



# MEDINA

## Deliverable D7.3

### Market, Innovation and Applicability Analysis

<b>Editor(s):</b>	Simo Opara, Mika Leskinen
<b>Responsible Partner:</b>	NIXU
<b>Status-Version:</b>	V2.0
<b>Date:</b>	24.12.2021
<b>Distribution level (CO, PU):</b>	PU (Public)

<b>Project Number:</b>	952633
<b>Project Title:</b>	MEDINA

<b>Title of Deliverable:</b>	Market, Innovation and Applicability Analysis
<b>Due Date of Delivery to the EC</b>	30.4.2021

<b>Work package responsible for the Deliverable:</b>	WP7 – Awareness, Training and Sustainability
<b>Editor(s):</b>	NIXU
<b>Contributor(s):</b>	Juncal Alonso (TECNALIA), Leire Orue-Echevarria (TECNALIA), Artsiom Yautsiukhin (CNR), Jesus Luna Garcia (Bosch), Marinella Petrocchi (CNR), Immanuel Kuntz (Fraunhofer)
<b>Reviewer(s):</b>	Iñaki Etxaniz and Leire Orue-Echevarria (TECNALIA)
<b>Approved by:</b>	All Partners
<b>Recommended/mandatory readers:</b>	WP2-WP3-WP4-WP5-WP6

<b>Abstract:</b>	This document reports surveys and analysis about solutions, trends, and initiatives in the fields relevant to MEDINA. The report will be updated to accommodate future trends and exploitation analysis in D7.6.
<b>Keyword List:</b>	Market analysis, exploitable results, business models.
<b>Licensing information:</b>	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) <a href="http://creativecommons.org/licenses/by-sa/3.0/">http://creativecommons.org/licenses/by-sa/3.0/</a>
<b>Disclaimer</b>	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	22.04.2021	First draft version. Comments received from TECNALIA	TECNALIA, NIXU
v0.2	05.05.2021	Comments and suggestions received by TECNALIA and consortium partners	TECNALIA, NIXU, BOSCH, FABASOFT, CNR
v0.9	15.05.2021	Final modifications	ALL
v1.0	17.05.2021	Final version for submission	TECNALIA
V1.1	9.12.2021	Comments from EU Review implemented, Ready for Review	NIXU
V1.2	23.12.2021	TECNALIA quality review comments implemented	TECNALIA, NIXU
V2.0	24.12.2021	Ready for submission	TECNALIA

---



---

## Table of contents

---



---

Executive Summary .....	8
1 Introduction .....	9
1.1 About this deliverable .....	9
1.2 Document structure .....	9
1.3 Naming of Key Results.....	9
1.4 Definitions .....	10
2 Business case.....	11
2.1 Building the trust.....	11
2.2 Why do customers need continuous audits?.....	11
2.3 Target users “Personas” .....	12
2.4 MEDINA solution and Key results.....	12
2.4.1 Standardized online cloud security metrics, controls & TOMs catalogue .....	14
2.4.2 Support for threat and risk assessment .....	14
2.4.3 Machine-Readable Certification language .....	14
2.4.4 Trustworthy, Automatic & Continuous evidence gathering and Management..	15
2.4.5 Automatic & Continuous Cloud Certificate evidence evaluation.....	15
2.4.6 Certificate Monitoring and management tool for Auditors.....	15
2.4.7 MEDINA Deployment Support .....	15
2.5 MEDINA framework components .....	16
2.6 MEDINA benefits for Cloud Service Providers .....	19
3 Market analysis and the path towards the market.....	22
3.1 Exploitation channels of MEDINA results per Persona .....	22
3.1.1 Compliance manager.....	22
3.1.2 Chief Information Security Officer (CISO) .....	24
3.1.3 Internal Control Owner (ICO) .....	24
3.1.4 Auditor (internal + external) .....	26
3.2 Market trends.....	27
3.3 Alternative solutions available in the market .....	27
4 Regulatory framework .....	36
5 Deployment models .....	38
5.1 Web tools (SaaS) .....	38
5.2 Containerized tools .....	38
5.3 Others.....	38
6 Value proposition canvas for Personas .....	39
6.1.1 Value proposition canvas for “Auditor” .....	41
6.1.2 Value proposition canvas for “Compliance Manager” .....	42

6.1.3	Value proposition canvas for “Internal Control Owner” .....	43
6.1.1	Value proposition canvas for “CISO” .....	44
7	Initial business model canvas .....	45
7.1	Business model canvas for MEDINA.....	45
7.1.1	Business model canvas for the Repository of Metrics and Measures (KR1).....	46
7.1.2	Business model canvas for the Risk based selection of controls to reach the certification assurance levels (KR2).....	47
7.1.3	Business model canvas for the Certification language (KR3) .....	48
7.1.4	Business model canvas for the Continuous Evidence management Tools (KR4) .....	49
7.1.5	Business model canvas for the Cloud Certificate Evaluator (KR5) .....	50
7.1.6	Business model canvas for the Risk-based auditor tool (KR6) .....	51
7.1.7	Business model canvas for the MEDINA framework as a whole.....	52
8	Conclusions .....	53
9	References.....	54
	APPENDIX A: Key Results in MEDINA .....	56

---

## List of tables

---

TABLE 1. TARGET USERS AND STAKEHOLDERS (ADOPTED FROM [1] [2]) .....	12
TABLE 2: MEDINA FRAMEWORK COMPONENTS (EXTRACTED FROM [8]) .....	16
TABLE 3 MAPPING COMPONENTS VS KEY RESULTS .....	18
TABLE 4: MAPPING OF THE MEDINA COMPONENTS WITH THE PERSONAS.....	19
TABLE 5: VALUE FOR FABASOFT (CSP) .....	20
TABLE 6: VALUE FOR BOSCH (CSP).....	21
TABLE 7. EXPLOITATION OF KR5 FOR COMPLIANCE MANAGERS.....	23
TABLE 8. EXPLOITATION OF KR5 FOR CISOS. ....	24
TABLE 9. EXPLOITATION OF KR5 FOR ICOS.....	25
TABLE 10. EXPLOITATION OF KR5 FOR AUDITORS.....	26
TABLE 11: MARKET SUMMARY OF ALTERNATIVE SOLUTIONS .....	28
TABLE 12. KEY PLAYERS IN THE CLOUD SECURITY POSTURE MANAGEMENT COMPETITIVE LANDSCAPE .....	33
TABLE 13: BUSINESS MODEL CANVAS FOR STANDARDISED ONLINE CLOUD SECURITY METRICS, CONTROLS & TOMS CATALOGUE .....	46
TABLE 14 BUSINESS MODEL CANVAS FOR SUPPORT FOR THREAT AND RISK ASSESSMENT.....	47
TABLE 15 BUSINESS MODEL CANVAS FOR CERTIFICATION LANGUAGE .....	48
TABLE 16 BUSINESS MODEL CANVAS FOR AUTOMATIC & CONTINUOUS EVIDENCE GATHERING AND MANAGEMENT TOOLS .....	49
TABLE 17 BUSINESS MODEL CANVAS FOR CLOUD CERTIFICATE EVIDENCE EVALUATOR.....	50
TABLE 18 BUSINESS MODEL CANVAS FOR CERTIFICATE MONITORING AND MANAGEMENT TOOLS FOR AUDITORS .....	51
TABLE 19 BUSINESS MODEL CANVAS FOR MEDINA FRAMEWORK .....	52
TABLE 20: KEY RESULTS IN MEDINA (SOURCE: [3]).....	56

---

---

## List of figures

---

---

FIGURE 1. MEDINA FRAMEWORK HIGH LEVEL VIEW (SOURCE: MEDINA'S OWN CONTRIBUTION) .....	13
FIGURE 2. BASIC WORKFLOW FOR MEDINA (ADOPTED FROM [3]) .....	14
FIGURE 3: VALUE PROPOSITION CANVAS AS LANDSCAPE ORIENTATION.....	40
FIGURE 4. VALUE PROPOSITION CANVAS FOR AUDITOR PERSONA .....	41
FIGURE 5. VALUE PROPOSITION CANVAS FOR COMPLIANCE MANAGER.....	42
FIGURE 6. VALUE PROPOSITION CANVAS FOR ICO .....	43
FIGURE 7: VALUE PROPOSITION FOR CISO .....	44
FIGURE 8. BMC NINE BUILDING BLOCKS (SOURCE [22]) .....	45

## Terms and abbreviations

API	Application Programming interface
AWS	Amazon Web Services
CAB	Conformity Assessment Body
CISO	Chief Information Security Officer
CNL	Controlled Natural Language
CSA	Cloud Security Alliance
CCM	Cloud Control Matrix
CSAP	Cloud Security Assessment Platform
CSC	Cloud Services Consumer
CSP	Cloud Services Provider
CSPM	Cloud Security Posture Management
CWPP	Cloud Protection Workload Platform
DoA	Description of Action
DSL	Domain Specific Language
EISA	Enterprise information security architecture
ENISA	European Union Agency for Cybersecurity
EUCSA	EU Cybersecurity Act
EUSEC	EU Security Certification
GDPR	General Data Protection Regulation
HIDS	Host based intrusion detection system
IAAS	Infrastructure as a Service
IAM	Identity and Access Management
ICO	Internal Control Owner
ICT	Information and communication technology
ISMS	Information security management system
ISO	International organisation for standardisation
JSON	Javascript Object Notation
KR	Key Result
NCCA	National Cybersecurity Certification Authority
NIST	National institute of standards and technology
NLP	Natural Language processing
OSCAL	Open Security Control Assessment Language
OWASP	Open Web Application Security Project
PAAS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
RDS	Relational Database Service
SAAS	Software as a service
SoA	Statement of Applicability
TOM	Technical and Organisational Measure
VAT	Vulnerability assessment tool
WP	Work Package
XML	extensible markup language
YAML	YAML Ain't Markup Language

## Executive Summary

This deliverable (D7.3) is an analysis of market potential, trends, players, and business scenarios that can be used when defining the exploitation strategies of MEDINA's commercial partners.

The main objective of MEDINA in this respect is to ensure that all the relevant communities will be reached out to in an interactive way, integrating their market analysis into this document. The aim is also to address future adoption and ensure the sustainability of the project results by considering the market trends, the business scenarios and the consortium and partners' needs and strategies.

The performed market analysis indicates that the trends are in favour for MEDINA as Cloud Security Posture Management and Certification language are gaining momentum in the Cloud Security Arena. It was also identified that MEDINA will create most of the value for stakeholders in security/risk management positions.

This deliverable will be further used a guideline by the MEDINA partners in their marketing efforts, as well as will be further used by D7.6 and D7.7 (Exploitation and sustainability Report-V1), to report the achieved results.

Deliverables D6.1 (Use cases specification and evaluation methodology) and its update D6.2 [1] [2] are intricately linked to this deliverable.



# 1 Introduction

## 1.1 About this deliverable

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.

The areas the project will cover in the cloud security industry are the Certification metrics and specification languages, Automated evidence management, Management of certificates and Continuous compliance. The challenging areas this project will tackle are areas like security validation, testing, machine-readable certification language, cloud security performance and audit evidence management. We also wish to get a good overview of the activities in which the projects outcomes are used for generating commercial value to the various partners. That is, in which ways the partners will benefit from the MEDINA project. This overall objective will be pursued by defining and managing a consistent strategy structured around specific analysis and exploitation activities.

Within the goal of the Sustainability and Exploitation MEDINA strategy, the Market, Innovation and Applicability Analysis will analyse the market by collecting existing approaches, products, and research projects. Additionally, the task will take a closer look at the applicability of the project results. This is to get a full overview of the market possibilities and to highlight the factors that weigh heavily on the success of the project.

This document's objectives, as part of the Sustainability and Exploitation MEDINA strategy, are complementary and related to those in the Communication and Dissemination tasks. Therefore, the activities in both must be synergic and strongly coordinated. The exploitation activity will look at the concrete plans by the project's partners, external subjects and to define MEDINA's outcomes into their offered product. All MEDINA partners have contributed to this deliverable. The Market Analysis Report will detail the market potential, trends, players, and business scenarios tied to the individual partners' exploitation strategies.

## 1.2 Document structure

Section 1 of this document consists of a brief introduction to MEDINA and the problems it aims to solve. The continuous certification challenges and how MEDINA proposes to solve them are included in section 2. Section 3 lists and characterizes the exploitable results and business models (market analysis). Section 4 details the regulatory framework for MEDINA. The deployment models and how they impact in the prizes/licenses are explained in Section 5. Section 6 lists the Value Proposition Canvas for Typical MEDINA users i.e. personas. Section 7 details and explains the Business model canvas for MEDINA. Conclusion (Section 8) ends the deliverable.

## 1.3 Naming of Key Results

Key Results are defined in the Description of Action [3]. To make the content more accessible for general public, Key Results are renamed to reflect the value and function of each result. See Appendix A for mapping of Key result naming.

## 1.4 Definitions

Next, some definitions of the terms extracted from the MEDINA glossary [4] that are used along this document are presented.

### **Asset**

Asset is a valuable entity of an organization that needs protection from cyber security threats.

### **Security control**

Security controls are “commands” given to an organisation which (if followed correctly) can reduce or mitigate security the risk to target asset. Controls can include any type of policy, procedure, technique, method, solution, plan, action or device designed to help accomplish that goal.

### **Security control framework**

Security control framework is a set of above security controls

### **Security Metrics**

A security metric is a description of a process that measures a particular characteristic of a target asset, in order to obtain information about the effectiveness of the information security management system.

### **Measurement**

A measurement means the process of implementing Security Metric such as gathering data like system logs, test results, configuration files, security events and sometimes the results of other measurements. The result of this process is called “measurement result” and often collectively referred to as *evidence*.

### **Technical and Organizational Measures (TOM's)**

Technical measures can be defined as the measures and controls implemented to a technical entity such as device, network or software.

Organizational measures can be defined as a set of internal policies, organizational methods, standards and controls to ensure the security of an organization.

When combined these are referenced as TOM's.

## 2 Business case

The detailed Business case for MEDINA will be developed together with MEDINA partners in later phase of the project and here only a high-level view is provided.

### 2.1 Building the trust

European cloud services providers face multiple challenges to gain customers' trust for cloud services consumed. The existing market for certification schemes is fragmented. The generic ISO / IEC 27001 based scheme is leading the market but other schemes such as national frameworks are less adopted [5]. The European certification on cloud services (EUCS) aims at diminishing this fragmentation in the European market by providing a certification mutually recognized in Europe. This opens a new market window.

Another problem in the certification schemes market is related to security controls. The focus of each scheme is targeted for a specific need and thus requires different security controls [5]. If a Cloud Services Provider wants to fulfil several schemes needs, this would require multiple audits to meet all the requirements from all schemes and standards. The EU-SEC<sup>1</sup> project sought to tackle this challenge and produced a complete list of Security Controls from which to select a suitable subset that would facilitate that. The possibility to reuse evidence remains however a challenge.

