



MEDINA

Deliverable D3.3

Tools and techniques for the management of trustworthy evidence - v3

Editor(s):	Cristina Regueiro
Responsible Partner:	Fundación TECNALIA Research and Innovation (TECNALIA)
Status-Version:	Final – v1.0
Date:	30.04.2023
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	Tools and techniques for the management of trustworthy evidence – v3
Due Date of Delivery to the EC	30.04.2023

Work package responsible for the Deliverable:	WP3 - Tools to gather evidence for high-assurance cybersecurity certification
Editor(s):	Cristina Regueiro (TECNALIA)
Contributor(s):	Hrvoje Ratkajec (XLAB) Immanuel Kunz (FhG) Franz Josef Deimling (Fabasoft) Cristina Regueiro (TECNALIA)
Reviewer(s):	Marinella Petrocchi (CNR) Cristina Martínez (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	WP3, WP4, WP5 and WP6

Abstract:	This deliverable will encompass techniques on how to integrate different tools to gather and manage trustworthy evidence on various levels as well as on how to ensure the trustworthiness of evidence across the life-cycle, i.e., using Blockchain/DLT. There will be three iterations of the deliverable, an initial prototype, reflecting an early stage of integration in the technical framework (D3.1), the second release (D3.2) will be based on a refinement of the technical architecture, finally the third iteration (D3.3) will reflect the implementation of the use cases. This deliverable is the result of Task 3.1 and Task 3.5.
Keyword List:	Evidence, gathering tools, trustworthiness, Blockchain, EUCS
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	30.01.2023	First draft version of the TOC considering D3.2 as basis	Cristina Regueiro (TECNALIA)
v0.2	31.01.2023	Revised the description of VAT and Wazuh in Appendix D	Hrvoje Ratkajec (XLAB)
v0.3	14.02.2023	New GEC techniques description	Immanuel Kunz (FhG)
v0.4	30.03.2023	Updates on the Trustworthiness system	Cristina Regueiro (TECNALIA)
v0.5	05.04.2023	Minor updates on the text	Cristina Regueiro (TECNALIA)
v0.6	13.04.2023	QA internal review	Marinella Petrocchi (CNR)
v0.7	13.04.2023	Updates based on the internal review feedback	Cristina Regueiro (TECNALIA), Immanuel Kunz (FhG)
v0.8	24.04.2023	QA internal review	Cristina Martínez (TECNALIA)
V0.9	28.04.2023	Updates based on the internal review feedback	Hrvoje Ratkajec (XLAB) Immanuel Kunz (FhG) Franz Josef Deimling (Fabasoft) Cristina Regueiro (TECNALIA)
v1.0	30.04.2023	Ready for submission	Cristina Martínez (TECNALIA)

Table of contents

Terms and abbreviations.....	9
Executive Summary	11
1 Introduction	12
1.1 About this deliverable.....	12
1.1 Document Structure	12
1.2 Updates from D3.2.....	13
2 MEDINA Evidence Management Tools Architecture	14
2.1 Architecture	14
2.2 Data Model	18
2.3 Sequence Diagrams	21
2.3.1 Continuous Evidence Gathering and Collection	21
2.3.2 Security Assessment.....	24
2.3.3 Orchestrator	24
2.3.4 MEDINA Evidence Trustworthiness Management System.....	25
3 MEDINA Evidence Management Tools to Gather Evidence of High Assurance Level Requirements.....	29
3.1 Cloudfitor	29
3.2 Codyze.....	31
3.3 Vulnerability Assessment Tools (VAT)	31
3.4 Wazuh	32
3.5 Assessment and Management of Organisational Evidence (AMOE)	33
3.6 The Generic Evidence Collector (GEC)	34
3.6.1 Descriptions of Techniques	35
4 Coverage of EUCS requirements by the MEDINA Evidence Management Tools.....	48
5 MEDINA Evidence Trustworthiness Management System	54
5.1 Functional Description	54
5.1.1 Fitting into overall MEDINA Architecture.....	54
5.1.1 Component card	56
5.1.2 Requirements	59
5.2 Technical Description.....	60
5.2.1 Prototype architecture	60
5.2.2 Description of components	61
5.2.3 Technical specifications	72
5.3 Delivery and Usage	73
5.3.1 Package information.....	73
5.3.2 Installation instructions	73

5.3.3	User Manual	73
5.3.4	Licensing information	74
5.3.5	Download	74
5.4	Advancements within MEDINA.....	74
5.5	Limitations and Future Work	75
6	Checklist for the Self-assessment of EUCS security requirements	76
7	Conclusions	84
8	References	85
9	Appendix A: Current state of practice of Tools and Techniques in Management of Evidence 89	
9.1	Assessment of security performance configuration of cloud workloads	89
9.1.1	Cloud-Native Configuration Monitoring.....	89
9.1.2	Commercial tools.....	90
9.1.3	Standardized template export.....	90
9.2	Security assessment of computing infrastructure	91
9.2.1	Vulnerability assessment.....	91
9.2.2	Intrusion detection	91
9.3	Information of data flows in cloud applications	92
10	Appendix B: Assessment of Organizational Measures using NLP	94
10.1	Document types and methods	94
10.1.1	Dataset.....	94
10.1.2	Natural language text documents	95
10.2	Information extraction from log files	95
10.3	Difference analysis.....	95
10.3.1	Difference analysis on images	96
10.3.2	Difference analysis on textual documents	96
10.3.3	Bytewise Comparison	96
10.3.4	Difference analysis using document features	96
11	Appendix C: MEDINA Evidence Trustworthiness Management System API description	98
11.1	Blockchain account Management	98
11.2	Blockchain transactions generation: General system management	99
11.3	Blockchain transactions generation: Orchestrator's functionalities	101
12	Appendix D: EUCS Requirements coverage per tool within the MEDINA Evidence Management Tools	105
12.1	Cloudfoghorn	105
12.2	Codyze.....	109
12.3	VAT.....	112
12.4	Wazuh	116

12.5	AMOE	119
12.6	Generic Evidence Collector (GEC)	127
13	Appendix E: Self-assessment Questionnaires for EUCS basic requirements	131
13.1	Organization of Information Security	131
13.2	Information Security Policies	133
13.3	Risk Management	138
13.4	Human Resources	143
13.5	Asset management	150
13.6	Physical security	152
13.7	Operational security	158
13.8	Identity, Authentication and Access Management	170
13.9	Cryptography & Key management	179
13.10	Communications Security	183
13.11	Portability and Interoperability	190
13.12	Change and configuration management	193
13.13	Development of Information Systems	196
13.14	Procurement Management	200
13.15	Incident Management	202
13.16	Business Continuity	207
13.17	Compliance	209
13.18	User documentation	211
13.19	Dealing with Investigation Requests from Government Agencies	214
13.20	Product Safety and security	216

List of Tables

TABLE 1.	OVERVIEW OF DELIVERABLE UPDATES WITH RESPECT TO D3.2	13
TABLE 2.	SUMMARY OF THE 34 SELECTED REQUIREMENTS FROM THE AUGUST 2022 DRAFT CANDIDATE EUCS [3]	48
TABLE 3.	SUMMARY OF THE FINAL COVERAGE OF THE MEDINA EVIDENCE MANAGEMENT TOOLS FOR THE 34 HIGH LEVEL REQUIREMENTS FROM THE DRAFT CANDIDATE EUCS [3]	51
TABLE 4.	MEDINA EVIDENCE TRUSTWORTHINESS MANAGEMENT SYSTEM TECHNICAL SPECIFICATIONS	72
TABLE 5.	COVERAGE OF EUCS REQUIREMENTS BY THE MEDINA QUESTIONNAIRES	80
TABLE 6.	COVERAGE OF EUCS REQUIREMENTS BY THE MEDINA QUESTIONNAIRES FOR EACH EUCS CATEGORY	80
TABLE 7.	SUMMARY OF CLOUDITOR'S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2 .	105
TABLE 8.	SUMMARY OF ADDITIONAL REQUIREMENTS COVERAGE OF CLOUDITOR	108
TABLE 9.	SUMMARY OF CODYZE'S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2	109
TABLE 10.	SUMMARY OF VAT'S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2	113
TABLE 11.	SUMMARY OF WAZUH'S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2	116

TABLE 12. SUMMARY OF AMOE’S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2	119
TABLE 13. SUMMARY OF ADDITIONAL REQUIREMENTS COVERAGE OF AMOE	122
TABLE 14. SUMMARY OF GEC’S COVERAGE OF THE 34 EUCS HIGH LEVEL REQUIREMENTS IN TABLE 2	127
TABLE 15. CHECKLIST FOR OIS BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	131
TABLE 16. CHECKLIST FOR ISP BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	133
TABLE 17. CHECKLIST FOR RM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	138
TABLE 18. CHECKLIST FOR HR BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	143
TABLE 19. CHECKLIST FOR AM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	150
TABLE 20. CHECKLIST FOR PS BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	152
TABLE 21. CHECKLIST FOR OPS BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	158
TABLE 22. CHECKLIST FOR IAM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	170
TABLE 23. CHECKLIST FOR CKM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	179
TABLE 24. CHECKLIST FOR CS BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	183
TABLE 25. CHECKLIST FOR PI BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	190
TABLE 26. CHECKLIST FOR CCM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	193
TABLE 27. CHECKLIST FOR DEV BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	196
TABLE 28. CHECKLIST FOR PM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	200
TABLE 29. CHECKLIST FOR IM BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	202
TABLE 30. CHECKLIST FOR BC BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	207
TABLE 31. CHECKLIST FOR CO BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	209
TABLE 32. CHECKLIST FOR DOC BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	211
TABLE 33. CHECKLIST FOR INQ BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	214
TABLE 34. CHECKLIST FOR PSS BASIC ASSURANCE REQUIREMENTS (SOURCE: MEDINA’S OWN CONTRIBUTION)	216

