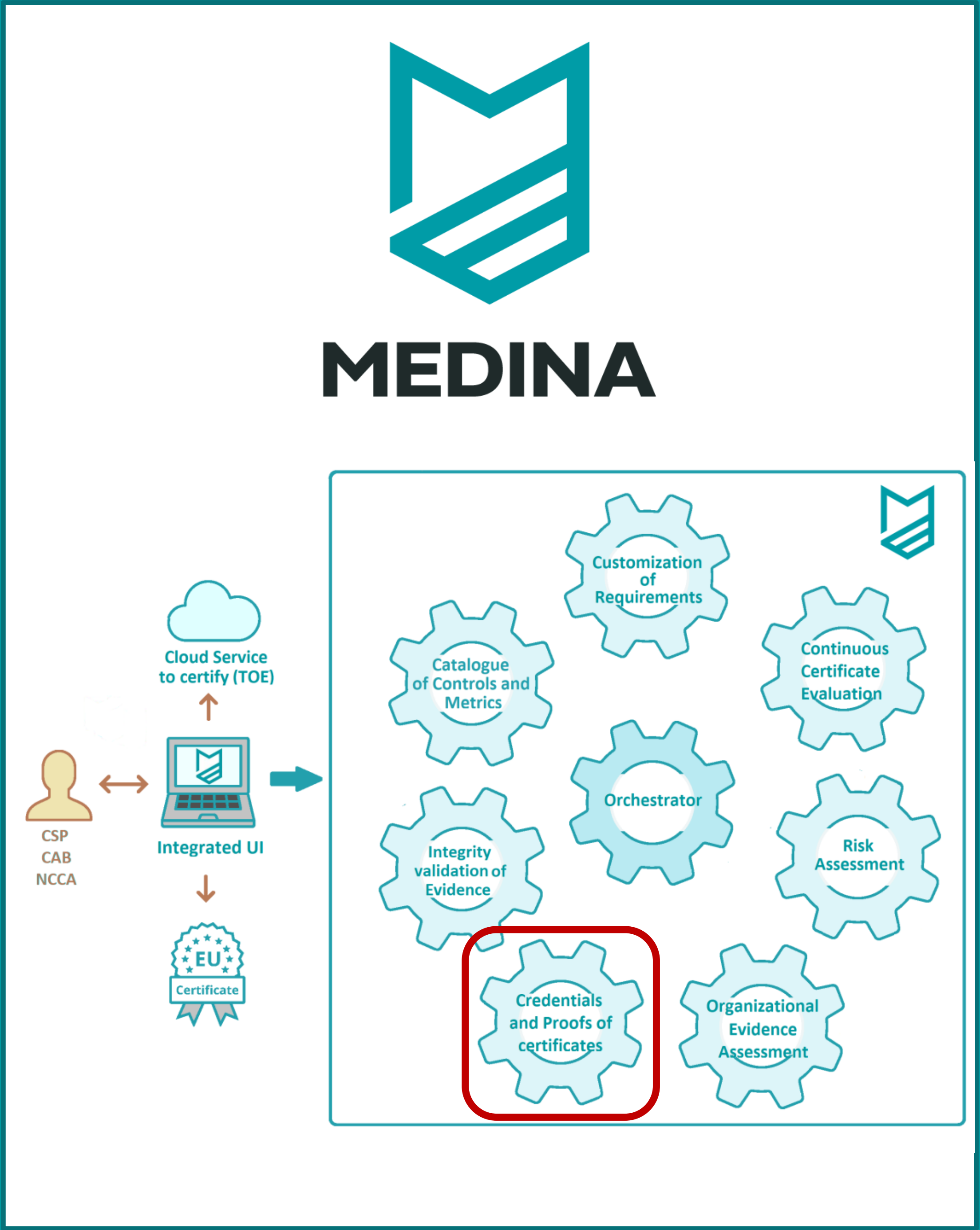
Credentials and Proofs of certificates - Certificate Proof Response and Validation