The final challenge that European cloud providers face when seeking a certification is the selection of the Conformity Assessment Method. There is a multitude of different practices to select from, such as ISO-based, ISAE-based, self-assessment and evidence based [5], each with different scope, depth, and process, deteriorating the trust and confusing consumers.

The solution to the above problems is mandated to ENISA in the Cybersecurity Act, but also ENISA has been facing an important challenge as there is not a specific cloud certification framework nor tools or methods to support the suggested security controls, assurance levels or conformity assessment methods compliant with the Cybersecurity Act requirements. To close this gap, ENISA created an ad-hoc working group that has been working since March 2020 in the definition of the European certification on cloud services (EUCS).

MEDINA's mission is to provide a platform with a state-of-the-art toolset and to leverage a continuous cloud security certification with trustworthy evidence-management methods. In essence, MEDINA will help CSPs (IaaS, PaaS and SaaS providers) to gain continuous certification status aligned with the EU Cybersecurity Act (EU CSA) [6] and the EUCS.

The long-term aim is to provide "Cloud Security Certification language" to enable the automation to meet changing requirements arising from the threat landscape.

### 2.2 Why do customers need continuous audits?

Certifications obtained once year is no longer satisfying the needs of the cloud customers in the higher end of the market, like finance and governmental institutions. Instead of "point-in-time" auditing they would like to have a continuous assurance service. The concept of continuous auditing requires novel and automated tools that at given interval performs, in what ISO/IEC 27k terminology names as "surveillance audits".

---

<sup>1</sup> <https://cordis.europa.eu/project/id/731845/es>

Today's technology becomes obsolete very quickly. DevOps practices widely used nowadays in software development which include continuous integration and deployment principles introduce changes in production environments thus changing the traditional auditing baseline activities and rendering evidences useless.

Continuous auditing can be defined in a following way [7]:

*“Method where results are achieved by continuously measuring specific attributes of an information system and comparing these results with pre-established security objectives. The results of this continuous auditing process are then shared in real-time with customers in a way that protects the cloud provider's confidential operations”*

## 2.3 Target users “Personas”

MEDINA framework is targeted to help Cloud Services Providers, Cloud Service users and both internal and external Auditors, including Conformity Assessment Bodies (CABs) to meet security requirements that arise from their specific needs.

MEDINA is intended to be used by users with different roles, i.e. Personas, as defined in [1] [2], and which are briefly described below for understandability purposes. Each Role is assigned set of responsibilities in the CSP organisation.

The concept of Personas is used in the Value Proposition Canvas later in this document.

Table 1. Target Users and Stakeholders (adopted from [1] [2])

Role Persona	Description
Compliance Manager	Responsible for the implementation of the Security Control Frameworks
	Responsible for the correct implementation of the internal controls
	Responsible for incident management
Chief Information Security Officer (CISO)	Responsible for security in the company, chooses what Security Controls should be implemented
Internal Control Owner (ICO)	Responsible for creating the internal controls
	Executing the internal controls
Auditor	Performs all actions required to audit a Company
	Responsible for performing internal audits

Deliverables D6.1 and D6.2 [1] [2] describe the Use Cases in more detail and its aim is to illustrate the use of MEDINA framework in different organizations.

## 2.4 MEDINA solution and Key results

MEDINA Key deliverables and Key results conforming the MEDINA solution are depicted in Figure 1 and are briefly described in following paragraphs. More detailed information about these Key Results and others related to dissemination, standardization, and Use Cases (KR7-KR9) are included in Appendix A.

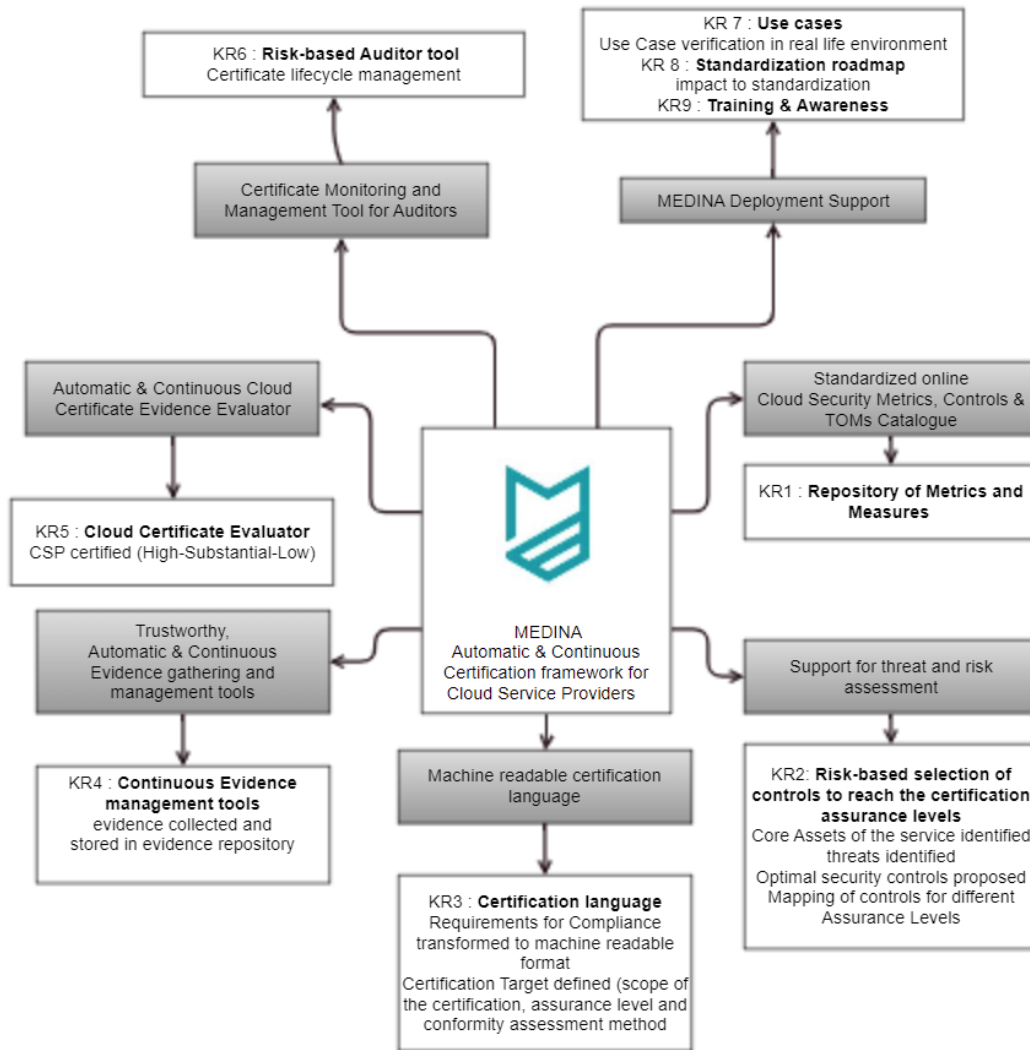


Figure 1. MEDINA framework high level view (source: MEDINA’s own contribution)

The MEDINA Basic workflow is illustrated in Figure 2. Users of the solution have their own swim line in the figure and time flows from left to right. There are several workflows developed for different use cases and this diagram is only for illustrating the basic concept, adapted and extended from the one already in the DoA [3].

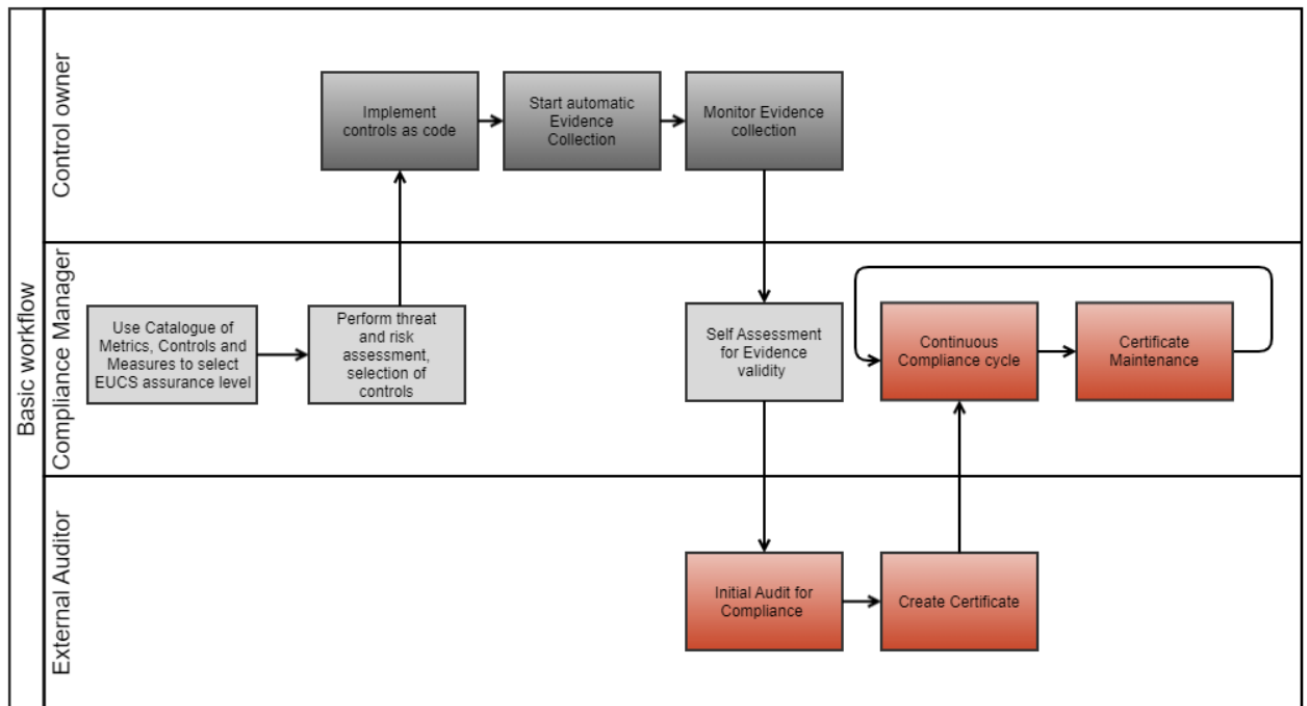


Figure 2. Basic workflow for MEDINA (adopted from [3])

### 2.4.1 Standardized online cloud security metrics, controls & TOMs catalogue

As described in [4], the main goal of the catalogue is to have an automated tool where a CSP compliance manager can select a security scheme and he can obtain all the information and guidance related to that security scheme, namely the controls, the security requirements, and the levels, that is, all what can be considered “static” information that appears in the standard. The MEDINA Catalogue is extended with metrics, the controls similar in other schemes, and eventually will include the self-assessment questionnaires or references to the tools that would aid in the automated monitoring and collection of evidences.

### 2.4.2 Support for threat and risk assessment

Cloud Services Providers will start the certification process with the selection of suitable security metrics for the selected certification target (i.e., describing the scoped cloud service’s assets, and EUCS assurance level). MEDINA supports this decision making in two different ways. Firstly, with an “EUCS preparedness tool” guiding CSPs on identifying the controls which should be improved in order to achieve the required assurance level and by taking into account the CSP’s risk appetite. Secondly, with a dynamic risk assessment coupled to MEDINA’s continuous (automated) monitoring and aiming to maintain the EUCS certificate’s lifecycle, while supporting CSPs and CABs on timely identifying non-compliances.

### 2.4.3 Machine-Readable Certification language

One of the key aspects of MEDINA is the ability to express most relevant aspects of a security certification scheme in a machine-readable format, written with MEDINA “Certification language”

Terms and conditions of certification schemes are usually available in English natural language, such as in the EUCS. Without the help of semi-automation, producing machine-readable code is a rigorous and manual translation procedure.

When the selected requirements defining the scope of the compliance are translated into Security Metrics, the certification itself can now be expressed in a machine-readable way. The MEDINA certification language, expressed in a machine-readable way, serves multiple purposes in the MEDINA framework. Firstly, it serves as a reference, to which the collected evidence is evaluated against. Secondly, it serves as a document between the CSP and the auditor to state the scope of the audit and that could potentially be seen as a Statement of Applicability (SoA), for example in the context of ISO 27001.

#### **2.4.4 Trustworthy, Automatic & Continuous evidence gathering and Management**

The next step towards achieving a continuous certification is the collection of actual, technical evidence at code, and service level as well as organizational evidences, namely policies and procedures. By leveraging this combined approach, evidence collection can lead to more accurate results, for example, by comparing the configuration of a firewall by means of static code analysis of Infrastructure-as-Code files and to actual deployed service.

Trustworthiness of evidences is achieved by block chain technology adapted for MEDINA.

#### **2.4.5 Automatic & Continuous Cloud Certificate evidence evaluation**

Achieving a continuous certification is the process of continuously evaluating whether the appropriate evidence collected supports the fulfilment of individual requirements of a certification target. The Cloud Certificate Evaluator tool provides techniques to evaluate technical evidence against a certification target.

Cloud Services Providers are responsible for establishing the technical implementation of an evidence collection and evaluation pipeline. The CSPs are also in charge of providing an appropriate interface implementing the MEDINA specification language to provide evidence and measurement results directly to the auditors.

A technical implementation needs to be audited from three aspects. First, the chosen metrics must be suitable to provide appropriate evidence for the chosen controls. Secondly, the pipeline itself must be conducting the measurements in a correct and trustworthy way. Finally, the tool must be configured correctly in the target environment to be able to gather and assess the evidences collected.

#### **2.4.6 Certificate Monitoring and management tool for Auditors**

This dynamic risk-based “Auditor Monitoring tool” aims to manage the whole life cycle of a cloud security certification, i.e., from its initial issuance to continuous renewal, revocation, or suspension up to an eventual removal, if the associated cloud services reach their end-of-life.

#### **2.4.7 MEDINA Deployment Support**

MEDINA offers a set of Use Cases that will be used to validate the framework in several public cloud service providers [1] [2]. Example of a Use case can be “MEDINA shall continuous update the certification state” and this functionality is verified in real environment.

MEDINA also aims to have an impact on standardization to enable the sustainability of the solution by providing feedback to ENISA on the implementation of the tools that would help CSPs comply with the EUCS.

MEDINA will additionally provide the necessary training to help customers to deploy the solution in their specific environments.

## 2.5 MEDINA framework components

MEDINA Key Results are implemented by means of different components in the framework. That is, a Key result is the outcome of the integration of one or more components, as defined in D5.1 [8]. The following table 2 gives a short summary of the functionality provided by each component. The detailed descriptions can be found in D5.1 [8].

The solution components described below aim at creating value and can be used by the different personas interacting with the MEDINA framework namely Auditor, Compliance Manager and Internal control owner. The matching of the key results with the components described below are shown in Table 3.