List of Figures

FIGURE 1. BUILDING BLOCKS VIEW OF THE MEDINA FRAMEWORK (SOURCE: D5.2 [6]).....	15
FIGURE 2. ARCHITECTURE OF THE MEDINA EVIDENCE MANAGEMENT TOOLS.....	16
FIGURE 3. MEDINA FRAMEWORK DATA MODEL (SOURCE: D5.2 [6])	19
FIGURE 4. DETAIL OF THE DATA MODEL USED BY THE MEDINA EVIDENCE MANAGEMENT TOOLS.....	20
FIGURE 5. SEQUENCE DIAGRAM OF THE MEDINA EVIDENCE MANAGEMENT TOOLS ARCHITECTURE.....	23
FIGURE 6. SEQUENCE DIAGRAM OF THE MEDINA EVIDENCE TRUSTWORTHINESS MANAGEMENT SYSTEM TRUSTWORTHY EVIDENCE AND ASSESSMENT RESULTS STORAGE.....	26
FIGURE 7. SEQUENCE DIAGRAM OF THE MEDINA EVIDENCE TRUSTWORTHINESS MANAGEMENT SYSTEM VALIDATION PROCESS.....	28
FIGURE 8. SCHEMATIC OVERVIEW OF THE CLOUDITOR COMPONENTS (SOURCE: D3.6 [2])	30
FIGURE 9. SCHEMA OF WAZUH, VAT AND RELATED COMPONENTS (SOURCE D3.6 [2])	32
FIGURE 10. AMOE ARCHITECTURE AND CONNECTIONS TO OTHER MEDINA COMPONENTS.....	33
FIGURE 11. POSITION OF EVIDENCE TRUSTWORTHINESS MANAGEMENT SYSTEM WITHIN THE MEDINA ARCHITECTURE (SOURCE: D5.2 [6]).....	55
FIGURE 12. MEDINA EVIDENCE TRUSTWORTHINESS MANAGEMENT SYSTEM (SOURCE: MEDINA'S OWN CONTRIBUTION).....	60
FIGURE 13. QUORUM BLOCKCHAIN NODE ARCHITECTURE (SOURCE: MEDINA'S OWN CONTRIBUTION)	61
FIGURE 14. MEDINA TRUSTWORTHINESS MANAGEMENT SYSTEM DATA MODEL.....	64
FIGURE 15. POSTMAN COLLECTION FOR VALIDATING BLOCKCHAIN CLIENT API	66
FIGURE 16. BLOCKCHAIN VIEWER ARCHITECTURE (SOURCE: MEDINA'S OWN CONTRIBUTION).....	66
FIGURE 17. BLOCKCHAIN VIEWER GRAPHICAL INTERFACE FOR ADMINISTRATORS.....	69
FIGURE 18. BLOCKCHAIN VIEWER GRAPHICAL INTERFACE FOR ORCHESTRATOR OWNERS	70
FIGURE 19. AUTOMATIC VERIFICATION SERVICE HOME PAGE.....	71
FIGURE 20. AUTOMATIC VERIFICATION SERVICE FORM	71
FIGURE 21. AUTOMATIC CORRECT INTEGRITY VERIFICATION SERVICE	72
FIGURE 22. AUTOMATIC INCORRECT INTEGRITY VERIFICATION SERVICE	72
FIGURE 23. EVIDENCE-BASED CONFORMITY ASSESSMENT (ADAPTED FROM [35])	76
FIGURE 24. SUMMARY OF THE EUCS CATEGORIES IN THE MEDINA QUESTIONNAIRES	78
FIGURE 25. EXCERPT OF THE CHECKLIST FOR THE OPERATIONAL SECURITY CATEGORY.....	79
FIGURE 26. SCORECARDS FOR THE OPERATIONAL SECURITY CATEGORY IN MEDINA QUESTIONNAIRES.....	81
FIGURE 27. OVERALL SCORECARD IN MEDINA QUESTIONNAIRES.....	82
FIGURE 28. INTEGRATION OF THE CHECKLIST OF THE MEDINA QUESTIONNAIRES IN THE CATALOGUE OF CONTROLS AND METRICS (SOURCE D2.2[17])	83

Terms and abbreviations

AM	Asset Management
AMOE	Assessment and Management of Organisational Evidence
API	Application Programming Interface
AWS	Amazon Web Services
BC	Business Continuity
CAB	Conformance Assessment Body
CCM	Change and Configuration Management
CI/CD	Continuous integration / continuous deployment
CIS	Centre for Internet Security
CKM	Cryptography and Key Management
CO	Compliance
CPG	Code Property Graph
CS	Communication Security
CSC	Cloud Service Customer
CSA or EU CSA	EU Cybersecurity Act
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management tool
DAST	Dynamic application security testing
DEV	Development of Information Systems
DoA	Description of Action
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
GDPR	General Data Protection Regulation
GEC	Generic Evidence Collector
HIDS	Host-based Intrusion Detection Systems
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IaC	Infrastructure as Code
IaaS	Infrastructure as a Service
IAM	Identity, Authentication and Access Control Management
IDS	Intrusion Detection Systems
IM	Incident Management
INQ	Dealing with Investigation requests from government agencies
ISP	Information Security Policies
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KR	Key Result
HIDS	Host-based Intrusion Detection System
IM	Incident Management
NIDS	network-based IDS
NIST	National Institute of Standards and Technology
NLP	Natural language processing
OIS	Organizational Information Security
OPS	Operational Security
OSSEC	Open Source HIDS SECURITY

OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PI	Portability and Interoperability
PM	Procurement Management
PS	Physical Security
PSS	Product Security
RBAC	Role Based Access Control
REST	Representational State Transfer
RM	Risk Management
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SQL	Structured Query Language
UI	User Interface
DOC	User Documentation
VAT	Vulnerability Assessment Tools
VM	Virtual Machine

Executive Summary

This document aims to present the work related to the architecture of the *MEDINA Evidence Management Tools* [KR4] and the *MEDINA Evidence Trustworthiness Management System*, which aims to ensure that all evidence and assessment results are secured. The architecture, data model and sequence diagrams of the *MEDINA Evidence Management Tools* are proposed, extending the models already presented in D5.2 [1].

While the technical details of the tools that compose the *MEDINA Evidence Management Tools* [KR4] are presented in D3.6 [2], their main ideas and motivation are presented in this document. Moreover, the current coverage of the high assurance level requirements identified in the August 2022 draft candidate version of the EUCS scheme [3] has been matched with the different tools comprising the *MEDINA Evidence Management Tools*.

This document also presents the functional and technical details of the *MEDINA Evidence Trustworthiness Management System*, how it fits into the MEDINA framework, the architecture and description of the prototype and how it is delivered.

Finally, although MEDINA focuses mostly on the automated monitoring and the high-level assurance of the EUCS certification scheme, CSPs, especially the smaller ones, may still struggle in ensuring certification of non-automatable requirements. Therefore, the checklist presented in section 6 is aimed at these small CSPs so that they can be guided in their self – assessment and can know which kind of evidence they should provide to the CABs when carrying out a third-party assessment. This is an innovation brought in by MEDINA.

1 Introduction

1.1 About this deliverable

This document is the final iteration of *Tools and techniques for the management of trustworthy evidence*. It presents the final version of the tool used for trustworthy evidence management in MEDINA and the architecture of the *MEDINA Evidence Management Tools* [KR4]. The technical details of said tools are described in D3.6 [2]. The document also presents a checklist for EUCS-based security self-assessment.

1.1 Document Structure

The deliverable is structured as follows. Section 1 gives the context for the results reported in this document, its scope, structure, and mentions the relationship to other work in the MEDINA project as well as the modifications of this document in comparison with its second version, D3.2 [4].

Section 2 is devoted to the structural description of the *MEDINA Evidence Management Tools*, consisting of *Clouditor*, *Wazuh*, the *Vulnerability Assessment Tools (VAT)*, *Codyze*, *Assessment and Management of Organisational Evidence (AMOE)* and the *Generic Evidence Collector (GEC)*. All these tools convene into an orchestrator. This section explains the associated architecture, the data model, and the sequence diagrams.

Section 3 briefly introduces the tools that comprise the *MEDINA Evidence Management Tools*, and section 4 shows the coverage of said tools with respect to the high assurance level requirements requiring automated monitoring identified in the August 2022 draft candidate version of the EUCS scheme [3]. The values related to the KPIs have also be assessed.

Section 5 presents the final version of the *MEDINA Evidence Trustworthiness Management System*, including the functional description, the description of components, as well as the technical specifications and the delivery and usage.

Section 6 presents a self-assessment model for the basic, substantial and high assurance levels. This work is complementary to the work that MEDINA has done for the high assurance level requirements involving automated monitoring. The main target users of this work are small and medium CSPs.

Section 7 summarizes and briefly comments on the reported results.

Appendix A: Current state of practice of Tools and Techniques in Management of Evidence presents the current state of practice in the assessment of security performance configuration of cloud workloads, assessment of computing infrastructure and information of data flows, comparing them briefly to the solutions that MEDINA has developed.

Appendix B: Assessment of Organizational Measures using NLP describes some basics for the development of the AMOE tool, in particular related to the extraction of evidence based on metrics from certain documents linked to the organizational measures.

Appendix C: MEDINA Evidence Trustworthiness Management System API description contains the API description of the *MEDINA Evidence Trustworthiness Management System*, including return codes.

Appendix D: EUCS Requirements coverage per tool within the MEDINA Evidence Management Tools presents the EUCS 2022 requirements coverage for each of the evidence management tools: *Clouditor*, *Codyze*, *VAT*, *Wazuh*, *AMOE* and *GEC*.

Appendix E: Self-assessment Questionnaires for EUCS basic requirements presents the exhaustive checklist for self-assessment model developed for the requirements identified as basic assurance level.

1.2 Updates from D3.2

This deliverable evolves from D3.2 [4], so much of its content is common to that included in the previous document, with the ultimate goal of providing a self-contained deliverable that facilitates the reader's understanding. For simpler tracking of progress and updates with regards to the previous deliverable version (D3.2), Table 1 shows a brief overview of the changes and additions to each of the document sections.

Table 1. Overview of deliverable updates with respect to D3.2

Section	Change
2	<i>MEDINA Evidence Management Tools</i> architecture and data models have been updated. Additionally, the sequence flow of the <i>MEDINA Evidence Trustworthiness Management System</i> has been updated including the new automatic hashes verification service component.
3	The description of the tools has been updated and new Generic Evidence Collector techniques have been included.
4	The analysis of the draft version of the EUCS scheme has been updated (*), obtaining the final values for KPI1.1 and KPI 1.2.
5	The description of the <i>MEDINA Evidence Trustworthiness Management System</i> has been updated and extended with the new automatic verification service component. Section 5.1.1 (dedicated to the component card) is also added.
6	The description of the checklists has been updated.
7	Conclusions are aligned.
Appendix A	Appendix already present in D3.2, describing the current state of practice of tools and techniques in management of evidence
Appendix B	Appendix already present in D3.2, describing the assessment of organizational Measures using NLP.
Appendix C	Appendix already present in D3.2, describing the API of the <i>MEDINA Evidence Trustworthiness Management System</i>
Appendix D	Updated analysis of the coverage of the draft version of the EUCS scheme for each evidence gathering tool. (*)
Appendix E	Minor updates to the basic self-assessment questionnaires for the requirements defined in the draft version of the EUCS scheme. (*)

(*) Please note that the EUCS requirements referred in this deliverable correspond to a draft version of the ENISA catalogue, and are not intended for being used outside the context of MEDINA.

2 MEDINA Evidence Management Tools Architecture

This section presents the updated architecture of the *MEDINA Evidence Management Tools*, which integrates several tools, namely *Vulnerability Assessment Tool (VAT)*, *Wazuh*, *Clouditor*, *Codyze*, *Assessment and Management of Organisational Evidence (AMOE)* and *Generic Evidence Collector (GEC)*, as well as proprietary tools coming from the MEDINA use cases. This section aims to describe the architecture of this toolset, its data model, and its sequence diagrams.

The description contains much information in common with D3.2 [4] with the final aim of providing a self-contained section that facilitates the reader's understanding.

2.1 Architecture

The architecture of the MEDINA framework has been proposed in the deliverable D5.1 [5] and updated in D5.2 [6]. It is composed by several building blocks, as shown in Figure 1. Each building block corresponds to a well differentiated functionality of the proposed architecture, which has been updated to include the novel *GEC component*. In the case of evidence management, more than one of the depicted blocks take part in the whole process. More concretely, the processes involved are: (i) Organizational evidence gathering and processing (depicted as block n. 1 in Figure 1); (ii) Technical measures collection and assessment (depicted as block n. 2 in Figure 1); and (iii) Orchestration of evidence management and trustworthiness processing (depicted as block n. 3 in Figure 1).