- DEMO -



Credentials and Proofs of certificates

- ➤ Installation
  - - Deployment
  - - Technical Specifications

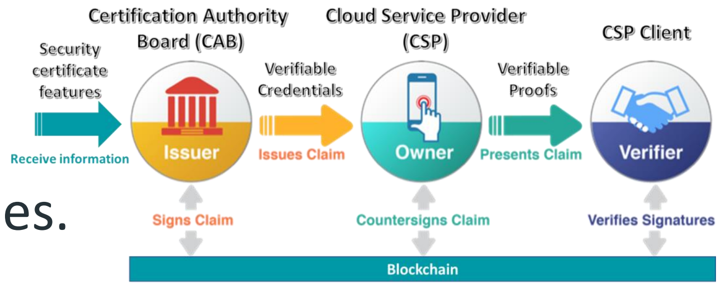

MEDINA
Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

Deployment

- **Issuer is provided as a service** by TECNALIA for validation purposes.

- **Owner can be locally deployed**:
  - Login MEDINA artifact:
    - ***sudo docker login optima-medina-docker-dev.artifact.tecnalia.com*** *(enter your username and password; registration in Orein is needed in advance)*
  - Pull the Docker image:
    - ***sudo docker pull optima-medina-docker-dev.artifact.tecnalia.com/wp4/t43/ssi-framework-ui-test:2.0.1***
  - Run the Docker image:
    - ***sudo docker run -d -p 8080:8080 –name medina_ssi_webapp optima-medina-docker-dev.artifact.tecnalia.com/wp4/t43/ssi-framework-ui-test:2.0.1***
  - The Owner component will be available at https://localhost:8080/

- **Verifier is provided as a service** by TECNALIA for validation purposes.