Table 2: MEDINA framework components (extracted from [8])

Component	Functionalities provided
Continuous certification evaluation	Evaluates the compliance level on all levels of the certification hierarchy (resources, requirements, controls, control groups, standard) based on the aggregation of assessment results and configuration.
Catalogue of metrics, controls and TOMs	Endorsement of Security Control Frameworks and related attributes (Security requirements, categories, controls, reference TOMs, metrics, evidences and assurance levels) Provision of guidance for the (self-)assessment of the requirements. Filtering of the information based on some values for the attributes Selection of requirements of a certain assurance level Selection of requirements from a certain framework Selection of metrics related to reference TOM Homogenization of the certification schemes: Provision of information about related requirements from different frameworks especially referenced to the EUCS
Clouditor	Evidence gathering- Assessment of evidences
CNL Editor	CNL Editor will allow work on CNL document, i.e. a requirement description (metadata) + a list of metrics in the form of a list of Obligations.
CNL translator	Translates the natural language text (English) of Security Requirements (TOMs) to the CNL obligations by recommending/predicting a set of metrics and integrating them into the CNL.
Codyze	Static code analysis and validation of program specifications
DSL mapper	Mapping of the CNL obligations + metadata output to a DSL (e.g. rego <sup>2</sup> )
Orchestrator	Provide interfaces to the databases. Forwards assessment results to the certificate evaluation. Forwards assessment result hashes to the trustworthiness system.
Organizational evidences gathering and processing	Gathering and processing organizational evidences. Provides evidences to the Clouditor for assessment.
Risk Assessment and Optimisation Framework	A questionnaire-based risk assessment facility to evaluate CSP-specific risk levels for predefined threats. <ul style="list-style-type: none"> <li>• Selection the most cost-effective requirements/TOMs (to optimise effort)</li> </ul>

<sup>2</sup> <https://www.openpolicyagent.org/docs/latest/policy-language/>



Component	Functionalities provided
	<ul style="list-style-type: none"> <li>• Risk-based evaluation of deviation from the framework to determine if the deviation is major or minor</li> </ul>
Trustworthiness System	<p>Maintains an improved audit trail of evidences and assessment results. Provides a record of information on a verifiable way (verification). Provides a record of information on a permanent way (traceability). Guarantees resistance to modification of stored data (integrity).</p>
Vulnerability Assessment Tool (VAT)	<p>Detection of web vulnerabilities by running integrated vulnerability scanners to scan web applications (OWASP ZAP1, w3af2)</p> <ul style="list-style-type: none"> <li>• Network reconnaissance (running hosts, open ports – exposed services) using integrated Nmap3</li> <li>• Detection of vulnerable software (known vulnerable service versions)</li> <li>• Running custom scripts for detection of specific vulnerabilities</li> <li>• Scheduling repeating vulnerability scans In MEDINA, VAT will be offered to the users as a tool to help CSPs satisfy compliance with certain EUCS controls as well as an evidence gathering tool.</li> </ul>
Wazuh	<p>In general, Wazuh is a HIDS solution that provides the following functionalities:</p> <ul style="list-style-type: none"> <li>• Malware and intrusion detection</li> <li>• Log data analysis</li> <li>• File integrity monitoring</li> <li>• Vulnerability detection</li> <li>• Configuration assessment</li> <li>• (Limited) monitoring of data about AWS &amp; Azure infrastructure with simple compliance assessment.</li> </ul> <p>In MEDINA, Wazuh will be offered to the users as a tool to help CSPs satisfy compliance with certain EUCS controls as well as an evidence gathering tool</p>
Automation Certification Life-Cycle	<p>Updates the certificate states and assurance levels defined in the EUCS scheme based on the evaluation results.</p> <p>Provides a tool for appropriate entities (CAB) to issue/update/revoke and sign security certifications for the cloud providers based on the updated certificate state.</p> <p>Provides a tool for appropriate entities (CAB) to publish the certificate state in a public register</p>
Evidence Collection	<p>This component of the MEDINA architecture has the objective of interfacing native Cloud Security Posture Management's (CSPM2) assessment functionalities, to the MEDINA's Orchestrator component. Contrary to the Clouditor component, which directly interacts with the rest of MEDINA's architecture, basically all existing CSPMs have their own (proprietary) API specification for consuming/providing data related to the continuous monitoring/assessment processes they implement. Component uses CSPM-specific interfaces for allowing the Orchestrator to consume the assessment results and evidence gathered by native CSPM (e.g., Azure Security Center). The main advantage of CSPM-specific interfaces in the "Native Assessment" component, refers to facilitating early adopters to leverage MEDINA in their existing cloud ecosystems.</p>

The mapping of the above solution components of the MEDINA Framework to the Key Results shown is described in the table below.

Table 3 Mapping components vs Key Results

Component in MEDINA framework:	Mapping to MEDINA Key Results:					
	#1	#2	#3	#4	#5	#6
Catalogue of metrics, controls and TOMs	x					
Risk Assessment and Optimisation Framework		x				
CNL Editor			x			
CNL translator			x			
DSL mapper			x			
Orchestrator (Databases)				x		
Organizational evidences gathering and processing				x		
Vulnerability Assessment Tool				x		
Wazuh (monitoring for threat detection, integrity, incident response and compliance)				x		
Evidence Collection (from Cloud Native APIs)				x		
Codyze (Static Code Analyzer)				x		
Clouditor				x	x	
Continuous certification evaluation					x	
Company Compliance dashboard					x	
Trustworthiness System				x		x
Automation Certification Life-Cycle						x

The following table illustrates the use of solution components by the personas [1] [2].

Table 4: Mapping of the MEDINA components with the Personas

	Auditor	Compliance Manager	Internal Control Owner	CISO
<b>Component Name in Medina framework:</b>	<b>Adding value for *)</b>			
Catalogue of metrics, controls and TOMs		x	x	
Risk Assessment and Optimisation Framework		x		x
CNL Editor			x	
CNL translator			x	
DSL mapper			x	
Orchestrator (Databases)		x		
Organizational evidences gathering and processing	x	x		
Vulnerability Assessment Tool	x	x		
Wazuh (monitoring for threat detection, integrity, incident response and compliance)	x	x		
Evidence Collection (from Cloud Native APIs)	x	x		
Codyze (Static Code Analyzer)	x	x		
Clouditor	x	x		
Continuous certification evaluation	x	x		
Company Compliance dashboard	x	x	x	x
Trustworthiness System	x			
Automation Certification Life-Cycle	x			

\*) illustrative , depends on the actual workflow

## 2.6 MEDINA benefits for Cloud Service Providers

To ensure the viability of the MEDINA Solution it will be first deployed by Consortium members Bosch and Fabasoft.

Bosch will use MEDINA to assure the security of a set of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) deployments that are commonly used for Internet of Things (IoT) backends, in at least three public cloud computing services: Microsoft Azure, Amazon Web Services (AWS), and Fabasoft Cloud. In addition, Fabasoft will deploy SaaS services to both Public and Private Cloud customers with a need for a High Assurance level of MEDINA.

Expected value from MEDINA for a Cloud Service Provider Fabasoft and Cloud Services Consumer Bosch is summarized below in Table 5 and

Table 6.

Table 5: Value for Fabasoft (CSP)

MEDINA Key Results	Pains	Gains (Value for Fabasoft)
<b>KR#1 Repository of Metrics and Measures</b> <b>Value statement:</b> Standardized online Cloud Security Metrics, Controls & TOMs Catalogue	Fabasoft collects and manages security controls with specific TOMs in an offline document, called Internal Control Matrix	Fabasoft can use the MEDINA repository to collect and manage Security Controls and implemented metrics and measures.
<b>KR#2 Risk-based selection of Controls to reach the Certification Assurance Levels</b> <b>Value statement:</b> Support for threat and risk assessment	Currently, risk processes with respect to requirements in certain Cloud Security Frameworks are available and implemented.	Dynamic risk management is ready to be integrated into Fabasoft processes and used for continuous certification processes.
<b>KR#3 Certification language</b> <b>Value statement:</b> Machine-Readable Certification language	Lack of machine-readable language for representing certification-related concepts.	NLP-enabled certification language based on EUCS is available.
<b>KR#4 Continuous evidence management tools</b> <b>Value Statement:</b> Trustworthy, Automatic & Continuous Evidence gathering and management Tool	Certification-related evidence is managed manually.	Automated management of certification-related evidence is deployed
<b>KR#5 Cloud Certificate evaluator</b> <b>Value Statement:</b> Cloud Certificate Evidence Evaluator	Certification process for EUCS does not exist. Other certification schemes rely on manual processes.	High level of automation is delivered to EUCS certification processes at Fabasoft.
<b>KR#6 Risk based Auditor tool</b> <b>Value Statement:</b>	BSI C5 Type2 audit is done in a traditional <i>manual</i> way	A MEDINA approach of a continuous, risk-based audit can be implemented into the

MEDINA Key Results	Pains	Gains (Value for Fabasoft)
Certificate Monitoring and management tool for Auditors	with weeks of actual auditing activities.	Fabasoft certification processes.

Table 6: Value for Bosch (CSP)

MEDINA Key Results	Pains	Gains (Value for Bosch)
<b>KR#1 Repository of Metrics and Measures</b> <b>Value statement:</b> Standardized online Cloud Security Metrics, Controls & TOMs Catalogue	Bosch EISA only contains generic and non-EUCS specific TOMs. Metrics do not exist in Bosch EISA.	Bosch EISA extended with EUCS TOMs, standardized metrics, and corresponding governance processes.
<b>KR#2 Risk-based selection of Controls to reach the Certification Assurance Levels</b> <b>Value statement:</b> Support for threat and risk assessment	Only static risk processes are available in our IT security governance framework.	Dynamic risk management is integrated into Bosch's processes and deployed as part of our continuous cloud compliance service.
<b>KR#3 Certification language</b> <b>Value statement:</b> Machine-Readable Certification language	Lack of machine-readable language for representing certification-related concepts.	NLP-enabled certification language based on EUCS is available and integrated into Bosch's cloud processes.
<b>KR#4 Continuous evidence management tools</b> <b>Value Statement:</b> Trustworthy, Automatic & Continuous Evidence gathering and management Tool	Certification-related evidence is managed manually.	Automated management of certification-related evidence is deployed, and widely used during Bosch's EUCS audit processes.
<b>KR#5 Cloud Certificate evaluator</b> <b>Value Statement:</b> Cloud Certificate Evidence Evaluator	Certification process for EUCS does not exist. Other certification schemes rely on manual processes.	High level of automation is delivered to EUCS certification processes at Bosch.

MEDINA Key Results	Pains	Gains (Value for Bosch)
<b>KR#6 Risk based Auditor tool</b> <b>Value Statement:</b> Certificate Monitoring and management tool for Auditors	Existing cloud security posture management tools lack of risk management notions.	Seamless integration of cloud-native security posture management tools with MEDINA's risk-based auditor tool. Corresponding risk management framework processes are modified accordingly.

### 3 Market analysis and the path towards the market

This section presents the market analysis performed for MEDINA. Section 3.1 dives into how the different Personas can be addressed by means of different exploitation channels and the MEDINA Key results. Market trends in the field of security and certification are identified in section 3.2. Section 3.3 presents an initial market summary that will be improved and developed in further versions of this document.

#### 3.1 Exploitation channels of MEDINA results per Persona

This section presents an initial version of a MEDINA's market segmentation analysis. This analysis has the main aim of, based on the Personas defined in Deliverable 6.1 and D6.2 [1] [2], (see Table 1), and the MEDINA results, differentiate the different exploitation channels and potential activities that will be, or could be, carried out.

To this end, four exploitation channels have been identified:

1. **Transfer of knowledge and further research:** the MEDINA result will be exploited through a transfer of intellectual property or through new research projects, funded by public or private organizations.
2. **New product or service:** the result will be exploited by means of new products or services. This can entail services surrounding the open source components, for instance.
3. **Improvement of existing products or services:** the result will be exploited through an already existing product or service but improved thanks to MEDINA.
4. **Training:** exploited through training activities.

##### 3.1.1 Compliance manager

The compliance manager has as main responsibility the implementation and life-cycle management of the security control frameworks of an organization such as the EUCS in the focus of MEDINA. Such responsibility also includes the management of non-compliances or incidents, among other aspects. Depending on the size of an organization, there might be one central compliance manager, or this role can be shared by regional/business unit-related compliance managers.

The table below presents the potential exploitation channels for each of the MEDINA results for compliance managers.

Table 7. Exploitation of KRs for Compliance Managers

Key Result	Exploitation Channels			
	Transfer of knowledge and further research	New product or service	Improvement of existing products or services	Training
<b>Repository of Metrics and Measures (KR1)</b>		Y	Y	Y
<b>Risk-based selection of Controls to reach the Certification Assurance Levels (KR2)</b>		Y	Y	Y
<b>Certification language (KR3)</b>				
<b>Continuous evidence management tools (KR4)</b>		Y		
<b>Cloud Certificate Evaluator (KR5)</b>		Y		
<b>Risk-based Auditor tool (KR6)</b>		Y	Y	Y
<b>use cases (KR7)</b>				Y
<b>Standardization (KR8)</b>				Y
<b>Training (KR9)</b>				Y

In summary, the previous table shows that focus of MEDINA’s exploitation activities for Compliance Managers will cover the following topics:

- Bringing the repository of metrics and measures (i.e., KR1) close to the industrial practice, so compliance managers can use it in the context of their (existing) lifecycle processes for security control frameworks.
- In the practice, it is very complicated for compliance managers to relate security controls to associated business risks. MEDINA’s KR2 outcomes, in particular training activities, will support compliance managers to bridge this gap.
- New software tools/services for the management of digital evidence related to compliance processes (KR4) and supporting the lifecycle of certifications like EUCS (KR6) will provide a whole new perspective to the current industrial practice of compliance managers. Development of related visualizations and automation (KR5) will complement the “compliance manager toolbox” to improve existing tools and processes.
- Lastly, MEDINA will also leverage training activities (KR9) to promote the transfer of knowledge related to the MEDINA framework, in particular by compiling practical experience from the validation scenarios (KR7) and standardization activities (KR8). We foresee that these exploitation activities will have a major impact on compliance managers willing to achieve (or understand the implications) of the novel EUCS certification.



### 3.1.2 Chief Information Security Officer (CISO)

The CISO role, a company-wide responsible for topics related to cybersecurity (EUCS included), is a major stakeholder from the exploitation perspective in MEDINA. At the current state of practice, most CISOs rely on commercial tools for visualizing highly aggregated indicators related to the security compliance posture of their organization. Such information is essential to support their decision making on cybersecurity investments, and other measures aimed to mitigate the risks of being non-compliant (which could even become a showstopper for making business in some, highly regulated, market verticals).

In Table 8, the exploitation channels of the MEDINA results for CISOs can be seen

Table 8. Exploitation of KRs for CISOs.