- *Building block 1* of the MEDINA framework implements both a **repository for the organizational** evidence, as well as NLP-based techniques for their processing. This processing **assesses CSP-related documentation** (e.g., security concepts, operation manuals) for conformance with the certification scheme's requirements.
- Complementary to this functionality, *building block 2* of the MEDINA framework provides the **assessment of technical measures** by integrating a variety of tools (including native CSP functionalities). This building block targets the multi-layer assessment of the target-of-certification cloud service, i.e., the related IaaS, PaaS, and SaaS stack.
- All the assessment results, obtained either from the gathered organizational or technical measures, are holistically **processed, stored and tamper-proofed** by the components shown in *building block 3*. This block also shows the *Orchestrator*, the component responsible for launching and stopping the rest of components as well as forwarding the data it receives.

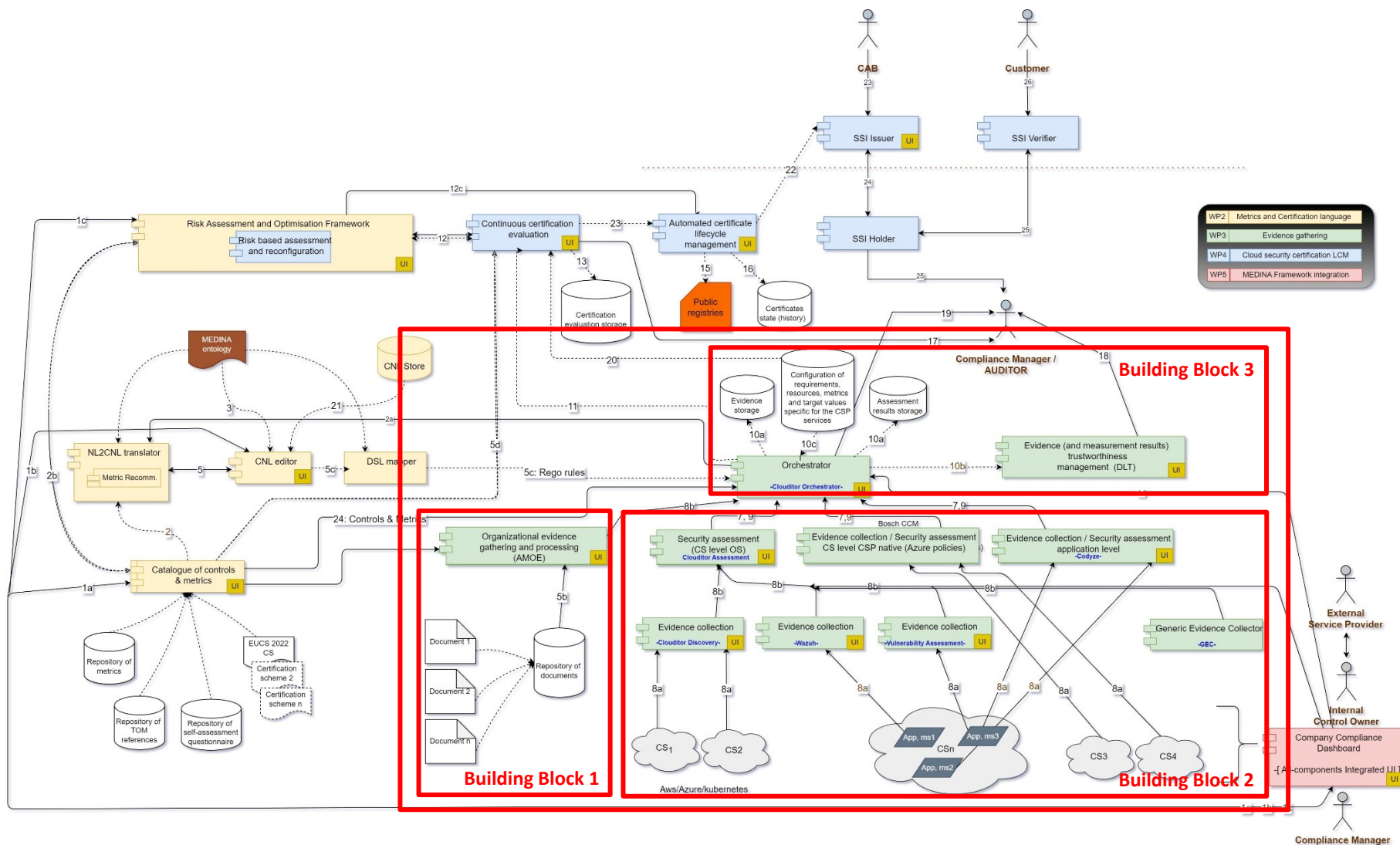


Figure 1. Building blocks view of the MEDINA framework (source: D5.2 [6])

Figure 2 shows a more detailed architecture of the components involved in evidence management, which is described in the following paragraphs. All relevant tools in this document are depicted in green.

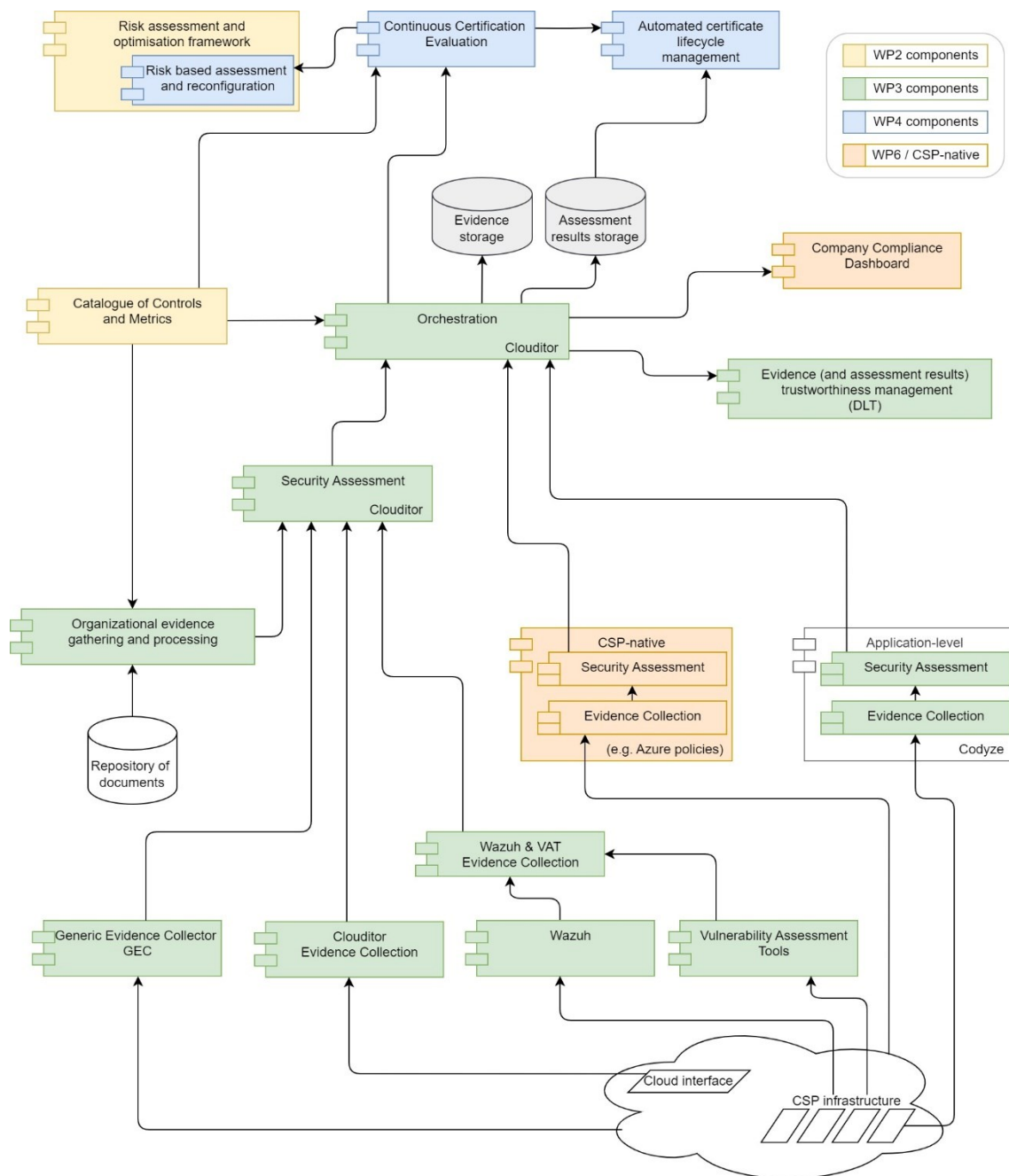


Figure 2. Architecture of the MEDINA Evidence Management Tools

Continuous Evidence Gathering and Collection Tools

This component collects evidence from the CSP infrastructure and posts it to the *Security Assessment* component. Evidence can be of different nature and is gathered by different tools¹:

¹ The interested reader can find more information in D3.6 [2]

- Technical Evidence Collection tools, that gather evidence from the CSP infrastructure (e.g., *Clouditor*, *Wazuh*, *VAT* or *GEC*).
- Application-Level Evidence Collection tools, that gather evidence from the static code analysis or specifications of applications (e.g., *Codyze*).
- Organizational Evidence Gathering tools, that automatically collect organizational evidence by examining the *Repository of Documents* and transform this evidence in the form of technical evidence (e.g., *AMOE* that uses Natural Language Processing (NLP)).

Security Assessment

The *Security Assessment* component assesses evidence from the evidence collection tools and pushes the results to the *Orchestrator*. It first obtains existing metrics (from the *Catalogue of Controls and Metrics*²), and uses them to assess incoming evidence via a policy engine. Figure 5 shows the sequence diagram.

Orchestrator

The *Orchestrator* is the central component in the MEDINA framework, and as such it is responsible for launching and stopping components in the *MEDINA Evidence Management Tools*, as well as forwarding data to other components. The *Orchestrator* receives evidence and assessment results from the *Security Assessment* and stores them. In addition, it posts (checksums of) evidence and assessment results to the *MEDINA Evidence Trustworthiness Management System*, and also forwards assessment results to the *Continuous Certification Evaluation* for evaluating them³.

The main sub-components of the *Orchestrator* are the two databases for the storage of evidence and assessment results.

MEDINA Evidence Trustworthiness Management System

The *MEDINA Evidence Trustworthiness Management System* provides a secure mechanism to maintain an audit trail of evidence and assessment results involved in the auditing process. It is implemented by means of Smart Contracts backbone by a Blockchain network.

The sub-components of the *MEDINA Evidence Trustworthiness Management System* are:

- Blockchain client, needed by the *Orchestrator* to interact with the Blockchain.
- Blockchain network with the required Smart Contracts to provide the trustworthy functionality.
- Blockchain monitor listening to events from the Smart Contracts.
- Blockchain monitor client to consume the information in the monitor and provide it graphically to auditors.
- Automatic verification service of the evidence and assessment results recorded on the Blockchain.