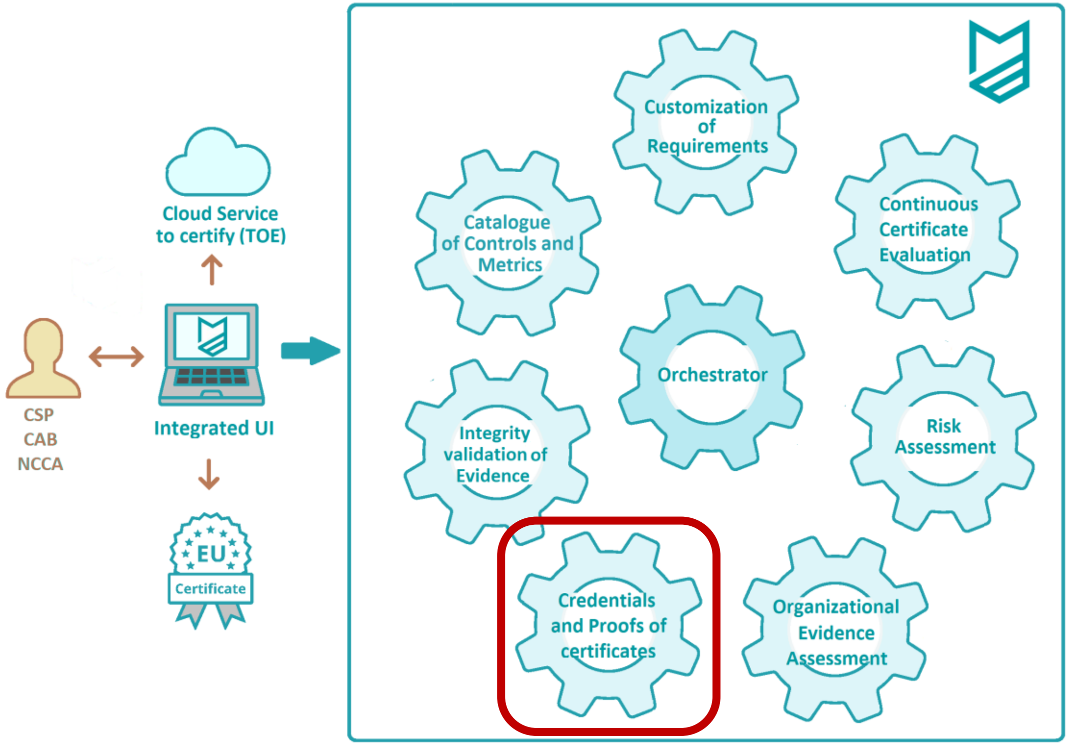
Installation

- Technical specifications
  - Hyperledger Indy as Blockchain technology.
  - Hyperledger Aries as backend.
  - API developed in Python.
  - Frontend developed with React framework.
  - Docker for installation.

Credentials and Proofs of certificates

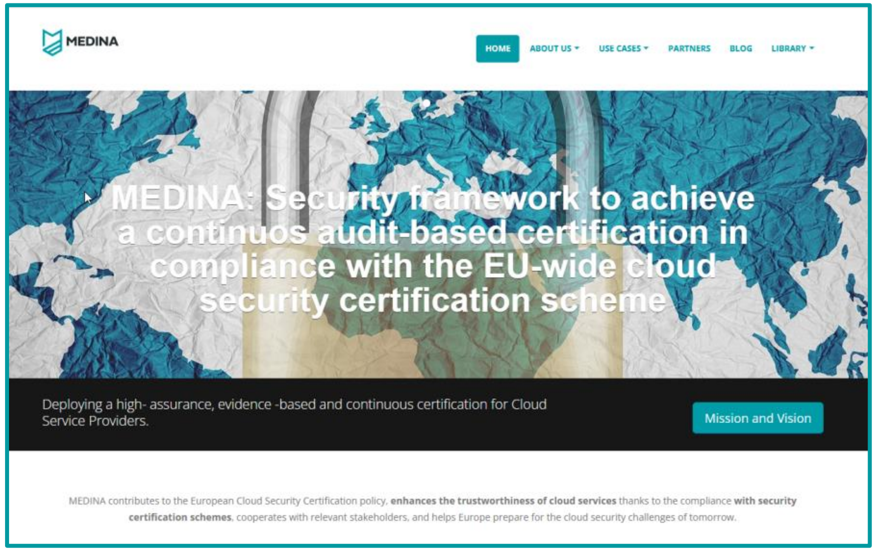
- ➤ Further information

MEDINA


Cloud Service to certify (TOE)
CSP
CAB
NCCA
Integrated UI
EU
Certificate
Customization of Requirements
Catalogue of Controls and Metrics
Continuous Certificate Evaluation
Orchestrator
Integrity validation of Evidence
Risk Assessment
Credentials and Proofs of certificates
Organizational Evidence Assessment

MEDINA – Further Reading

- Further details are available in our public reporting (deliverables) at the **MEDINA web** *https://medina-project.eu/public-deliverables*
- Framework demonstrator is available in the MEDINA **YouTube channel** *https://www.youtube.com/@MedinaprojectEU*
- MEDINA Community in **Zenodo** *https://zenodo.org/communities/medina*
- Source code in the public **GitLab** *https://git.code.tecnalia.com/medina/public*



MEDINA: Security framework to achieve a continuos audit-based certification in compliance with the EU-wide cloud security certification scheme

Deploying a high- assurance, evidence -based and continuous certification for Cloud Service Providers.

MEDINA contributes to the European Cloud Security Certification policy, **enhances the trustworthiness of cloud services** thanks to the compliance **with security certification schemes**, cooperates with relevant stakeholders, and helps Europe prepare for the cloud security challenges of tomorrow.

MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

www.medina-project.eu

@MedinaprojectEU

MEDINA Project - Continuous cloud security certification

@MedinaprojectEU

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer
AISEC

Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

BOSCH

Fabasoft®

XLAB

nixu cybersecurity.

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