Key Result	Exploitation Channels			
	Transfer of knowledge and further research	New product or service	Improvement of existing products or	Training
<b>Repository of Metrics and Measures (KR1)</b>				
<b>Risk-based selection of Controls to reach the Certification Assurance Levels (KR2)</b>				
<b>Certification language (KR3)</b>				
<b>Continuous evidence management tools (KR4)</b>				
<b>Cloud Certificate Evaluator (KR5)</b>				
<b>Risk-based Auditor tool (KR6)</b>		Y	Y	Y
<b>use cases (KR7)</b>				Y
<b>Standardization (KR8)</b>				Y
<b>Training (KR9)</b>				Y

Enhancing existing CISO tools and visualizations with automation/continuous assessments indicators, and risk-based information (KR6) to complement existing decision support systems in the organization. Integration of financial impact notions in MEDINA's risk-based tool will surely prove beneficial to organizations willing to embrace EUCS.

CISOs would also benefit from MEDINA's training activities related to the developed framework and corresponding to lessons learned during the validation activities with EUCS. Each MEDINA-trained CISO will achieve the knowledge related to the topic of continuous audit and how it benefits their own organizations in the pursue of EUCS.

Given the upcoming release of the EUCS (expected Q4/2022 at the time of writing), the MEDINA consortium foresees CISO training activities as a high-impact exploitation outcome from our project.

### 3.1.3 Internal Control Owner (ICO)

In addition to the Compliance Manager, many organizations delegate the management of daily compliance activities to the Internal Control Owner. This is an essential role that guarantees

scalable cybersecurity governance tasks in organizations. Whereas the Compliance Manager can define security policies and cybersecurity compliance rules in an organization, the ICO will be the main responsible for its implementation and execution. Considering such assumptions, the following table summarizes our main KR's which will be leveraged in MEDINA's exploitation activities for this specific market segment of ICOs.

Table 9. Exploitation of KR's for ICOs

Key Result	Exploitation Channels			
	Transfer of knowledge and further research	New product or service	Improvement of existing products or services	Training
<b>Repository of Metrics and Measures (KR1)</b>	Y	Y	Y	Y
<b>Risk-based selection of Controls to reach the Certification Assurance Levels (KR2)</b>	Y	Y	Y	Y
<b>Certification language (KR3)</b>	Y	Y	Y	Y
<b>Continuous evidence management tools (KR4)</b>		Y	Y	Y
<b>Cloud Certificate Evaluator (KR5)</b>		Y	Y	Y
<b>Risk-based Auditor tool (KR6)</b>	Y	Y	Y	Y
<b>use cases (KR7)</b>				Y
<b>Standardization (KR8)</b>				Y
<b>Training (KR9)</b>				Y

As seen in the table above, exploitable outcomes (KR's) from MEDINA for the ICO market are focused on the following topics:

- Deep understanding and leverage of KR1 – KR3 i.e., MEDINA's outcomes related to elements in security control frameworks. Notice that we also include KR3, because we foresee it as exploitable outcome for ICOs struggling with understanding new frameworks like EUCS in their daily job. Exploitation activities also comprehend technology/knowledge transfer and training, which is needed to create the required expertise in organizations willing to fully benefit from MEDINA.
- The expected outcomes from KR4 and KR5 are also seen as essential for ICOs, although in this case we do not foresee as exploitation channel the knowledge transfer, because ICOs are not expected to further develop such tools. Upcoming validation activities (in WP6) might change that assumption.
- As exploitable outcome for ICOs is specially seen KR6, where the cloud security certification's lifecycle will be automatically managed. ICOs are expected customers (from an exploitation perspective) of this toolset, given the integrated features for automatically managing complex certifications from schemes like EUCS. Activities in all exploitation channels are expected for KR6 in the case of the ICO market segment.
- In analogy to compliance managers, we also expect to deliver trainings to ICOs in relationship to exploitable outcomes from KR7 – KR9 e.g., standardization activities, and lessons learned from validation pilots.

### 3.1.4 Auditor (internal + external)

Another market segment relevant to MEDINA includes internal auditors (e.g., those responsible for checking compliance to internal control frameworks), and external auditors included in the category of Conformance Assessment Body (CAB). From a MEDINA perspective, this market segment also comprises the so-called NCCA (National Cybersecurity Certification Authority), which will play an essential role in the EUCS certification scheme.

In this deliverable we will not make a split between the internal/external auditors from an exploitation perspective, although future work in WP7 might consider that direction depending on the interim outcomes from MEDINA’s activities. For the time being, the following table summarizes the different exploitation channels for the auditor market segment.

Table 10. Exploitation of KR for Auditors

Key Result	Exploitation Channels			
	Transfer of knowledge and further research	New product or service	Improvement of existing products or services	Training
<b>Repository of Metrics and Measures (KR1)</b>				Y
<b>Risk-based selection of Controls to reach the Certification Assurance Levels (KR2)</b>				Y
<b>Certification language (KR3)</b>				
<b>Continuous evidence management tools (KR4)</b>	Y	Y	Y	Y
<b>Cloud Certificate Evaluator (KR5)</b>	Y	Y	Y	Y
<b>Risk-based Auditor tool (KR6)</b>	Y	Y	Y	Y
<b>use cases (KR7)</b>				Y
<b>Standardization (KR8)</b>				Y
<b>Training (KR9)</b>				Y

We foresee strong interest of auditors in the outcomes related to the tools developed by the technical work packages, which result in KR4 – KR5. Such toolset provides auditors with the mechanisms to automatically manage the certification lifecycle, therefore releasing them of manual task which are in their current practice. To fully profit from MEDINA’s toolset, our exploitation channels for the auditors’ market segment include technical deep dives (trainings), and open discussions about new research challenges which can be achieved with public or private funding.

Auditors are also interested in familiarizing themselves with the techniques and catalogues developed by the project (KR1), for which training sessions will be used as exploitation channels. In a similar manner, the MEDINA consortium also foresees auditors’ interest on topics related to risk-based selection of security controls (KR2) which is a common audit practice nowadays, but strongly dependent on manual processes and subjective assessments. Finally, we will also plan for training sessions focused on presenting lessons learned from our validation use cases

(KR7), and standardization related to topics like EUCS (KR8). Both topics are of interest for both CABs and NCCAs given the upcoming EUCS.

### 3.2 Market trends

MEDINA framework can be positioned along with the Cloud Security Posture Management (CSPM) tool market providing however additional capabilities to perform continuous & automated audits. CSPM tools are competing with cloud native tools and evolving rapidly. As cloud provider services see an increase in use, an explosion in the number of unmanaged risks in the mission-critical digital industry has occurred. Cloud Security Posture Management (CSPM) automates cloud security management across the diverse cloud infrastructures.

The CSPM term was coined by Gartner and, according to their description [9], can be defined as:

*“CSPM offerings continuously manage cloud risk through the prevention, detection, response, and prediction of where excessive cloud infrastructure risk resides based on common frameworks, regulatory requirements and enterprise policies. The core of CSPM offerings proactively and reactively discover and assess risk/trust of cloud services configuration (such as network and storage configuration), and security settings (such as account privileges and encryption)”*

MEDINA aims to differentiate from the competition by:

- providing an end-to-end solution;
- bridging the concept of continuous (automated) monitoring and continuous auditing and providing the tools for that;
- being the first solution that implements the EUCS, but that can be used also for other schemes such as BSI C5 that also have the notion of continuous monitoring;
- providing trust, ensuring that neither the evidences collected, nor the results are protected.

According to an article in AppviewX [10], Cloud Security Posture Management is among the top trends we are seeing in the cyber security industry. This means that there is a fair amount of competition and MEDINA needs to stand out from the crowd.

Another important trend happening nowadays is the “Compliance as code” trend, realized in MEDINA through the Certification language. According to [11], a certification language *“can be summarized as the codification of your compliance controls so their adherence, application and remediation can be automated. Typically, Certification language tools work by enabling compliance stakeholders to define how IT resources must be configured in order to meet compliance controls”*. The trend of “as a code” is gaining momentum, and MEDINA is planning on leveraging this as well.

### 3.3 Alternative solutions available in the market

In this section an analysis of existing tools and sources relevant for MEDINA are shown, including their (functional) description and the relationship with the MEDINA Key Results. This is an initial version of the market analysis, which will be enlarged in upcoming deliverables.

Table 11: Market summary of alternative solutions

Solution/ tool name	Reference	Solution's description	Related KR
ISO/IEC 19086-4 (Cloud Security Service Level Agreements)	<a href="https://www.iso.org/standard/68242.html">https://www.iso.org/standard/68242.html</a>	ISO/IEC 19086-4 (Cloud Security Service Level Agreements), provides a non-certifiable set of quantitative/qualitative service level objectives for CSPs	KR1
Reference document on security measures for Operators of Essential Services	<a href="https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf">https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf</a>	Reference implementations of organizational and security measures in critical infrastructures	KR1
CIS Controls™ and CIS Benchmarks™	CIS Controls™ <a href="https://www.cisecurity.org/controls/">https://www.cisecurity.org/controls/</a>  And control list: <a href="https://www.cisecurity.org/controls/cis-controls-list/">https://www.cisecurity.org/controls/cis-controls-list/</a>  CIS Benchmarks™ <a href="https://www.cisecurity.org/cis-benchmarks/">https://www.cisecurity.org/cis-benchmarks/</a>	Reference implementations of organizational and security measures for several controls, with examples for various CSPs	KR1
Azure Security Benchmark	<a href="https://docs.microsoft.com/en-us/security/benchmark/azure/">https://docs.microsoft.com/en-us/security/benchmark/azure/</a>	Reference implementations of organizational and security measures for Azure	KR1
NIST-Performance Measurement Guide for Information Security	First version (2008) <a href="https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final</a>  Draft of the Second version (September 2020) <a href="https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft">https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft</a>	Metrics implementations	KR1

Solution/ tool name	Reference	Solution's description	Related KR
AWS- Best Practices for Security, Identity, & Compliance	<a href="https://aws.amazon.com/products/security/?nc1=h_ls">https://aws.amazon.com/products/security/?nc1=h_ls</a>	Reference implementations of organizational and security measures for AWS	KR1
Compliance validation for Amazon RDS	<a href="https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/RDS-compliance.html">https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/RDS-compliance.html</a>	Reference implementations of organizational and security measures for Amazon RDS	KR1
PRISMA TM	Reference to Prisma Suite.  <a href="https://docs.paloaltonetworks.com/prisma.html">https://docs.paloaltonetworks.com/prisma.html</a>	The Prisma suite secures a public cloud environment, SaaS applications, internet access, mobile users, and remote locations through a cloud-delivered architecture. It is a comprehensive suite of security services to effectively predict, prevent, detect, and automatically respond to security and compliance risks without creating friction for users, developers, and security and network administrators, the suite is composed by: <ul style="list-style-type: none"> <li>• Prisma Cloud. Cloud application security (redlock)</li> <li>• Prisma Access (SASE). Cloud access security</li> <li>• Prisma SaaS. SaaS application security</li> <li>• Prisma SD-WAN. Solution that enables the cloud-delivered branch</li> <li>• VM-Series. Cloud-native security</li> <li>• CN-Series. Solution that helps to secure Kubernetes environments with the CN-Series Firewall</li> </ul>	KR1, KR5
TIC – CCN Security Guidelines	Reference to a document in Spanish: Cloud services usage.  <a href="https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-">https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-</a>	Reference implementations of organizational and security measures for Spanish ENS, including examples from several CSPs	KR1

Solution/ tool name	Reference	Solution's description	Related KR
	<a href="https://entornos-cloud/file.html">entornos-cloud/file.html</a>		
RSA Archer	<a href="https://www.rsa.com/content/dam/en/data-sheet/rsa-archer-grc-platform.pdf">https://www.rsa.com/content/dam/en/data-sheet/rsa-archer-grc-platform.pdf</a>  <a href="https://www.rsa.com/de-de/products/integrated-risk-management/archer-platform">https://www.rsa.com/de-de/products/integrated-risk-management/archer-platform</a>	Platform for managing integrated risk management program. It can: <ul style="list-style-type: none"> <li>• Manage policies, controls, risks, assessments, and deficiencies.</li> <li>• Automate business processes</li> <li>• Deliver real-time reports</li> <li>• On premise or host (SaaS)</li> <li>• Integration with external systems to support data analysis, process management and reporting</li> </ul>	KR2
Neupart Secure ISMS	<a href="https://www.neupart.com/products">https://www.neupart.com/products</a>	Secure ISMS is an information security management system that enables organisations to efficiently manage IT risks and compliance requirements, such as ISO 27001/2, EU Data Protection Regulation and PCI DSS. <p>It includes the following packages:</p> <ul style="list-style-type: none"> <li>• Secure ISMS Risk: Includes risk treatment, business impact assessments, vulnerability analysis, Static and dynamic reports, amongst others.</li> <li>• Secures ISMS Compliance: Manage those tasks that are part of an ISO 27001 Information Security Management.</li> <li>• Secure ISMS BCP, Business continuity plans availability</li> </ul> <p>Some other characteristics.</p> <ul style="list-style-type: none"> <li>• On premise or host (SaaS).</li> <li>• GDPR package also available</li> </ul>	KR2
US NIST's OSCAL	<a href="https://pages.nist.gov/OSCAL/">https://pages.nist.gov/OSCAL/</a>  Reference to OSCAL Catalog Model:  <a href="https://pages.nist.gov/OSCAL/documenta">https://pages.nist.gov/OSCAL/documenta</a>	OSCAL is an Open Security Controls Assessment Language created by the NIST, that is a set of formats expressed in XML, JSON and YAML. <p>The OSCAL Catalog Model represents a collection of controls, represented as a control catalogue. The OSCAL Catalog Model has been designed to represent security and privacy controls in</p>	KR3

Solution/ tool name	Reference	Solution's description	Related KR
	<p><a href="https://pages.nist.gov/OSCAL/catalog-layer/catalog/">tion/schema/catalog-layer/catalog/</a></p> <p>Reference to OSCAL tools:</p> <p><a href="https://pages.nist.gov/OSCAL/tools/">https://pages.nist.gov/OSCAL/tools/</a></p>	<p>standardized, machine-readable formats. The OSCAL catalog model standardizes the representation of control definitions from various sources (e.g., SP 800-53, ISO/IEC 27002, COBIT 5) allowing control information to be easily searched, imported, and exported by applications using a generic format.</p> <p>There are also some open-source tools:</p> <ul style="list-style-type: none"> <li>• OSCAL java library</li> <li>• XSLT Tooling</li> <li>• OSCAL KIT</li> <li>• OSCAL GUI</li> </ul>	
Azure Policies	<p><a href="https://docs.microsoft.com/en-us/azure/governance/policy/overview">https://docs.microsoft.com/en-us/azure/governance/policy/overview</a></p>	<p>Azure Policy is a service in Azure which allows to create policies which enforce and control the properties of a resource. When these policies are used, they enforce different rules and effects over the resources of a company, so those resources stay compliant with the companies' IT governance standards. Azure policy has three components:</p> <ul style="list-style-type: none"> <li>• Policy definition. That represents the conditions to be controlled</li> <li>• Policy assignment is the scope of what the policy definition can take effect around</li> <li>• Policy parameters</li> </ul> <p>Through its compliance dashboard, it provides an aggregated view to assess the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.</p>	KR3
AWS ConfigRules	<p><a href="https://docs.aws.amazon.com/config/latest/APIReference/API_ConfigRule.html">https://docs.aws.amazon.com/config/latest/APIReference/API_ConfigRule.html</a></p> <p>Page 292 of the following pdf. <a href="https://docs.aws.amazon.com/config/latest/APIReference/awconfig-">https://docs.aws.amazon.com/config/latest/APIReference/awconfig-</a></p>	<p>An AWS Config rule represents an AWS Lambda function that it is created for a custom rule or a predefined function for an AWS managed rule. The function evaluates configuration items to assess whether the AWS resources comply with the desired configurations. This function can run when AWS Config detects a configuration change to an AWS resource and at a periodic frequency (for example, every 24 hours).</p>	KR3