Every time a new evidence or assessment result is received, the *Orchestrator* writes the corresponding trustworthy information into the component. Then, the *MEDINA Evidence Trustworthiness Management System* generates an event with the information in the Blockchain, which is shown by the Blockchain monitor. At any time, the evidence and

² *Catalogue of Controls and Metrics* is developed in the scope of WP2 and reported in D2.2 [5].

³ The interested reader can find more information in D4.3 [7].

assessment results recorded on the Blockchain can be validated against their current values (by the *Orchestrator*). The interested reader can find more information in section 5.

2.2 Data Model

The data model of MEDINA framework has been described in the aforementioned architecture deliverable (D5.2 [6]). It describes the different data entities MEDINA components deal with. Figure 3 shows how the entities have been categorized into different groups depending on the building block they belong to.

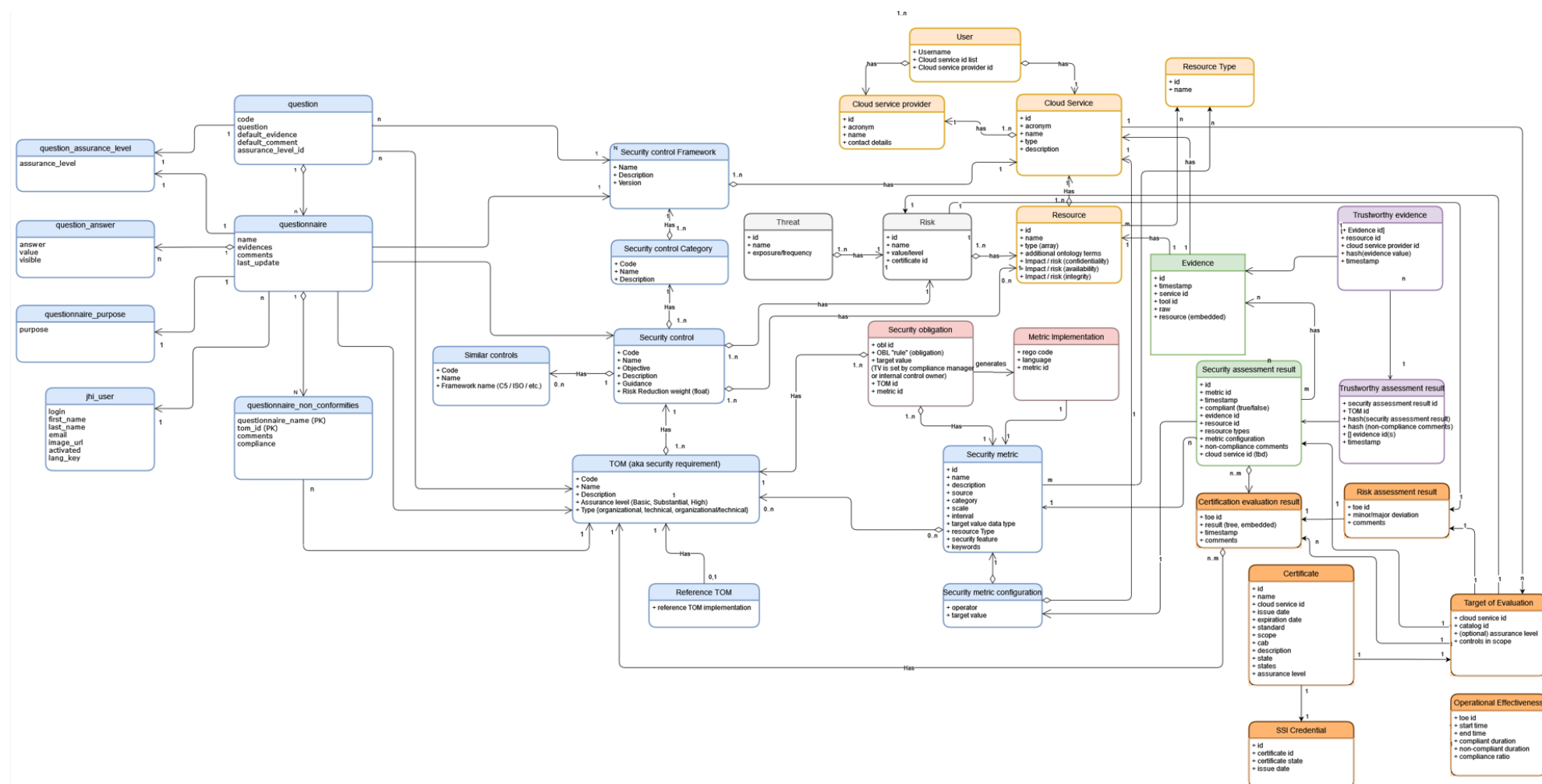


Figure 3. MEDINA framework data model (source: D5.2 [6])

Figure 4 shows a more detailed diagram, extracted from Figure 3, that represents only those entities that have relation with the *MEDINA Evidence Management Tools*, their attributes, and relations. The colour code is as follows:

- **Green** entities correspond to evidence gathering and assessment.
- **Purple** entities correspond to evidence trustworthiness or assessment result trustworthiness.

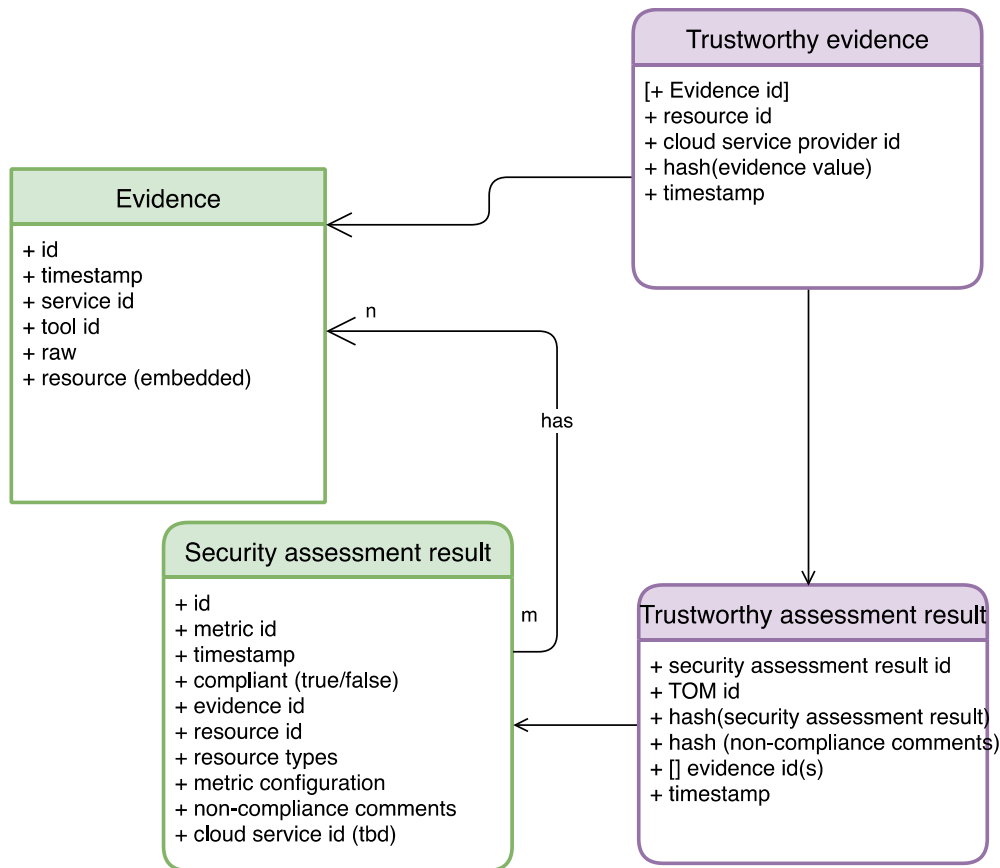


Figure 4. Detail of the data model used by the MEDINA Evidence Management Tools

The elements that appear in this entity-relation diagram are described below.

Security assessment result: is the outcome of assessing a piece of evidence against existing metrics (performed by the *Security Assessment* component).

Examples:

- Compliant
- Non-compliant

Every Security assessment result *is linked to* one or more pieces of **Evidence**, and has a **Trustworthy assessment result** that *represents* it.

Evidence: is the existence or verity of something. Objective evidence can be obtained through observation, measurement, test, or by other means. Objective evidence for the purpose of audit generally consists of records, statements of fact or other information which are relevant to the audit criteria and verifiable.

Examples:

- Terraform template for VM being assessed
- Audit logs from S3 bucket
- Documented security policy and procedures of a CSP

Every piece of evidence has a linked **Trustworthy evidence** which *represents* it.

Trustworthy evidence: is the representation of a piece of evidence produced, stored, and managed by the *MEDINA Evidence Trustworthiness Management System*. This component - based on digital signatures and Blockchain technology- guarantees that all the information stored is trustable, and even more, that every piece of data can always be traced back to its creator. Basically, this entity consists of a hash of the evidence and also includes a timestamp.

Trustworthy assessment result: is the representation of a Security assessment result produced, stored, and managed by the *MEDINA Evidence Trustworthiness Management System*. It includes a hash of the assessment result and a hash of the (possible) non-compliance comments, along with the timestamp. It stores a list of evidence ids produced by the Security Assessment Result and is *linked to* one or more pieces of **Trustworthy evidence**.

2.3 Sequence Diagrams

This section describes the components of the *MEDINA Evidence Management Tools* architecture using sequence diagrams.

2.3.1 Continuous Evidence Gathering and Collection

The *Continuous evidence gathering and collection* component (a.k.a. *Evidence Collection*) is used to collect evidence from CSPs and post it to the *Security Assessment* for further processing. The components related to the *Continuous evidence gathering and collection* are as follows:

- *Evidence Collection tools*, e.g., *Cloud Evidence Collector* or *Wazuh*
- *Security Assessment tools*, e.g., the *Security Assessment*
- *Database for the storage of evidence*
- *Database for the storage of assessment results*

In order to be able to collect and store evidence, the tools involved must first be registered. The registration steps can be found in steps 1 and 2 (see Figure 5).

1. The *Evidence Collection* tool must be registered in the *Security Assessment* tool so that the *Security Assessment* can trigger them.
2. The *Security Assessment* tool must be registered in the *Orchestrator* to enable the *Orchestrator* to trigger the appropriate *Security Assessment* tool.

Steps 3 and 4 start the evidence collection process (see Figure 5):

3. The *Orchestrator* triggers the *Security Assessment* tool to start the assessment by sending the required metric IDs.
4. The *Security Assessment* tool triggers the *Evidence Collection* tool to start collecting evidence based on the metric IDs.

The actual gathering and collection of evidence takes place in steps 5 and 6 (see Figure 5):

5. The *Evidence Collection* tool starts the monitoring of the CSPs based on the metric IDs.

6. The *Evidence Collection* tool posts all evidence to the *Security Assessment* tool for future processing and storing.

Finally, the *Orchestrator* stores evidence in step 13 (see Figure 5) to the corresponding *Database for evidence*. If the *Evidence Collection* tool should stop, the *Orchestrator* sends a stop statement in step 15 with the corresponding metric ID which is passed on by the *Security assessment*.