Solution/ tool name	Reference	Solution's description	Related KR
	<a href="#">apiref.pdf#API_ConfigRule</a>		
AWS Audit Manager	<a href="https://aws.amazon.com/es/audit-manager/">https://aws.amazon.com/es/audit-manager/</a>	<p>AWS Audit Manager it is a solution that helps to continuously audit the AWS usage to simplify the assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the “all hands-on deck” manual effort that often happens for audits and enable to scale the audit capability in the cloud as a business grows.</p> <p>It provides tools to assess if the policies, procedures, and activities or controls are operating effectively, it also includes features to manage stakeholder reviews of the controls and to build audit-ready reports with much less manual effort.</p>	KR2/KR6
Cloud Security Alliance	[12]	<p>Cloud Security Alliance (CSA) is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.” (Wikipedia)</p> <p>CSA published “The Continuous Audit Metrics Catalog” for compliance managers in october 2021. The catalogue covers topics of security metrics and continuous auditing and this work is closely linked to MEDINA Key Result of Cloud Security metrics catalogue. The key take-away is that security metrics needs to be designed carefully so that they enable automation i.e. continuous assurance.</p> <p>The metrics in the CSA catalogue aim to support internal CSP governance, risk, and compliance (GRC) activities and provide a helpful baseline for service-level agreement transparency</p>	KR1



As mentioned beforehand, MEDINA is highly related to the Cloud Security Posture Management (CSPM) market. Hence, special attention has been given to the CSPM market and a separate

analysis is provided in the table below. These tools are mostly related to KR4 and KR5 (Continuous Evidence management tools and Certificate evaluator respectively). This table details the key players in this area along with their key messages.

Table 12. Key players in the Cloud Security Posture management competitive landscape

Player	Key message
	<p>VerSprite developed the Cloud Security Assessment Platform (CSAP) to support our cloud security assessments and analysis. Our enterprise-ready cloud platform provides visual reporting in a way that makes cloud security easy to manage and prioritize risks.</p> <p>By providing organizations with a comprehensive view of their security posture, CISOs and security leaders now have a clear visibility into how their overall cloud environment is positioned against standard security framework.</p> <p>VerSprite's risk-based threat modelling process allows our security consultants to not only discover, analyse, and report on an organization's CSP hosted infrastructure, but also assess security risks and their related business impact. CSAP is delivered via a SaaS model where the only connection to the client's environment is via read-only 'audit' role.</p> <p><a href="https://versprite.com/security-offerings/security-products/cloud-security-assessment-platform/">https://versprite.com/security-offerings/security-products/cloud-security-assessment-platform/</a></p>
	<p>The Cloud Security Posture Management (CSPM) previously known as Cloud Infrastructure Security Posture Assessment was defined in response to the growing need of organizations to correctly configure public cloud IaaS and PaaS services and address cloud risks. CSPM is a class of security tools as defined by Gartner include use cases for compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization.</p> <p><a href="https://www.fugue.co/cloud-security-posture-management">https://www.fugue.co/cloud-security-posture-management</a></p>
 Falcon Horizon CSPM	<p>Cloud security posture management (CSPM) automates the identification and remediation of risks across cloud infrastructures, including Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). CSPM is used for risk visualization and assessment, incident response, compliance monitoring, and DevOps integration, and can uniformly apply best practices for cloud security to hybrid, multi-cloud, and container environments.</p> <p><a href="https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/">https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/</a></p>

Player	Key message
	<p>Zscaler Cloud Security Posture Management (CSPM) automatically identifies and remediates application misconfigurations in SaaS, IaaS, and PaaS to reduce risk and ensure compliance. Zscaler CSPM is part of the comprehensive, 100% cloud-delivered data protection capabilities in the Zscaler Cloud Security Platform.</p> <p><a href="https://www.zscaler.com/products/cloud-security-posture-management">https://www.zscaler.com/products/cloud-security-posture-management</a></p>
 Aqua Security	<p>Scan, monitor and remediate configuration issues in public cloud accounts according to best practices and compliance standards, across AWS, Azure, Google Cloud, and Oracle Cloud</p> <p><a href="https://www.aquasec.com/products/cspm/">https://www.aquasec.com/products/cspm/</a></p>
	<p>OpsCompass captures a high-fidelity snapshot of your entire cloud and all its configurations, creating a complete picture of your environment. From this snapshot, it generates a proprietary score and helpful graphs for your dashboard that indicate how you are performing against key compliance standards and identify compliance trends at a glance. You can then drill down to discover exactly where any compliance problems lie and how you can fix them.</p> <p><a href="http://www.opscompass.com/">http://www.opscompass.com/</a></p>
	<p>DivvyCloud is a Cloud Security Posture Management (CSPM) platform that provides real-time analysis and automated remediation across leading cloud and container technologies, including AWS, Azure, GCP, Alibaba, and Kubernetes. DivvyCloud protects cloud and container environments from misconfiguration, policy violations, threats, and IAM challenges.</p> <p>Once installed &amp; deployed, connected to your clouds, and configured, DivvyCloud discovers your infrastructure resources across all clouds and distills this information into a normalized database. This database is used to analyse cloud operations, identify risks, and take action according to user-defined policies and rules to alert, mitigate, or remediate problem.</p> <p><a href="https://docs.divvycloud.com/docs">https://docs.divvycloud.com/docs</a></p>
 CloudCheckr CMx High Security	<p>CloudCheckr CMx High Security is built to the highest levels of security and supports 300 rigorous controls in 17 control families from NIST 800-53. Combined with AI-based threat detection and daily automated internal vulnerability scans, our commercial-grade cloud computing security management will accelerate your cloud adoption in financial services, healthcare, and other regulated industries. With emerging public cloud security</p>

Player	Key message
	<p>challenges, get started with CMx High Security today to achieve cloud regulatory compliance, security compliance, and the optimal protection of your data.</p> <p><a href="https://cloudcheckr.com/">https://cloudcheckr.com/</a></p>
 <p><b>Check Point</b> SOFTWARE TECHNOLOGIES LTD</p> <p>CloudGuard</p>	<p>CloudGuard Cloud Security Posture Management, part of the CloudGuard Cloud Native Security platform, automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.</p> <p><a href="https://www.checkpoint.com/products/cloud-security-posture-management/">https://www.checkpoint.com/products/cloud-security-posture-management/</a></p>
 <p><b>PRISMA</b></p> <p>Paloalto networks</p>	<p>Prisma Cloud is the industry's only comprehensive Cloud Native Security Platform that delivers full lifecycle security and full stack protection for multi- and hybrid-cloud environments</p> <p><a href="https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management">https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management</a></p>

## 4 Regulatory framework

MEDINA is impacted by several regulatory frameworks, mandates and policy initiatives that will impact the applicability of MEDINA KRs in the market. This section provides an overview of such regulatory framework with special focus on the Cybersecurity Act, European Data Strategy and European Cloud Rule Book.

In the communication *“Digitizing European Industry. Reaping the full benefits of a Digital Single Market”* [13] the European Commission identified cloud computing as one of the major levers for improving industry digitization. However, according to Eurostat, the usage of Cloud Services in the European industry is not so extended [14].

The new policy initiatives, such as the Regulation for the Free Flow of non-personal data [15] and the Cybersecurity Act [6], adopted in 2018 and 2019 respectively, have been designed with the aim of boosting the adoption of cloud computing in Europe by seeking to generate trust among (business) consumers and consequently, facilitating the digital transformation of the industry and public sector.

The inexistence of an EU-wide cloud security certification scheme and the fragmentation in the cloud security certification market, *“has led to a lack of competition between cloud service providers in the Union, to various vendor lock-in issues, and to a serious lack of data mobility”* [15], hampering therefore the uptake of cloud as identified in the regulation of free flow of non-personal data.

To this end, article 6 of the regulation on free flow of non-personal data states that porting of data shall be facilitated by cloud service providers through the adherence to a self-regulatory code of conduct. It also mentions the need to have *“approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services”*.

The European Cybersecurity Act [6] (EU CSA) adopted in June 2019, and entered into force in 2021, that aims to *“create a framework for European Cybersecurity Certificates for products, processes and services that will be valid throughout the EU”*. According to the EU CSA, the CSPs will *“enable their users [users of products and services] to ascertain the level of security assurance and ensure that these security features are independently verified”*.

As stated above, the EU CSA is also applicable to ICT products and services beyond cloud services. Among these, edge services, edge nodes, 5G or IoT devices are included in such categorization.

In November 2019 [16] ENISA received the formal letter from the European Commission requesting, *“in accordance with article 48(2) of the EU Cybersecurity Act, [...] to prepare a cybersecurity certification candidate scheme for cloud services, taking into account existing and relevant schemes and standards”*.

In response to this inquiry, ENISA has created an ad-hoc working group [17] which has as main task to support ENISA in the preparation of this draft candidate cybersecurity certification scheme. The resulting draft version [18] of the scheme was released for public consultation during January-February 2021 and the feedback obtained is currently being analyzed and will be incorporated into the next versions of the scheme.

Regarding privacy regulations, the GDPR states that *“The Member States, the supervisory authorities, the Board and the Commission shall encourage [...] the establishment of data*

*protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation”.*

The European Data Strategy [19] released in February 2020 outlines a strategy for policy measures and investments to enable the data economy in Europe. Among the different problems identified in that communication, the adoption of cloud is mentioned, both from the consumer and provider side.

These problems include compliance with data protection regulation, multi-cloud interoperability, data portability, and the lack of a European cloud and data infrastructure.

The EU data strategy is built around 4 pillars:

- 1) A cross-sectoral governance framework for data access and use.
- 2) Enablers: Investments in data and strengthening Europe’s capabilities and infrastructures for hosting, processing and using data, interoperability.
- 3) Competences: Empowering individuals, investing in skills and in SMEs.
- 4) Common European data spaces in strategic sectors and domains of public interest.

To this end, the European Commission proposes to create *“a cloud services marketplace for EU users from the private and public sector [...] by Q4 2022”* where *“potential users (in particular the public sector and SMEs) [are] in the position to select cloud processing, software and platform service offerings that comply with a number of requirements in areas like data protection, security, data portability, energy efficiency and market practice”*, with the services endorsed to this marketplace adhering to the *“coherent framework [that will be developed] around the different applicable rules (including self-regulation) for cloud services, in the form of a ‘cloud rulebook’. In a first instance, the cloud rulebook will offer a compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection and data portability”*.

Other initiatives, like as Gaia-X [20], have created their own Policy and rules document, where aspects such as the ones mentioned previously are incorporated.

MEDINA will support these aspects already identified by the European Commission by providing CSPs with a solution that adheres to the cloud rulebook, more specifically in what respects to the cloud security certification aspects, which will allow them to be included in the cloud services marketplace should they desire to.

## 5 Deployment models

The different MEDINA Key Results, tools, and components, previously described in section 0, constitute the comprehensive MEDINA solution, thus the MEDINA framework.

This section briefly classifies MEDINA KRs attending to the technological framework required for its execution and deployment. The different deployment options will impact the business model of each KRs. The current section presents an initial classification of the KRs based on the envisioned deployment models at this initial stage of the project. This initial analysis will be extended and detailed in further versions of this deliverable and in deliverable D7.6 (Exploitation and sustainability Report) (from the business model impact perspective) and in D5.1 [8] and D5.2 (*MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy*, from the technical perspective).

### 5.1 Web tools (SaaS)

Web tools are accessible through any compatible browser: In MEDINA some of the tools will be offered as service, which are invoked for performing different functionalities. Internally these tools can be deployed following the multi-cloud approach. It is envisioned that the following MEDINA Key results, tools and components will be offered as Web Tools (SaaS): Repository of metrics and measures (KR1), Risk based selection of controls (KR2), Certification language (KR3), Cloud certificate Evaluator (KR5), Auditor Tool (KR6), and the MEDINA framework.

### 5.2 Containerized tools

Containerized tools are much like web tools, but in this case the web application can be installed locally. The difference between this case and the previous one depends on the exploitation model to be decided for each Key Result, tool or component and the needs from the users with respect to the usage of the component / tool (i.e., evidence storage shall be internal (local) to the CSP)). The following tools fit into this category: Repository of metrics and measures (KR1), Risk based selection of controls (KR2), Certification language (KR3), Cloud certificate Evaluator (KR5), Auditor Tool (KR6), the MEDINA framework, and Continuous evidence management tools (KR4).

### 5.3 Others

Other components may be delivered as software libraries or software clients to be included/imported in other software components from the CSPs/Auditors. This might be the case for the orchestrator component inside the Continuous evidence management tools (KR4).

The selection of the deployment model will be also influenced by the requirements of the certification stakeholders (i.e., auditors, CABs and NCCAs) who will only trust on the results gathered by the MEDINA tools because (i) they have participated in the implementation of the tools and (ii) the tools themselves are certified under the European Certification Framework, therefore a Continuous audit tools certification scheme is also needed.

## 6 Value proposition canvas for Personas

The Value Proposition Canvas [21] is a tool which can help to ensure that a product or service is positioned around what the customer values and needs. It provides an effective method to understand at a glance the customer requirements along with the product designs and services requested. It is a detailed look at the relationship between segments and value propositions. It has a clear connection also to the Business Model Canvas [22].

The Value proposition canvas is divided into two distinct areas: The Customer Profiles and The Product Map. The Customer Profiles comprise Customer Jobs, Customer Pains and Customer Gains. Similarly, The Product Map comprises three categories: Product & Services, Pain Relievers and Gain Creators. Each of these are described next.

**Customer Jobs** are the tasks or jobs that MEDINA potential users must complete, the needs to be satisfied or the issues to be solved.

**Customer Pains** is list of all the negative aspects that MEDINA potential users may experience before, during or after the previous tasks or jobs are performed. It may include, among others, frustrations, stoppers, negative feelings, increased cost etc.

**Customer Gains** list are all the positive outcomes or benefits that MEDINA potential users may get such as emotional appeals, functional advantages, cost-savings, etc.

**Product & Services** are the MEDINA Solution components that are relevant to each “persona” analysed.

**Pain Relievers** are features of MEDINA that provides a solution so that the user-facing negative aspects can be minimized.

**Gain Creators** outlines the benefits generated from MEDINA features for users. These may be functional, emotional, economic advantages, etc.

The square (the product map) is about products that are offered. The focus is made on features, functionalities, and benefits they can offer to not only attract customers but also to meet their requirements from the part represented as a circle.

The circle (Customer profile) is cut into three pieces where we have defined the customers’ tasks and expectations which are going to be fulfilled, as well as positive and negative experiences associated therewith. The purpose is not to be product-oriented; the purpose is to only deal with the customer challenges.

MEDINA creates value to different “personas” as defined in Chapter 3.1

For readability reasons the traditional Value proposition canvas is tilted 90 degrees and displayed as portrait.



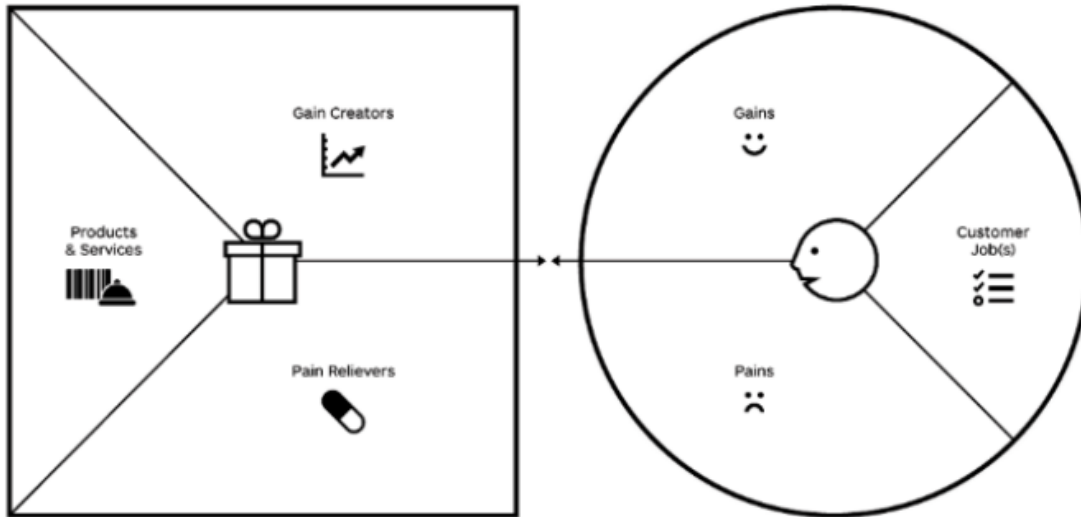


Figure 3: Value Proposition canvas as landscape orientation

### 6.1.1 Value proposition canvas for “Auditor”

The Auditor is responsible for the selected controls to be proven to be implemented. Usually there are few challenges to meet the objective of this task. Customers are sometimes poorly prepared, there is a lot of manual work to be done with limited resources and it is hard to keep up with the changes in the environment. In Figure 5 the link between MEDINA framework and how it generates gain and reliefs pain for the Auditor is described with a methodology described above.

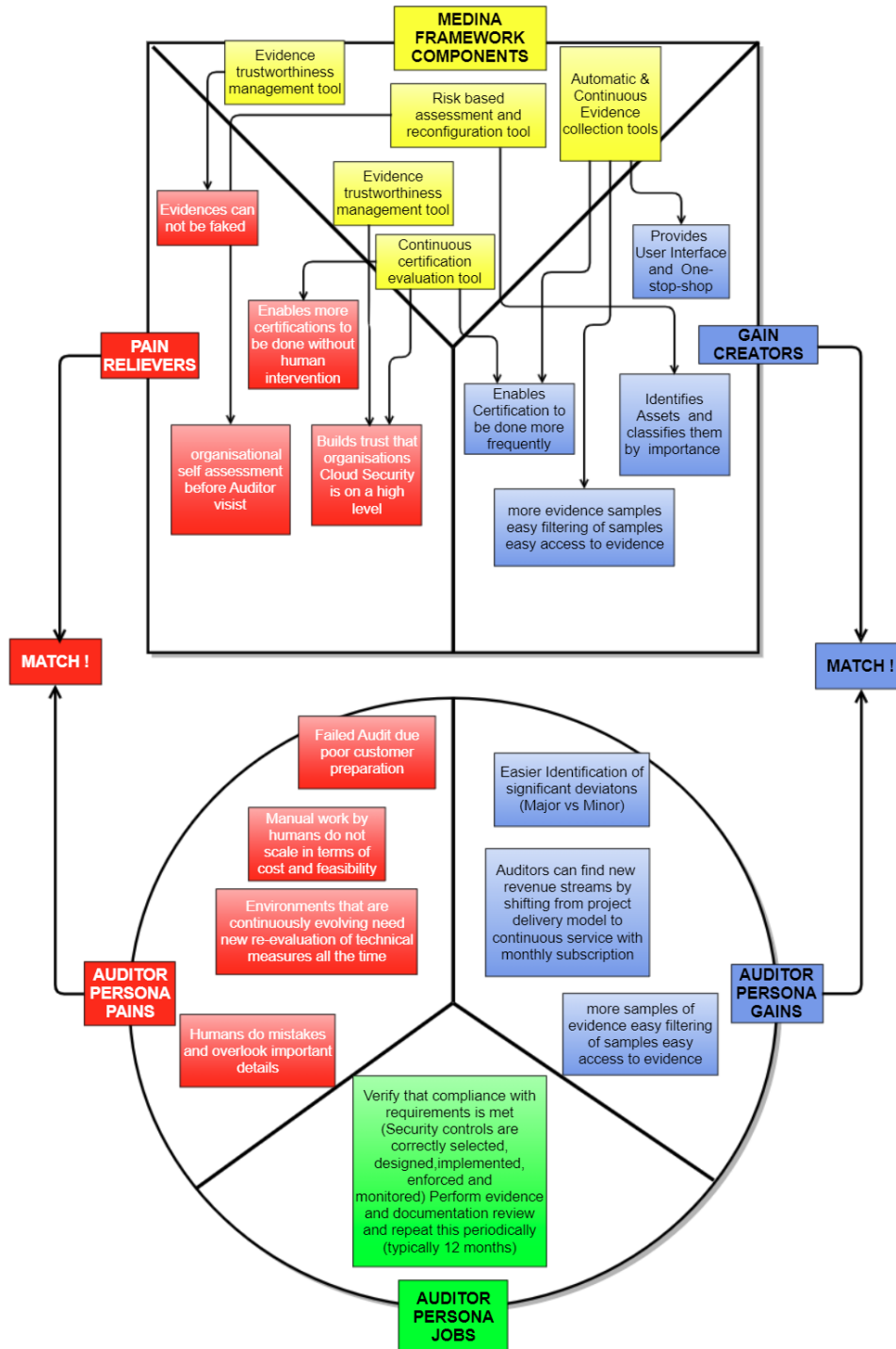


Figure 4. Value proposition canvas for Auditor Persona

### 6.1.2 Value proposition canvas for “Compliance Manager”

A Compliance Manager is in the spotlight as it comes to protecting the assets of a CSP. Without the support of the relevant tools, this task is rather overwhelming. In figure 6 it is described how MEDINA addresses the pains and gains for a Compliance Manager.

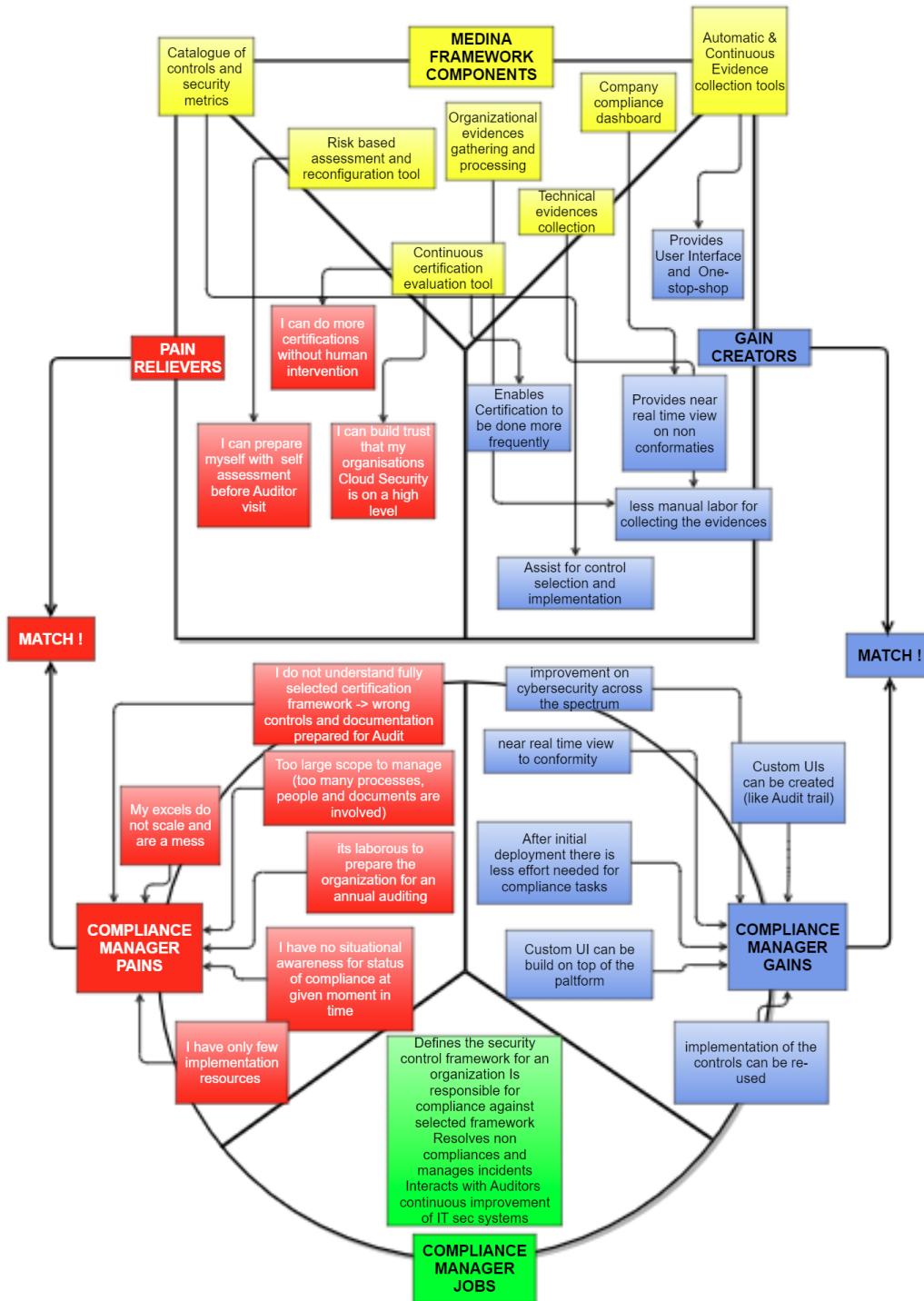


Figure 5. Value proposition canvas for compliance Manager

### 6.1.3 Value proposition canvas for “Internal Control Owner”

For internal controls owners there is the technically demanding task to actually implement and monitor that the crucial controls are in place as requested by compliance Manager. Again, MEDINA seeks to offer valuable support to fulfil the task.

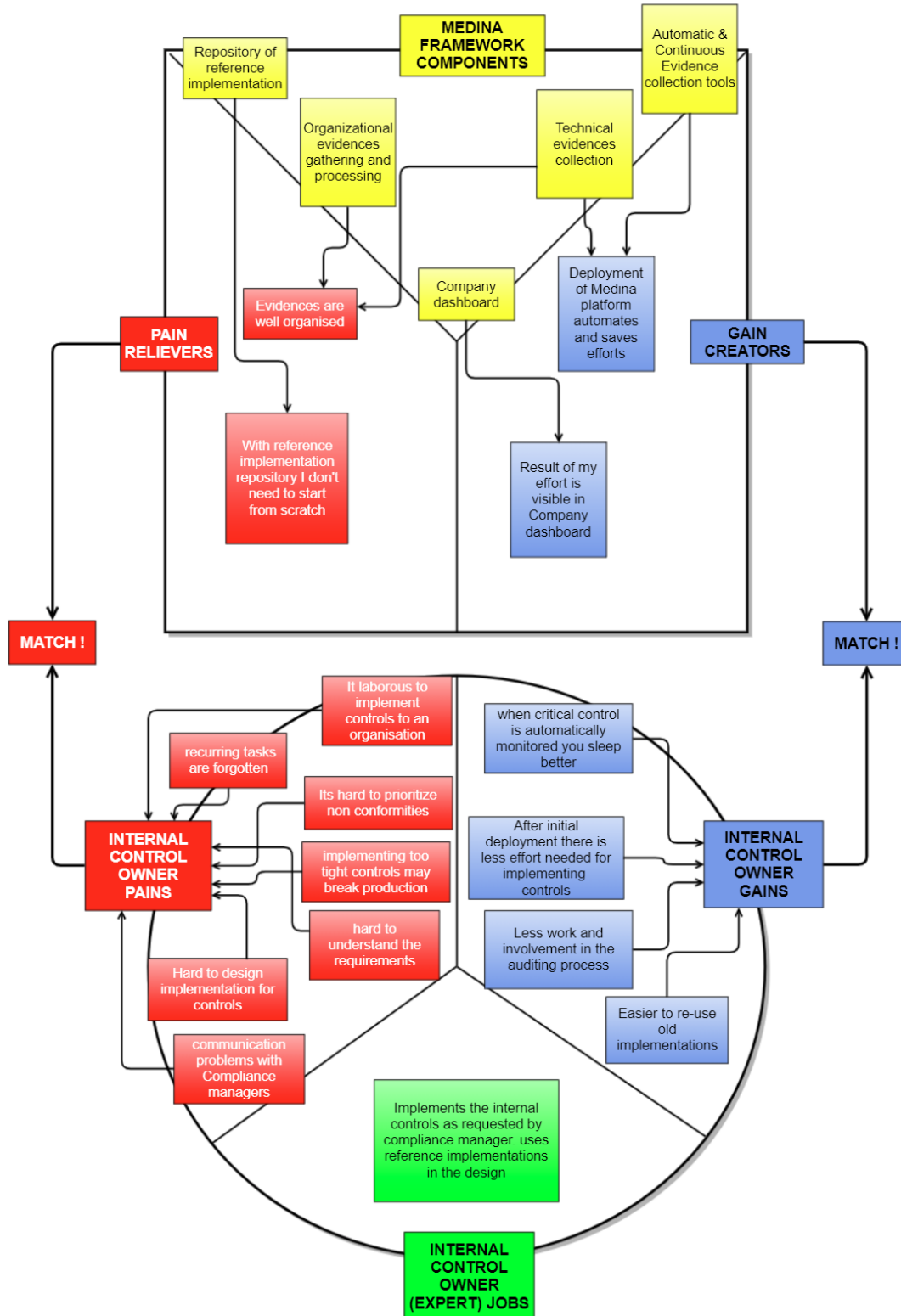


Figure 6. Value proposition canvas for ICO

### 6.1.1 Value proposition canvas for “CISO”

Ultimate accountability to protect the assets are a burden for the Chief Information Security Officer. MEDINA framework is not only a tool to achieve a higher certification level, but also a mean to increase revenues and create a new business opportunity.