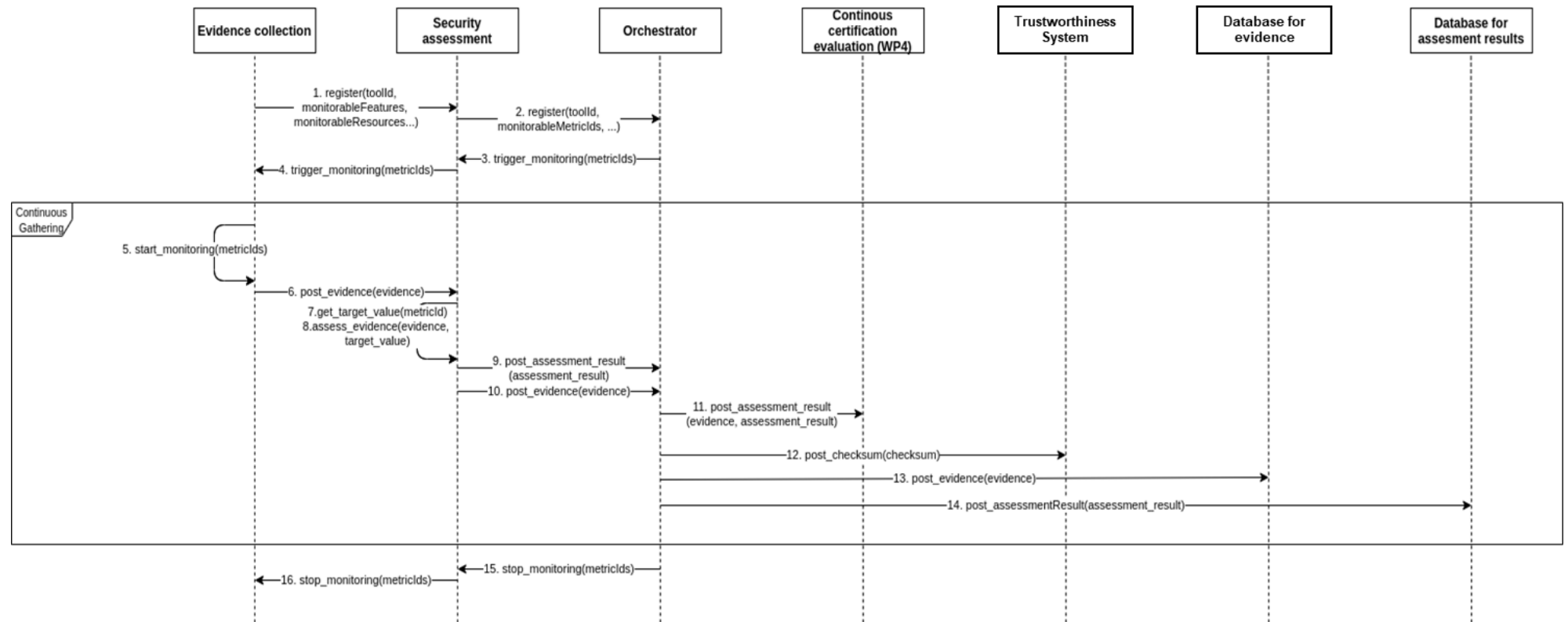


Figure 5. Sequence diagram of the MEDINA Evidence Management Tools architecture

2.3.2 Security Assessment

The *Security Assessment* tool assesses evidence from the *Evidence Collection* tools and pushes the results to the *Orchestrator*. Figure 5 shows the sequence diagram. Please note that the registration of the *Evidence Collection* tools in step 1 has already been described in section 2.3.1. The necessary components for the security assessment process are as follows:

- *Evidence Collection* tools, e.g., *Clouditor* or *Wazuh*
- *Orchestrator*

Step 3 triggers the *Security* assessment and step 4 triggers the *Evidence collection* tool (see Figure 5). Both steps are part of the security assessment.

3. The *Orchestrator* triggers the *Security Assessment* tool to start the assessment by sending the required metric IDs.
4. The *Security Assessment* tool triggers the *Evidence Collection* tool to start collecting evidence based on the metric IDs.

The actual security assessment takes place in steps 6-10 (see Figure 5):

6. The *Security Assessment* gets the evidence from the *Evidence Collection* tool.
7. The *Security Assessment* gets the target values based on the metric ID contained in the evidence.
8. The *Security Assessment* starts the assessment by using the evidence and the target value of step 7. The result is stored in the assessment result.
9. The *Security Assessment* posts the assessment result to the *Orchestrator* and in a later step the *Orchestrator* stores the assessment result in the database (step 14).
10. The *Security Assessment* posts the evidence to the *Orchestrator* and in a later step the *Orchestrator* stores the evidence in the database (step 13).

If the *Security Assessment* should stop, the *Orchestrator* sends a stop statement in step 15 with the corresponding metric ID which is passed on by the *Security assessment*.

2.3.3 Orchestrator

The *Orchestrator* is the central component in the MEDINA framework and is responsible for launching and stopping components in the *MEDINA Evidence Management Tools*, as well as forwarding data to other components. Figure 5 shows the corresponding sequence diagram. The important components that the *Orchestrator* interacts with are the following:

- *Security Assessment*
- *Continuous Certification Evaluation*⁴
- *MEDINA Evidence Trustworthiness Management System*
- *Database for evidence*
- *Database for assessment results*

The *Security Assessment* tools are registered in the *Orchestrator* as shown in step 2 and step 3 (see Figure 5):

2. The *Security Assessment* tool must be registered in the *Orchestrator* to enable the *Orchestrator* to trigger the appropriate *Security Assessment* tool.

⁴ CCE is developed in the scope of WP4 and reported in D4.3 [54]

3. The *Orchestrator* triggers the *Security Assessment* tool to start the assessment by sending the required metric IDs.

The relevant steps of the *Orchestrator* are steps 9-14 as follows (see Figure 5):

9. The *Orchestrator* gets the evidence from the *Security Assessment*.
10. The *Orchestrator* gets the assessment result from the *Security Assessment*.
11. The *Orchestrator* posts the assessment result to the *Continuous Certification Evaluation* for evaluating the result.
12. The *Orchestrator* posts the checksum of the assessment result to the *MEDINA Evidence Trustworthiness Management System*.
13. The *Orchestrator* stores the evidence in the *Database for evidence*.
14. The *Orchestrator* stores the assessment result in the *Database for assessment results*.

2.3.4 MEDINA Evidence Trustworthiness Management System

Figure 6 and Figure 7 show the sequence diagram of the *MEDINA Evidence Trustworthiness Management System*. The *Orchestrator* is the only MEDINA component with access to it, providing the trustworthy information about evidence and assessment results or checking previously recorded values in order to verify the integrity of information.

The *MEDINA Evidence Trustworthiness Management System* is composed of:

- Blockchain client, needed by the *Orchestrator* to interact with the Blockchain.
- Blockchain network with the required Smart Contracts, to provide the trustworthy functionality.
- Blockchain viewer, listening to events from the Smart Contracts.
- Blockchain viewer Client, to consume the information in the Viewer and provide it graphically to auditors.
- Automatic verification service, for current and recorded evidence and assessment results automatic validation.

The sequence of events for storing new data in the *MEDINA Evidence Trustworthiness Management System* is as follows (see Figure 6):

- The *Orchestrator* permanently writes the trustworthy information (hashes) about evidence or assessment results every time a new evidence or assessment result is received.
- Every time new trustworthy data about evidence or assessment results is written in the Blockchain, an event with the information is generated.
- As the Blockchain viewer is permanently listening to the events from the *MEDINA Evidence Trustworthiness Management System* in Blockchain, it will receive all the Blockchain events.
- The viewer client will be subscribed to the interesting events in the Viewer to graphically show the important information.

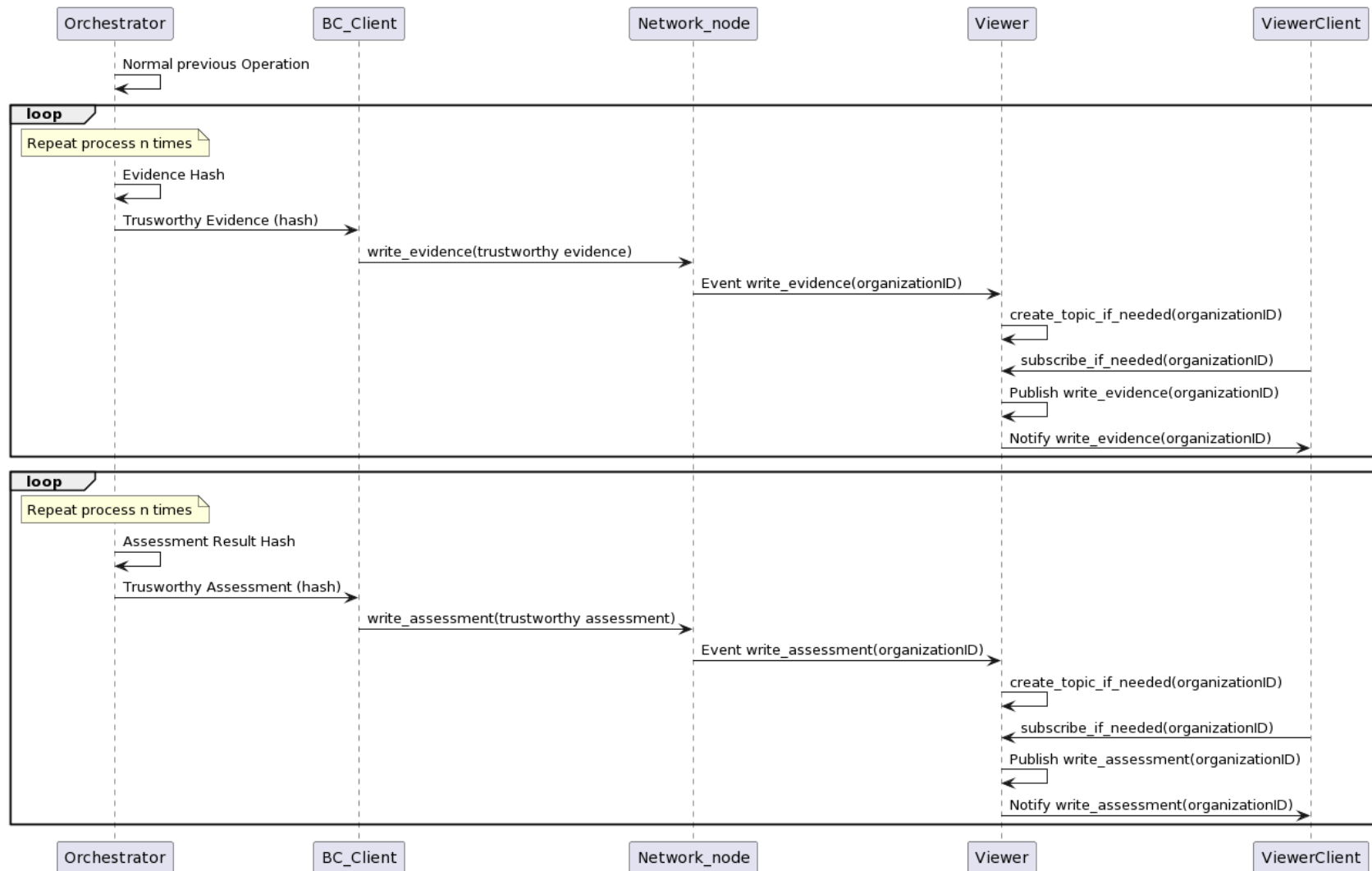


Figure 6. Sequence diagram of the MEDINA Evidence Trustworthiness Management System trustworthy evidence and assessment results storage