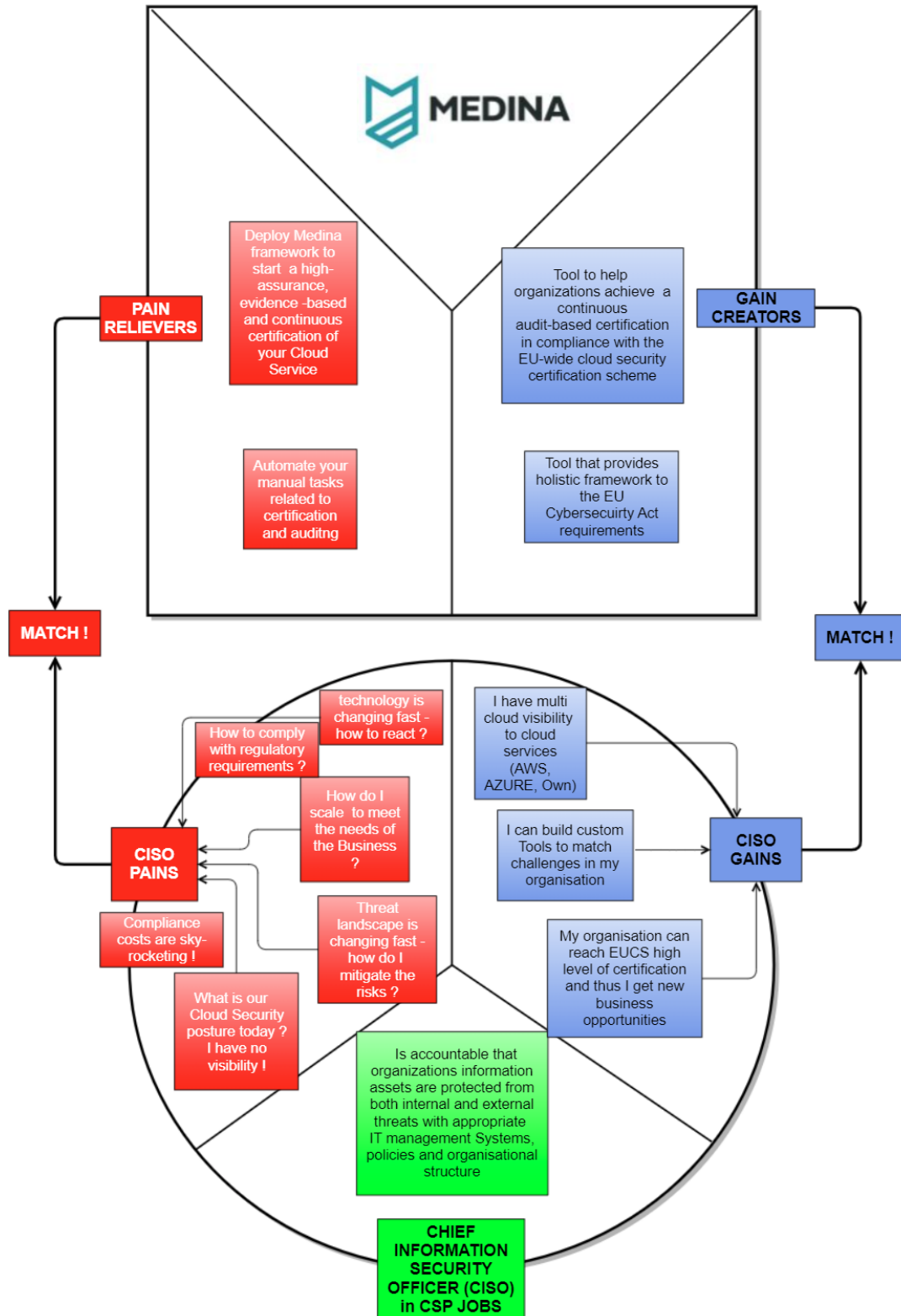


Figure 7: Value proposition for CISO

## 7 Initial business model canvas

### 7.1 Business model canvas for MEDINA

A Business Model Canvas [22] (BMC) is a strategic management template created by Alexander Osterwalder and used for developing new business models and documenting existing ones. It offers a visual chart with elements describing a firm's or product's value proposition, infrastructure, customers, and finances, assisting businesses to align their activities by illustrating potential trade-offs.

BMC focuses on nine elements generic to any business and is implemented in a table form. The idea is to answer few key questions that are presented below.

Figure 8. BMC nine building blocks (source [22])

DELIVERABLE				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
<i>Outsource some of the work to partners. Who are our key partners? Who are our key suppliers? Which key resources are we acquiring from partners? Which key activities do partners perform?</i>	<i>What key activities do our value propositions require?</i>	<i>What value do we deliver to the customer? Which one of our customer's problems are we helping to solve? What bundles of products and services are we offering to each customer segment? Which customer needs are we satisfying? Why Customer will buy your product and not the competitors ?</i>	<i>What type of customer relationship does each of our customer segments expect us to establish and maintain with them? Which ones have we established? How are they integrated with the rest of our business model? How costly</i>	<i>For whom are we creating value? Who are our most important customers?</i>
	<b>Key resources</b>		<b>Channels</b>	
	<i>What key resources do our value propositions require?</i>  - physical - intellectual - Human - Financial		<i>Through which channels do our customer segments want to be reached? How are we reaching them now? How are our channels integrated? Which ones work best? Which ones are most cost-efficient? How are we integrating them with customer routines?</i>	
<b>Cost structure</b>		<b>Revenue streams</b>		
<i>What are the most important costs inherent in our business model? Which key resources are most expensive? Which key activities are most expensive?</i>		<i>Where the money comes from ? For what value are our customers really willing to pay? For what do they currently pay? How are they currently paying? How would they prefer to pay? How much does each revenue stream contribute to overall revenue?</i>		

In the following sub-chapters, the Business Model Canvas for each of the Key Results of MEDINA are presented, created with the Strategyzer<sup>3</sup> tool.

<sup>3</sup> <https://www.strategyzer.com/>

### 7.1.1 Business model canvas for the Repository of Metrics and Measures (KR1)

The catalogue is the repository of security controls, requirements and metrics.

Table 13: Business Model Canvas for standardised online cloud security metrics, controls & TOMs Catalogue

KR#1 REPOSITORY OF METRICS AND MEASURES				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
Standards Developing Organizations which will contribute to feed the catalogue with new certification schemes CSPs, Open source SW communities willing to provide more technical functionalities into the catalogue.	<p>integration of additional and updated metrics/measures into the repository, along with the development of binding regulations and guidelines for cloud security certification scheme.</p> <ul style="list-style-type: none"> <li>Integration of metrics/measures from other international standards, if deemed interesting.</li> <li>Creation of non-binding good practices with elicited metrics/measures, and evidences, integration into cloud services development guidelines and internal security Prozesse</li> </ul>	<p>Provision of a repository of controls, similar controls in other schemes, security requirements, Reference TOM implementations, metrics and CSP service specific target value of the metrics, and evidence checklist quantitative for the continuous security certification of cloud services, with the goal of achieving the different levels of assurance envisioned in the EU CSA.</p>	B2C and B2B. Consultancy, OSS communities	<p>Cloud Service Providers (IaaS, SaaS, PaaS), connected services and IoT products (all market verticals) relying on cloud backends, auditors, National Certification Bodies, ENISA</p>
	<p>Key resources</p> <p>Sales team, Validation infrastructure</p> <ul style="list-style-type: none"> <li>MEDINA development team to implement further functionalities for continuous update of the controls and metrics, as well as for the repository itself.</li> <li>Training team</li> </ul>		Channels	
Cost structure		Revenue streams		
Personnel, licenses, Infrastructure providers.		Freemium schema. While the repository is free of use, fees will be charged if additional metrics are added under special requirement. Training activities.		

## 7.1.2 Business model canvas for the Risk based selection of controls to reach the certification assurance levels (KR2)

This tool provides the needed support for CSPs to make the right decisions to protect the critical information assets [4].

Table 14 Business Model Canvas for support for threat and risk assessment

KR2: RISK-BASED SELECTION OF CONTROLS TO REACH THE CERTIFICATION ASSURANCE LEVELS				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
CSPs willing to share their risk-related parameters Public and Private Security Analysts publishing and sharing threat/vulnerability/risk statistics	Key activities (exploitation): Productized as a SaaS solution in partner's solution portfolio.	Analysis/recommendation/decision-making support tool for CSPs and cloud consumers looking to select the EU CSA assurance level appropriate for their risk appetite	B2C and B2B. Consultancy, OSS communities	Cloud Service Providers (IaaS, SaaS, PaaS), Cloud Consumers, security consulting firms, auditors
	Maintenance and establishment of relations between new metrics and requirements/controls, and between new requirements (security certification schemas) and controls. Maintenance of threat frequency parameters. Creation of best practices for identification of key assets and estimation of their impact.			
	Key resources			
	Sales team, MEDINA development team to implement custom functionalities and for updated relations between metrics and requirements and requirements and controls. Training team		Freemium schema. The free part will be delivered open in OSS communities, while the premium part will be retained proprietary (e.g., SaaS or on-premises based installation).	
Cost structure		Revenue streams		
Personnel, licenses, Infrastructure providers.		Freemium schema. While the MEDINA tool is free of use, fees will be charged for implementing custom functionalities. Training activities.		



### 7.1.3 Business model canvas for the Certification language (KR3)

The problem that is addressed with this tool is that the technical and organizational measures that a cloud provider must fulfil, are usually written in natural language, which is ambiguous, open to different interpretation, error-prone and non-computer-readable. Also depending on a particular certification scheme, the exactly the same written measure, may still vary from one scheme to another [23].

Current tools, mostly excel based, used to address the need to define controls in a systematic way can grow quite large and complex and hence hard to understand and manage.

This tool provides a “code” that can be used as input for cloud providers assessment tools to verify the compliance between evidence and the metrics to be met.

Table 15 Business model Canvas for Certification language

KR3: CERTIFICATION LANGUAGE				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
Open Source SW communities (GitHub, others), Partners' commercial networks. Liaisons with ISO/IEC SC27/SC38, BSI, ETSI, DIN.	Key activities (sustainability): Open source version maintained by community. Standard specification maintained by respective SDO (ISO/IEC or other).	Standard-based representation in machine-readable format of TOMs (Technical and Organizational measures) related to the cloud certification process.	B2C and B2B. Consultancy, OSS communities	Cloud Service Providers (IaaS, SaaS, PaaS), auditors, certification bodies
	Key activities (exploitation): Active participation in relevant standardization bodies. Integration in products from commercial portfolio of partners.		Channels	
	Key resources		Freemium schema. The free part will be delivered open in OSS communities, while the premium part will be retained proprietary. Standard specification follows commercial channels of respective organization (e.g., ISO/IEC).	
Cost structure		Revenue streams		
Personnel		Freemium schema. While the MEDINA cert. language spec is free of use, fees will be charged for integration tasks. Training activities		

### 7.1.4 Business model canvas for the Continuous Evidence management Tools (KR4)

This tool aims at automatically and continuously gather and assess the evidences needed for the fulfilment of the security requirements established in EUCS. Moreover this tool makes sure that neither the assessment results nor the evidences are tampered with through their protection with DLTs [24] [25].

Table 16 Business model Canvas for Automatic & continuous evidence gathering and management tools

KR4: CONTINUOUS EVIDENCE MANAGEMENT TOOLS				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
OSS communities (GitHub, others), Partners' commercial networks.	Key activities (sustainability): Open source version maintained by community.	Simplified and automated management of audit evidence's lifecycle (collecting, protecting, updating, etc.), which can be leveraged in EU CSA's certification processes.  Flexible integration of new and custom tools  State-of-the-art monitoring techniques  Trustworthy management of sensitive evidences	B2C and B2B. Consultancy, OSS communities  Channels  Freemium schema. The free part will be delivered open in OSS communities, while the premium part will be retained proprietary (e.g., SaaS or on-premises based installation).	Cloud Service Providers (IaaS, SaaS, PaaS), Cloud Consumers, auditors, certification bodies.
	Key activities (exploitation): Productized as a SaaS solution in partner's solution portfolio.			
	Key resources  Sales team, MEDINA development team to implement custom functionalities. Training team. Standardization team.			
Cost structure		Revenue streams		
Personnel, licenses, Infrastructure providers.		Freemium schema. While the MEDINA tool is free of use, fees will be charged for implementing custom functionalities. Integration activities. Training activities		

### 7.1.5 Business model canvas for the Cloud Certificate Evaluator (KR5)

The problem that is addressed with this tool is CSPs need to demonstrate the compliance to certifications, not only once in a year, but in a continuous fashion. With this tool CSPs can demonstrate the compliance to the high level of assurance and reduce the risk of low-quality assessment results [26].

Table 17 Business model Canvas for Cloud Certificate Evidence Evaluator

KR5: CLOUD CERTIFICATE EVALUATOR				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
OSS communities (GitHub, others), Partners' commercial networks.	Key activities (sustainability): Open source version maintained by community.	Continuous evaluation of the overall certification posture	B2C and B2B. Consultancy, OSS communities	Cloud Service Providers who want to continuously ensure their compliance with EUCS requirements
	Key activities (exploitation): Productized as a SaaS/desktop solution in partner's solution portfolio.	Quick identification of risks, including critical non-conformities  Automation of tedious tasks like lifecycle management  Quick identification of interesting evidences for auditors		
	Key resources		Channels	
	Sales team, MEDINA development team to implement/integrate custom functionalities. Training team..		Freemium schema. The free part will be delivered open in OSS communities, while the premium part will be retained proprietary (e.g., SaaS or on-premises based installation).	
Cost structure		Revenue streams		
Personnel, licenses, Infrastructure providers.		Freemium schema. While the MEDINA tool is free of use, fees will be charged for implementing custom functionalities. Integration activities. Training activities		

### 7.1.6 Business model canvas for the Risk-based auditor tool (KR6)

As the goal of MEDINA is to make the status of a Cloud Security certificate publicly available, this tool that is operated by the auditors or CABs is used to manage the lifecycle of certificate from creation to revocation [26].

Table 18 Business model canvas for Certificate monitoring and management tools for Auditors

KR6: RISK-BASED AUDITOR TOOL				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
OSS communities (GitHub, others), Partners' commercial networks.	Key activities (sustainability): Open source version maintained by community.	Tool for continuously managing lifecycle of cloud security certificates. It can be used by whole cloud supply chain, and also cloud customers.	B2C and B2B. Consultancy, OSS communities	Cloud Service Providers (IaaS, SaaS, PaaS), Cloud Consumers, auditors, certification bodies.
	Key activities (exploitation): Productized as a SaaS/desktop solution in partner's solution portfolio.		Channels	
	Key resources		Freemium schema. The free part will be delivered open in OSS communities, while the premium part will be retained proprietary (e.g., SaaS or on-premises based installation).	
	Sales team, MEDINA development team to implement/integrate custom functionalities. Training team.			
Cost structure		Revenue streams		
Personnel, licenses, Infrastructure providers.		Freemium schema. While the MEDINA tool is free of use, fees will be charged for implementing custom functionalities. Integration activities. Training activities		

### 7.1.7 Business model canvas for the MEDINA framework as a whole

MEDINA framework is the integration of the results described above, in order to offer an end-to-end solution, covering from the wish of a CSP to get certified to the maintenance of such certificate, with a special focus on the high assurance level, which requires the notion of continuous [8].

In the below table MEDINA framework is summarized in terms of Business model Canvas

Table 19 Business model canvas for Medina framework

MEDINA as a whole				
Key partners	Key activities	Value propositions	Customer relationships	Customer segments
Medina Partners' commercial networks. Standards Developing Organizations CSPs, Open source SW communities (OSS), Conformance Assessment Body (CAB), National Cybersecurity Certification Authorities (NCCA)	Implementation of validation scenarios (WP6)	Framework composed of tools and procedures to facilitate EUCS adoption and continuous compliance by CSPs.	B2C B2B. Consultancy, OSS communities	Cloud Service Providers (IaaS, SaaS, PaaS), connected services and IoT products (all market verticals) relying on cloud backends, Internal security governance teams at CSPs, auditors, NCCAs, CABs, ENISA
	Standardization activities and EUCS engagements with ENISA			
	Dissemination activities within commercial networks	Automation features for EUCS' CABs in order to reduce costs of involved processes for high assurance.	Channels	
	Iteration and release of integrated Medina platform		Open Source SW communities Independent SW Vendors (ISV's), events, consultancy & training services, partners' networks and platforms.	
	Key resources			
	HW: Medina validation infrastructure SW: GitHub repository Human : Sales team, MEDINA development team Training team Standardization & Dissemination teams			
Cost structure		Revenue streams		
Personnel, licenses, enablement & run costs for Infrastructure providers.		Freemium schema. While the MEDINA tool is free of use, fees will be charged for implementing custom functionalities and premium features. Integration activities. Training & consulting activities		

## 8 Conclusions

This deliverable has presented the business case, initial market analysis and business model canvas of the MEDINA framework and the associated Key results. The document has started with a brief description of the main benefits for the customers when applying each of the results of MEDINA.

A brief market analysis has been presented. For this, the market trends have been elucidated and the potential competitors of MEDINA as a whole as well as of the different Key results have been identified, at least in an initial version. In addition to that, the exploitation channels of each Key Result for each stakeholder, based on the notion of Persona, has been identified.

The regulatory framework is very important for a solution such as MEDINA as it can affect the exploitability. A brief analysis of which are the regulations that can have an effect on the sustainability of the solution has also been introduced.

Finally, the value propositions and the business model of the different Key results of MEDINA have been presented. In the case of the value propositions, the approach has been to identify which are the benefits that each of the stakeholders or Personas, would obtain thanks to MEDINA as a whole. The business model canvas, however, are presented per Key Result.

The need for continuous and automatic security assessment is growing among Cloud Service Providers, driven especially by the new regulatory frameworks such as the EU Cybersecurity Act. However, the existence of tools that is able to support, end to end, the automatic monitoring and auditing is rather limited as presented in this document.

Next versions of this document will include a more in-depth market analysis, updated versions of the business model canvas and value proposition and the business plan.

## 9 References

- [1] MEDINA Consortium;, “D6.1-Use cases specification and evaluation methodology-v1,” 2021.
- [2] MEDINA Consortium;, “D6.2-Use cases specification and evaluation methodology-v2,” 2021.
- [3] MEDINA, "MEDINA Description of Action".
- [4] MEDINA Consortium;, “D2.1 – Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v1,” 2021.
- [5] L. Orue-Echevarria, C. Cortés, M. Alvarez, B. Sanchez and A. Ayerbe, “Certification schemes for cloud computing,” EU Publications office, Luxembourg, 2018.
- [6] European Comision, “REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"),” Brussels, 2017.
- [7] S. R. a. C. S. A. a. F. o. O. Alain Pannetrat, “<https://cloudsecurityalliance.org/blog/2020/03/20/continuous-auditing-and-continuous-certification/>,” [Online].
- [8] MEDINA Consortium, “D5.1-MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v1,” 2021.
- [9] Gartner, “Innovation Insight for Cloud Security Posture Management”.
- [10] M. Palanisamy, “Top 10 Cyber Security Trends to Watch out for in 2021,” 12 November 2020. [Online]. Available: <https://www.appviewx.com/blogs/top-10-cyber-security-trends-to-watch-out-for-in-2021/>.
- [11] J. Armitage, “Compliance as code,” 12 2 2021. [Online]. Available: <https://www.contino.io/insights/compliance-as-code>.
- [12] “The Continuous Audit Metrics Catalog,” [Online]. Available: <https://cloudsecurityalliance.org/artifacts/the-continuous-audit-metrics-catalog/>.
- [13] European comision, “Digitising European Industry Reaping the full benefits of a Digital Single Market,” 2016.
- [14] Eurostat, “Cloud computing - statistics on the use by enterprises,” 2021.
- [15] European Comision, “REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the free flow of non-personal data in the European Union,” 2018.

- [16] ENISA, “Cybersecurity certification: lifting the EU into the cloud,” 2019. [Online]. Available: <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-certification-lifting-the-eu-into-the-cloud>.
- [17] ENISA, “Call 02/19 - Cloud Services WG,” 2019. [Online]. Available: [https://www.enisa.europa.eu/topics/standards/adhoc\\_wg\\_calls](https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls).
- [18] ENISA, “EUCS – CLOUD SERVICES SCHEME,” 2020.
- [19] European Comision, “A European strategy for data,” Brussels, 2020.
- [20] Federal Ministry for Economic Affairs and Energy -Germany, “GAIA-X: Policy Rules and Architecture of Standards,” 2020.
- [21] “The Business Model Analyst,” [Online]. Available: <https://businessmodelanalyst.com/value-proposition-canvas/>. [Accessed 25 04 2021].
- [22] “Wikipedia, Business\_Model\_Canvas,” [Online]. Available: [https://en.wikipedia.org/wiki/Business\\_Model\\_Canvas](https://en.wikipedia.org/wiki/Business_Model_Canvas). [Accessed 20 04 2021].
- [23] MEDINA Consortium, “D2.3 Specification of the Cloud Security Certification Language-v1,” 2021.
- [24] MEDINA Consortium;, “D3.1-Tools and techniques for the management of trustworthy evidence-v1,” 2021.
- [25] MEDINA Consortium;, “D3.4-Tools and techniques for collecting evidence of technical and organisational measures-v1,” 2021.
- [26] MEDINA Consortium;, “D4.1 Tools and Techniques for the Management and Evaluation of Cloud Security Certifications,” 2021.
- [27] Medina, “Use Cases Specification and Evaluation Methodology,” 2021.
- [28] Medina, “Use Cases Specification and Evaluation Methodology,” 2021.



## APPENDIX A: Key Results in MEDINA

The following table shows an excerpt of MEDINA’s Description of Action (DoA) document, containing the proposed Key Results (KR), and associated key performance indicators (KPI).

Table 20: Key results in MEDINA (source: [3])

Id	Key result (DoA)	Value Statement	Description	KPI
KR1	<b>Repository of Metrics and Measures</b>	<b>Standardized online Cloud Security Metrics, Controls &amp; TOMs Catalogue</b>	This result entails a clear definition of the technical and organizational measures relevant for cloud service providers, along with the corresponding security metrics (both quantitative and qualitative) for security objectives/TOMs such as those related to system security and integrity, operational security, business continuity and incident management.	<p>KPI 1.1: Provide realizable metrics for at least 70% of the technical measures referenced in major standard frameworks (i.e., the upcoming EU Cloud Security Certification, ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5, and the ENISA Metaframework).</p> <p>KPI 1.2: Provide a concrete proposal for semi-automated evaluation of metrics related to at least 50% of the organizational measures in major standard frameworks (i.e., the upcoming EU Cloud Security Certification ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5, and the ENISA Metaframework).</p>
KR2	<b>Risk-based selection of Controls to reach the Certification Assurance Levels</b>	<b>Support for threat and risk assessment</b>	MEDINA proposes a tool-supported methodology for the selection of controls and associated TOMs, which address the concrete needs of a CSP taking into consideration both its risk appetite and requested certification’s assurance level <sup>4</sup> . The tool shall be based on a risk-assessment methodology and in order to help CSP, as well as an auditor, to identify the key assets, threats and existing weaknesses of the cloud system. Identification of those elements should support stakeholders in	<p>KPI 2.1: a framework and a tool supporting the required functionality is developed and integrated into the certification framework.</p> <p>KPI 2.2 The Risk-assessment tool is empirically validated in at least one of the use cases.</p>

Id	Key result (DoA)	Value Statement	Description	KPI
			reflecting their chosen TOMs in accordance to their risk strategy, along with risk treatment options.	
<b>KR3</b>	<b>Certification Language</b>	<b>Machine readable certification language</b>	MEDINA will provide a language specification which expresses most relevant aspects of a security certification scheme in machine-readable format using a domain specific language (DSL). Transformation from textual representations of major standards will be done semi-automated using NLP (Natural Language Processing).	KPI 3.1: Contribute with a machine-readable certification language for specifying relevant elements of the proposed certification framework. Such elements include technical and organizational measures, quantitative/qualitative security metrics, complex compliance conditions, and cloud supply chain elements.
<b>KR4</b>	<b>Continuous evidence management tools</b>	<b>Trustworthy, Automatic &amp; Continuous Evidence gathering and management Tools</b>	This result entails the provision of tools and techniques to manage and collect trustworthy evidence validating the provided cloud security certification, both at code and at service level based on the repository of metrics (see KR1) and depending on the selected Conformity Assessment Methods (CAMs). They analyse the security of the cloud applications' source code using novel techniques from the field of static code analysis, such as code property graphs and analyse the configuration and log files of new computing paradigms such as serverless functions. Furthermore, organisational measures will be addressed by the use of semantic document analysis using NLP. Technologies such as Blockchain or DLT will be explored to provide trustworthiness of the gathered evidence across the whole life-cycle	KPI 4.1: Provide techniques for the continuous gathering of evidence related to the implementation of 100% of the technical measures contributed in KPI 1.1;  KPI 4.2: Provide a (set of) techniques for guaranteeing trustworthiness of gathered evidence, and that such evidence can be used in audit processes compliant with Conformity Assessment Methodologies for the certification scheme/assurance level defined in Point (9) Article 2 of the EU CSA. This refers to: (1) Evidence based conformity assessment; (2) Third party conformity assessment in accordance with ISO approach; and (3) Third party conformity assessment in accordance with International Standards on Assurance Engagements (ISAE) 3000/3402.

Id	Key result (DoA)	Value Statement	Description	KPI
			and guarantee that an evidence can be used in a specific CAM/EU CSA assurance level.	
KR5	<b>Cloud Certificate evaluator</b>	<b>Automatic &amp; Continuous Certificate Evidence Evaluator</b>	This result is responsible for defining the proper techniques and developing tools to evaluate the collected evidence (see KR4), with the needed properties to reach a particular certification target specified in a machine-readable way (see KR3) by evaluating the efficiency/efficacy of the chosen controls (cf., KR2).	<p>KPI 5.1: Contribute the evaluation techniques for cloud supply chains based on all three certification assurance levels defined in the EU Cybersecurity Act.</p> <p>KPI 5.2: Existence of tools that implement the defined evaluation techniques (cf., KR4).</p>
KR6	<b>Risk-based Auditor tool</b>	<b>Certificate Monitoring and management tool for Auditors</b>	The auditor tool will manage the whole life cycle of cloud security certification in MEDINA e.g., issuing and revocation, as well as publishing the certification result to a public registry (if provided by the certification body). It will monitor the continuous compliance of the CSP with respect to the security controls and conformity assessment methods. Similar to the selection of controls, it follows a risk-based approach which provides flexibility to the certification process: since an ever-changing threat landscape often requires timely reaction from the security team provoking changes in the security configurations. These could be efficient from the risk treatment point of view, but will affect the previously obtained certificate, in the worst case, invalidating it. Timely adjustment of the CSP's risk profile and re-evaluation of efficiency of its security configuration is	<p>KPI 6.1: TRL5-ready tool implementing the cloud security certification process contributed by the MEDINA framework (refer also to KR4 and KR5).</p> <p>KPI 6.2: TRL5-ready tool implementing certificate management based on at least 80% of the testing/validation techniques developed by KPI 3.1.</p> <p>KPI 6.3: TRL5-ready tool implementing the continuous audit-based certification as defined by the EU Cybersecurity Act.</p> <p>KPI 6.4: Provide one criterion for certifying tools that can be used in the context of the EU Cybersecurity Act (e.g., for continuous evidence gathering).</p>

Id	Key result (DoA)	Value Statement	Description	KPI
			therefore crucial to align both compliance and security teams. The developed tools will explore the automation and management of cloud certifications based on smart contracts.	
KR7	Use Cases	Verified MEDINA use cases in real environment	Use cases will offer MEDINA partners the possibility to assess the usefulness and suitability of the MEDINA approach/toolset in real cases of CSPs. MEDINA use cases will cover IaaS, PaaS and SaaS.	KPI 7.1: Tools developed by the project must be validated in at least three public cloud service providers.  KPI 7.2: At least 70% of the requirements of the previous KRs are validated in each use case, with an overall coverage of 100%.
KR8	Standardization roadmap	Impact to standardization	This entails activities performed in the context of standardization and standards observation.	KPI 8.1: Provide at least one standardization roadmap and one standardization report with the activities performed to contribute to a standard.
KR9	Training and awareness activities	Training	To disseminate the project results to a larger audience, dedicated training and awareness material will be produced. This, for example, includes materials for Massive Open Online Courses (MOOCs), social media and participation in workshops, conferences and other events. The scientific results of the projects will be published in scientific journals and conferences.	KPI 9.1: Support at least 3 high-impact awareness activities related to the contributed framework, and in alignment to the on-going EU CSA activities led by EC and ENISA.  KPI 9.2: Provide 4 training activities in the course of the project.