Once some trustworthy data about evidence and assessment results is recorded in the *MEDINA Evidence Trustworthiness Management System*, the validity of a specific data can be also verified in the following ways (see Figure 7):

- **Manual validation:** The *MEDINA Evidence Trustworthiness Management System* provides a graphical dashboard (viewer client) to access the information recorded in the Blockchain and to be able to perform manual validations. For this purpose:
 - The user (auditor) looks for a specific evidence or assessment result ID and obtain its value from the *Orchestrator*.
 - The user manually calculates the hash of the obtained information (evidence or assessment result).
 - The user looks for the specific evidence or assessment result ID and obtain its previously recorded hash on the Blockchain through the graphical interface (Monitor).
 - Both hashes can be compared to identify if the obtained evidence or assessment result value has been tampered or modified.
- **Automatic verification:** The *MEDINA Evidence Trustworthiness Management System* also includes a local automatic verification service for the validation of evidence and assessment results recorded on the Blockchain, obtaining directly a true/false result of the evidence and assessment result validity. For this purpose:
 - The user (auditor) interacts with the automatic verification service providing the evidence or assessment result ID he is interested in.
 - The automatic verification service will automatically obtain the specific evidence or assessment result from the *Orchestrator*, calculate the hash and compare it with the previously recorded hash on the Blockchain.
 - The positive or negative result is then shared with the user.

The interested reader is referred to the deliverable D4.3 [7] for more details.

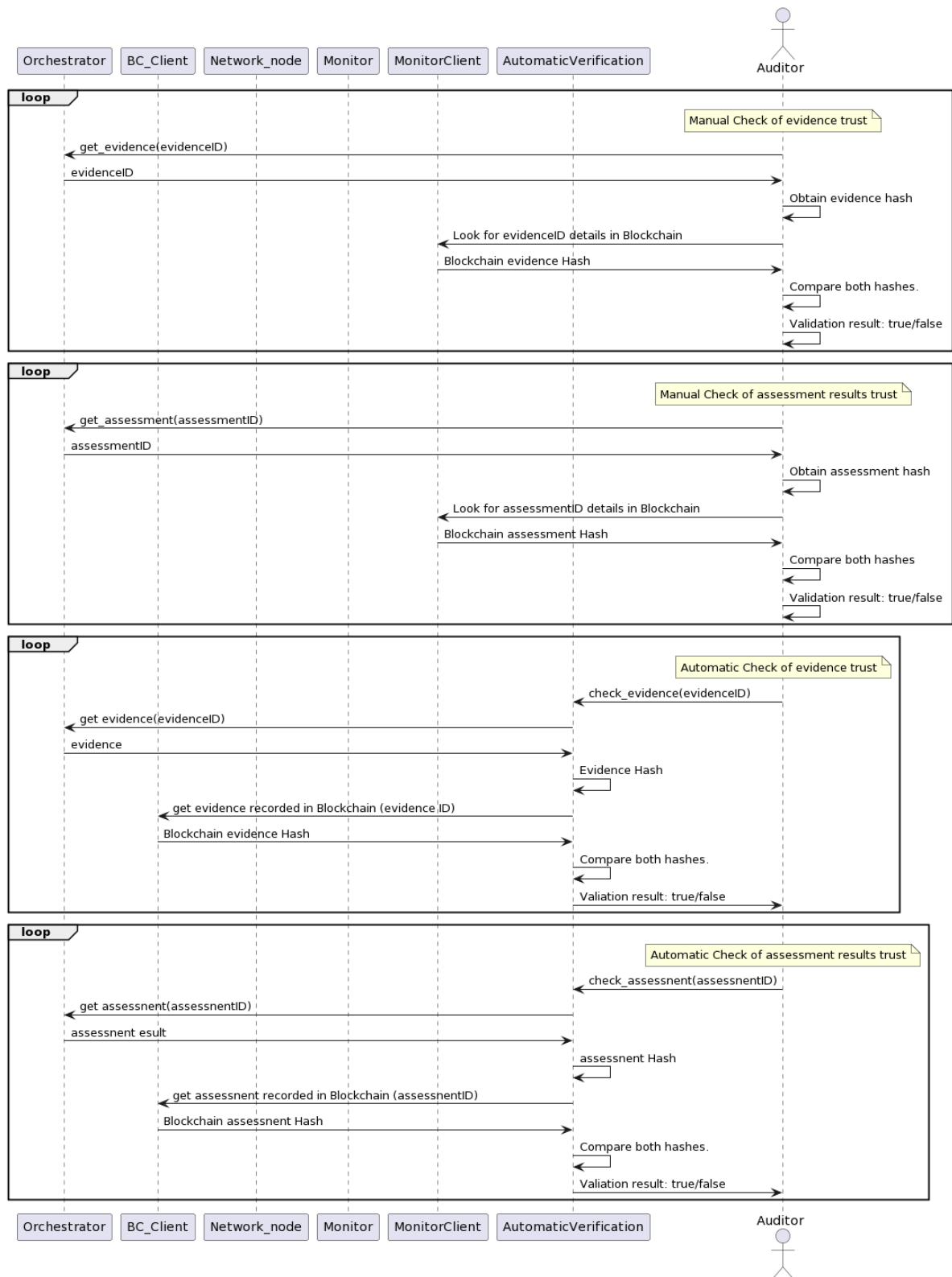


Figure 7. Sequence diagram of the MEDINA Evidence Trustworthiness Management System validation process

3 MEDINA Evidence Management Tools to Gather Evidence of High Assurance Level Requirements

This section briefly presents the tools that aim to close the gap between the current state of practice (see *Appendix A: Current state of practice of Tools and Techniques in Management of Evidence*), the requirements coming from the draft candidate version of the EUCS scheme [3], the MEDINA framework requirements (see D5.2 [6]) and the use cases' needs (see D6.2 [8]).

The description included in this section contains much information in common with D3.2 [4] with the final aim of providing a self-contained section that facilitates the reader's understanding.

As a recap, the *MEDINA Evidence Management Tools* component as explained in section 2 is composed of several tools: *Clouditor*, *Codyze*, *Vulnerability Assessment Tool (VAT)*, *Wazuh. Assessment and Management of Organisational Evidence (AMOE)* and the novel *Generic Evidence Collector (GEC)*. The updated technical details of these *MEDINA Evidence Management Tools* (implementation and user manual) can be found in the deliverable D3.6 [2].

3.1 Clouditor

Clouditor [9] is an open-source cloud assurance tool with the main goal to continuously evaluate if cloud resources are configured in a secure way and comply with requirements defined by the ENISA draft candidate scheme EUCS, such as data backup and recovery, logging, or data transmission security. *Clouditor* consists of three components that are depicted in Figure 8:

- *Cloud Evidence Collector*, for gathering evidence from the CSP.
- *Security Assessment*, to assess evidence against metrics and determine the compliance status.
- *Orchestrator*, as a central tool for launching components of the *MEDINA Evidence Management Tools* and directing data flows between components.

The *Cloud Evidence Collector* component discovers resource properties from various CSPs (e.g., AWS S3) and maps the collected data to *evidence* according to the MEDINA evidence data model, including the ontology terms defined in D2.5 [10]. For example, the ontology defines a common term for virtual machines ("VirtualMachine") across cloud providers – independently of their cloud provider-specific naming, like "EC2 Instance" in AWS. This common term is added to the evidence to allow the Security Assessment to apply appropriate metrics to the evidence (by the Ontology Mapper shown in Figure 8).

The *Security Assessment* component provides an interface to the *Evidence Collection* tools (see section 2.3.1) of which the *Cloud Evidence Collector* is just one example. Evidence is assessed against the metrics it retrieves from the *Orchestrator*, and then both the evidence and the assessment results, are sent to the *Orchestrator*. In this way, auditors can also review the original detailed evidence along with the assessment results.

The *Orchestrator* component is a central link in the MEDINA framework and is responsible for launching the rest of the *MEDINA Evidence Management Tools* and for directing the data flow between components also across components of different work packages. The tasks of the *Orchestrator* are as follows:

- Trigger the *Evidence Collection* tools, e.g., the *Cloud Evidence Collector*, for collecting evidence.
- Retrieve metrics from the *Catalogue of Controls and Metrics*.
- Provide metrics to the assessment component(s).

- Receive evidence and assessment results from the assessment components, such as the *Clouditor Security Assessment*.
- Securely store evidence and assessment results.
- Send assessment results to the *Continuous Certification Evaluation* component.
- Send checksums of evidence and assessment results to the *MEDINA Evidence Trustworthiness Management System*.

Connections to other components are defined and provided through APIs. An interface is provided for all assessment components which, in addition to the assessment results, also offers the possibility to send evidence. For the storage of evidence and assessment results in databases, interfaces to the *Evidence storage* and the *Assessment result storage*, respectively, are provided.

The *Clouditor* tool with its components is described in further detail in Deliverable D3.6 [2].

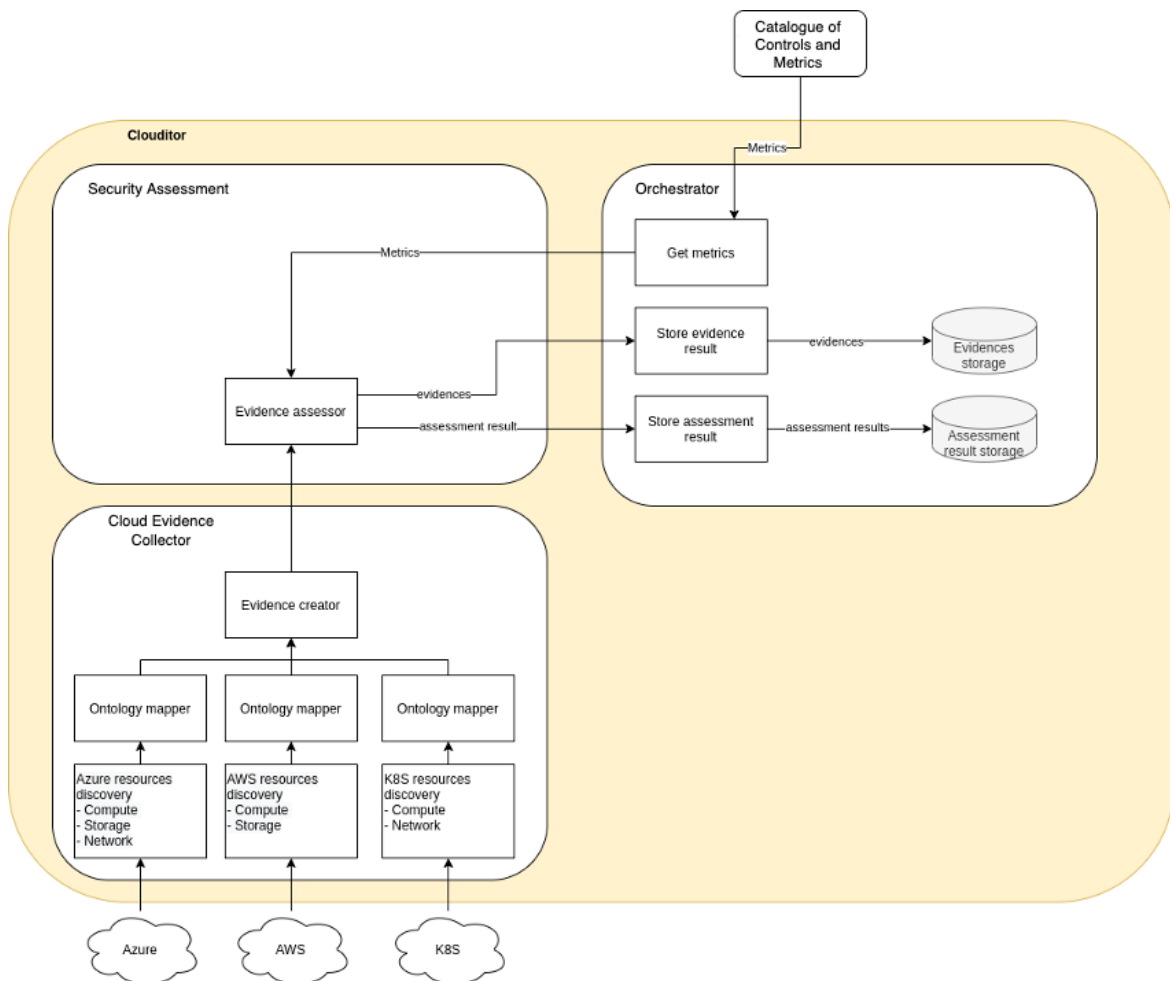


Figure 8. Schematic overview of the Clouditor components (source: D3.6 [2])⁵

⁵ Note that some integrations are missing in the figure, e.g., the *Orchestrator* forwards assessment results to the *Continuous Certification Evaluation* component and respective hashes to the *MEDINA Evidence Trustworthiness Management System*

3.2 Codyze

Codyze [11] is a static code analysis tool that focuses on verifying security compliance in source code, i.e., by inferring the correct use of cryptographic libraries. It operates on code property graphs and can handle non-compiling or even incomplete code fragments. It also aims at helping developers to generate “*insights into coding patterns of Java and C language coding automatically*”⁶.

Codyze collects and assesses evidence from the source code of cloud applications. It can be integrated into a CI/CD pipeline to collect evidence automatically and generate security assessments for further processing in environments such as Eclipse, IntelliJ, VSCode, and Visual Studio Code.

Codyze uses a domain-specific language called MARK⁷ to specify what properties source code must exhibit to be considered secure. MARK defines rules that *Codyze* evaluates. Rules are provided with *Codyze* and linked to metrics. An evaluation result of a rule can be a piece of evidence or an assessment result. The details depend on the specified rule.

Codyze represents an evidence collection tool (see Figure 2) that generates evidence according to the MEDINA data model. If *Codyze* can assess the evidence based on MARK rules, it generates assessment results. Evidence and assessment results are submitted to the *Orchestrator* for further processing, presentation, and inspection.

The technical implementation details of *Codyze* can be found on D3.6 [2].

3.3 Vulnerability Assessment Tools (VAT)

Vulnerability Assessment Tools (VAT) act as a modular vulnerability detection and scanning framework, thus representing an evidence collection tool (see Figure 2) that generates evidence according to the MEDINA data model. VAT is composed of several integrated vulnerability scanner tools and a possibility to easily include custom scripts to monitor the infrastructure either for availability or to detect specific threats. Scanning tasks can be configured to run periodically on a schedule, triggered manually, or integrated into various CI workflows.

CSPs can use *VAT* to satisfy some EUCS requirements by gathering evidence for those requirements related to vulnerability detection, use of encrypted communication, detection of new devices in the network, etc.

Once installed within the CSP infrastructure, *VAT* builds evidence containing measurements performed on the monitored resources and sends this evidence to the *Security Assessment* component for further processing. Figure 9 shows the schema of the closely related components of *VAT* and interactions between them. The interaction with other MEDINA components is implemented with the use of an *Evidence Collector* component that also interacts with *Wazuh* (see section 3.4). The (*Wazuh* & *VAT*) *Evidence Collector* periodically queries *VAT*'s APIs to examine its configuration and scan results in order to determine compliance with various metrics and generate the respective evidence.

Internally, *VAT* consists of several micro-services: a scheduler that periodically triggers scanning tasks, an API server for external communication, a collection of Docker images that contain the vulnerability scanners (w3af [12], OWASP ZAP [13], Nmap [14]) and some logic to interact with

⁶ <https://tracxn.com/d/companies/codyze.io>

⁷ <https://github.com/Fraunhofer-AISEC/codyze-mark-eclipse-plugin>

other VAT components, a database for storing results, and a web-based user interface for the configuration and review of scanning results.

The VAT tool is described in more detail in deliverable D3.6 [2].

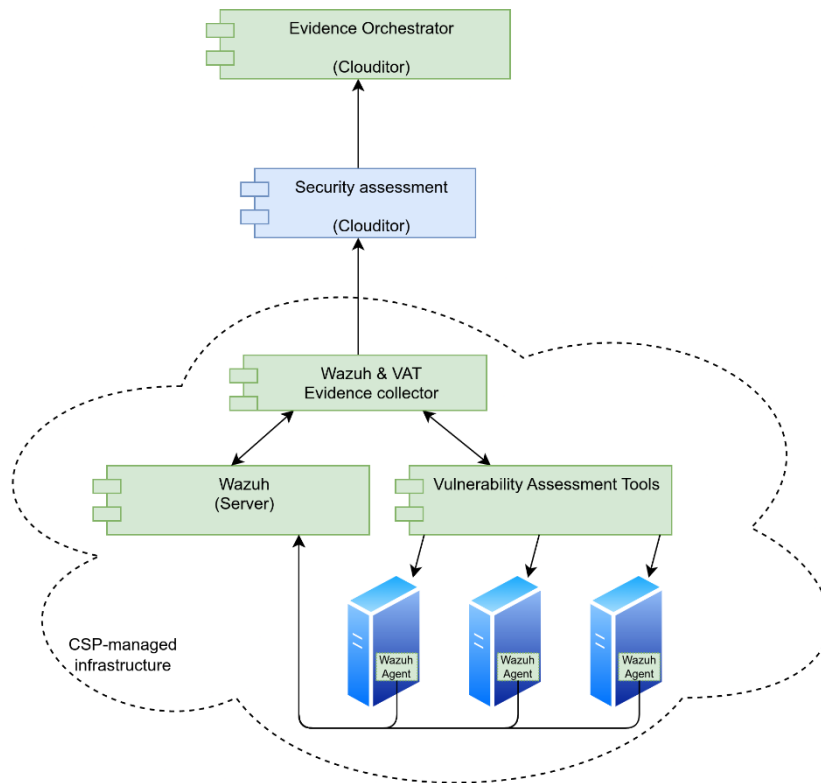


Figure 9. Schema of Wazuh, VAT and related components (source D3.6 [2])

3.4 Wazuh

Wazuh [15] is an open-source host-based intrusion detection system (HIDS) with multiple modules that support (SIEM-like) security analytics, log data analysis, file integrity monitoring, vulnerability detection, and other defensive security tasks. It is an evidence collection tool (see Figure 2) that generates evidence according to the MEDINA data model.

In the scope of MEDINA, *Wazuh* is offered to the CSPs as a security solution that can help to check several EUCS requirements on malware protection, logging, threat analytics, and automatic monitoring (alerting). It can also serve as an integration point for a variety of other solutions that produce log files. If erroneous or anomalous log entries appear, *Wazuh* can alert the user according to the configured rules. By using *Wazuh* at the CSP's side, the MEDINA framework can gather information about the configuration of its modules, providing evidence of compliance with various certification requirements.

The deployment of *Wazuh* consists of several *Wazuh* agents, programs installed on the monitored machines, and a *Wazuh* server that gathers data from the agents and acts as their *Orchestrator*. The *Wazuh* server also contains an Elasticsearch database with a modified Kibana user interface for easier analytics. As presented in Figure 9, *Wazuh* is connected to the MEDINA components through an *Evidence Collection* component, which connects to *Wazuh*'s APIs to examine the configurations and possible alerts detected, and based on this data generates evidence about the fulfilment of the respective metrics.

The Wazuh tool is described in more detail in deliverable D3.6 [2].

3.5 Assessment and Management of Organisational Evidence (AMOE)

The *Assessment and Management of Organisational Evidence (AMOE)* tool is an open-source program, developed to enable evidence extraction and assessment of policy documents. *AMOE* uses specifically developed organisational metrics that aim to measure concrete parts or values in policy documents.

Figure 10 depicts the architecture of the tool and the connections to other MEDINA components with which it interacts directly, namely the *Catalogue of Controls and Metrics*⁸ and the *Orchestrator*. For further details on the functional and technical description of *AMOE*, the interested reader is referred to deliverable D3.6 [2].

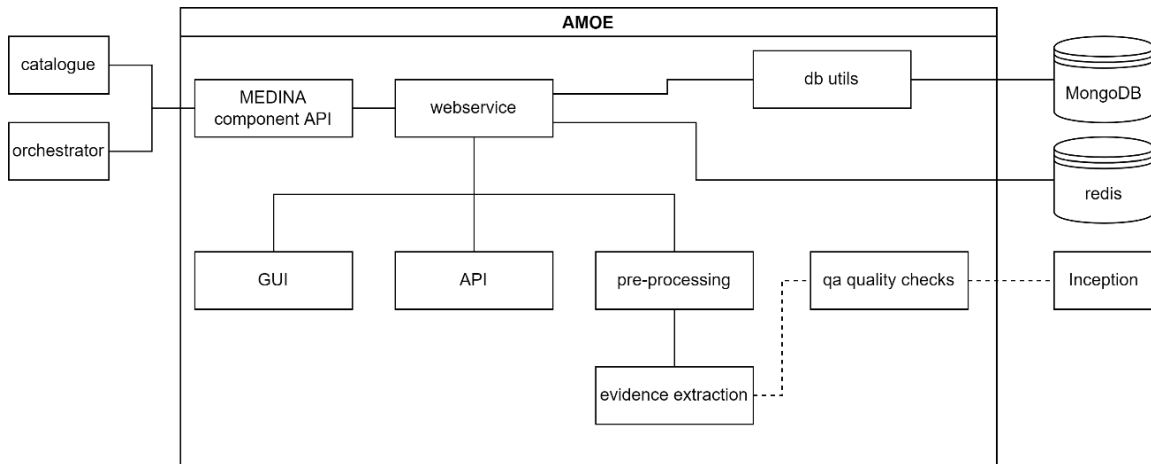


Figure 10. AMOE architecture and connections to other MEDINA components

In the context of MEDINA, compliance managers or auditors can use *AMOE* to inspect the compliance of a policy document with a set of organisational metrics. After uploading a document, the evidence is extracted in the background and can be viewed via the tool's GUI. Besides the extracted evidence, the GUI also displays assessment hints. The assessment hints derived by *AMOE* should aid the user to decide the compliance status for each metric. Once a compliance status has been set, the assessment result can be forwarded to the rest of the MEDINA framework tools – by sending it to the *Orchestrator*. The uploaded policy documents and extracted evidence are linked to a cloud service set by the user. Users can only access data for which they have the permission (set by an attribute in the Keycloak-authentication-token).

Interactive functionality is provided in the GUI but can be also implemented in an external tool, such as the *Company Compliance Dashboard (CCD)*⁹. For the latter purpose, *AMOE* offers a REST API. The main functionalities of the GUI and the API are as follows:

- Upload a policy document
- Retrieve uploaded documents
- Retrieve extracted evidence including assessment hints
- Set the compliance status / assessment result of an organisational metric
- Forward the assessment result to the *Orchestrator*

Appendix B: Assessment of Organizational Measures using NLP describes different types and methods that are relevant for the extraction of organizational evidence. As a summary, the input

⁸ *Catalogue of Controls and Metrics* is developed in the scope of WP2 and reported in D2.2 [5]

⁹ *CCD* is developed in the scope of WP6 and reported in D6.3 [55]

for an evidence extraction system can include textual, tabular and image files. Depending on the input, different methods need to be applied. To ensure high quality output, a dataset needs to be comprised to test the system.

For natural text documents a possible approach would be to use question-answering systems – e.g., models based on Bert¹⁰. These can use a question as input and retrieve the answer from a given text. Such models are pre-trained and can be downloaded and used from huggingface¹¹. Depending on the model, assumptions and circumstances have to be considered for a successful evidence extraction. The system provides an answer and a pseudo probability to indicate confidence. Depending on the structure of the log files, evidence can be extracted using regular expressions or XPath queries. NLP might not be necessary as the files are usually not just plain text.

The focus in MEDINA is on policy documents as this is relevant for the project partners Bosch and Fabasoft. AMOE works based on a natural language processing (NLP) approach rather than information extraction from log files, difference analysis on images, textual documents or document features, or bitwise comparison. AMOE uses the keywords defined in the organisational metrics to retrieve the relevant sections of a document and then performs queries in the form of questions. The answer to the query is computed with the pre-trained question answering model¹². The AMOE assessment hint is then calculated on the basis of the metric target value and extracted answer. The results can be investigated via GUI or API.

In Figure 1, Building Block 1 displays the position of AMOE within the MEDINA framework and the links to the next component neighbours. It depicts the link to the *Orchestrator*, as the assessment results can be forwarded directly to the *Orchestrator*. For generating the results, AMOE pulls metric information from the *Catalogue of Controls and Metrics* and the *Orchestrator*.

3.6 The Generic Evidence Collector (GEC)

The requirements defined in the EUCS certification scheme [3] cover a diverse set of categories including human resources, physical security, and procurement management. Therefore, gathering evidence for these categories requires a diverse set of tools and techniques. For some of the requirements, e.g., configuring a secure protocol for transport encryption, we may assume that a CSP is using one of the large cloud infrastructure providers or a CSPM solution to manage the configuration. In this case, we may address the requirement by an implementation that checks the configuration for this cloud provider, e.g., with the *Cloud Evidence Collector*.

However, for many other requirements there are a multitude of measures that a CSP can implement to fulfil the requirement. Consider the following example of the EUCS requirement HR-03.4H which states: *“All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.”*

A CSP may implement this requirement in many different ways. For instance, a software-as-a-service solution may be used to manage users and the policy acknowledgements. Or the CSP may only use a simple text document to store the acknowledgements. Also, the access control

¹⁰ [https://en.wikipedia.org/wiki/BERT_\(language_model\)](https://en.wikipedia.org/wiki/BERT_(language_model))

¹¹ <https://huggingface.co/>

¹² <https://huggingface.co/deepset/roberta-base-squad2>

system can be implemented in various ways. So, it is difficult to cover this requirement in a comprehensive manner with one of the tools described in sections 3.1 to 3.5. Therefore, an additional evidence gathering tool has been defined in MEDINA, called the *Generic Evidence Collector (GEC)*, which implements a generic collector that can be easily adapted to any CSP-specific system, i.e., it is not a complete implementation but a template that can be adapted to specific systems. In addition, the tool contains descriptions of techniques in text and/or pseudo-code form that provide detailed guidance for a CSP to successfully implement evidence collection.

The *Generic Evidence Collector (GEC)* is a template for a custom evidence collector which is based on the *Cloud Evidence Collector*. It presents a self-contained module that can be deployed as a Docker container. It also holds the code for setting up a connection to the *Security Assessment* and implements the MEDINA data model for evidence (see Figure 2). It is therefore completely compliant with the MEDINA data model and APIs. A CSP wishing to integrate the *GEC* with a specific system only needs to complete the API calls to the CSP-specific system; the response must be translated into the MEDINA evidence model. Techniques for performing these steps are described below.

3.6.1 Descriptions of Techniques

This section includes descriptions of some of the techniques related to the 34 EUCS requirements [3] that require an automatic monitoring to be implemented.

A technique is a method for gathering (and possibly assessing) evidence. The techniques described in the following include explanations of the respective metrics associated to the EUCS requirements, certain assumptions as well as the pseudocode for their implementation. Please note that we combine the evidence collection and assessment result creation in the technique description. In some cases, however, it would also be possible to create Rego code instead, to be used in the existing *Security Assessment* component. It is up to the MEDINA user how to put it into practice.

3.6.1.1 Technique for OIS-02.4H requirement

OIS-02.4H: The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.

Assumptions: We assume that measures for segregation of duties are defined as RBAC constraints. For example, such a constraint may define that no user is allowed to have permissions to deploy software artefacts to a development environment *and* permissions to approve an artefact for release to the production environment. Also, we assume that user roles and permissions are managed in a respective RBAC system, like Active Directory¹³.

Possible methods: To check this requirement, existing users and their roles and permissions need to be compared to the segregation of duties constraints, i.e., for any pair of roles given to a certain user, it needs to be checked whether they violate one of the constraints.

Pseudocode

```
users = getUsers()
segregationOfDuties = get SegregationOfDuties() // a map of roles that must not be mixed

for user in users:
```

¹³ <https://azure.microsoft.com/de-de/products/active-directory/>

```

for role in user.roles:
    // for every role the user has, check if it has a constraint in the segregation of
    // duties map; if this constrained role is also in the user's roles, it is a violation
    if segregationOfDuties.get(role) in user.roles:
        evidence = createEvidence(user, segregationOfDuties)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)

```

Metrics

To define a metric related to segregation of duties, we use the approach by Kunz et al. [16]. They propose a metric for the opposite of segregation of duties, i.e., *mixed duties*. Mixed duties calculate the overlap in existing roles. Thus, a metric in this context may define an upper limit for the mixed duties metric:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
OIS-02.4H	MixedDuties	[0, ..., 1]	<=	0.1	Float	Identity

3.6.1.2 Technique for ISP-03.5H requirement

ISP-03.5H: The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.

Assumptions: We assume that the approved exceptions are documented in a table form, e.g., in an Excel document, which documents each exception along with its validity period.

Possible methods: To monitor the list of exceptions, it is necessary to retrieve it regularly (e.g., daily), and check its exceptions and validity periods against their expiration. If reasonable assumptions can be made about the implementation of the exceptions, their implementation can also be checked. For example, an exception to segregation of duties constraints can be checked automatically in the user management system.

Pseudocode

```

exceptionList = getExceptionList()

for exception in exceptionList:
    if exception.validity < Time.now():
        evidence = createEvidence(exception)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)

```

Metrics

A metric in this context may define an upper limit for existing expired exceptions:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
ISP-03.5H	NumberOfExceptions	[0, ...]	<=	0	Integer	Exception

Alternative metrics include a temporal overview, e.g., the average time it takes to fix an expired exception.

3.6.1.3 Technique for HR-03.4H and HR-04.3H requirements

HR-03.4H: All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.

HR-04.3H: The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program.

Assumptions: Employee acknowledgements of documents, such as information security policies or completion of training, can be documented in several ways. We assume that they are either managed in a software-as-a-service solution like SAP or they are managed manually in a simple text document.

Possible methods: To check this requirement, an *Evidence Collector* should: 1) compare access requests against policy acknowledgements, or 2) compare a list of existing user accounts against the list of policy acknowledgements. Option 1) requires the *Evidence Collector* to retrieve a list of access requests to sensitive systems and check whether the requesting party has acknowledged the security policies, while option 2) simply requires retrieving both lists and comparing them as shown below.

Pseudocode

```
acknowledgements = getSecurityPolicyAcknowledgements()
sensitiveRolesList = getSensitiveRolesList()
userList = getUserList()
// only process the users that have a sensitive role
filteredUserList = userList.filter(user.roles in sensitiveRolesList)
for user in filteredUserList::
    if user not in acknowledgements:
        evidence = createEvidence(user)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context can define an upper limit for existing users that have access to sensitive systems without having acknowledged policies:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
HR-03.4H	NumberOfMissing-PolicyAcknowledgements	[0, ...]	<=	0	Integer	Identity
HR-04.3H	NumberOfMissing-Trainings	[0, ...]	<=	0	Integer	Identity

Alternative metrics include a temporal overview, e.g., of how many users are in this non-compliant state on average. Also, an overview, e.g., of how many users are untrained on average or how long it takes the average user to complete training once registered as a new user, are possible metrics.

3.6.1.4 Technique for HR-05.2H requirement

HR-05.2H: The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure.

Assumptions: We assume that a list of current users and their role assignments are available through a user management system, such as Active Directory¹³.

Possible methods

- Technique to *implement* the procedure: The procedure mentioned in HR-05.2H can be implemented as a periodic program which, for instance, runs in a serverless function in the cloud system. This function could retrieve the list of users and a list of active contracts to check whether only active contracts have a respective user in the cloud system.
- Technique to *monitor* the procedure: To monitor the application of the procedure, the *Evidence Collector* can perform a health check of the underlying Compute resource (e.g., the serverless function). Furthermore, it can retrieve the results of the procedure, i.e., a list of currently active users along with an indication of their contract activity.

Pseudocode

```
usersAndContracts = getUsersAndContractsList()
for entry in usersAndContracts::
    if entry.contract.status == "terminated":
        evidence = createEvidence(entry)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may define a grace period for revoking access rights of users with terminated contracts:

Requirement ID	Metric ID	Scale	Operator	Target Value (days)	Target Value Type	Resource Type
HR-05.2H	Revocation-GracePeriod	[0, ...]	<=	5	Integer	Revocation-Period

3.6.1.5 Technique for HR-06.2H requirement

HR-06.2H: The [non-disclosure and confidentiality] agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored.

Assumptions: We assume that a supplier's acceptance is performed in a dedicated web application which allows to cryptographically sign the acceptance.

Possible methods: To monitor the acceptations, the list of active external service providers and suppliers must be compared to the cryptographically signed acceptations in the web application.

Pseudocode

```
suppliers = getActiveSuppliers()
acceptations = getActiveAcceptations()

for supplier in suppliers:
    supplierAcceptation = get(acceptations, supplier):
    if supplierAcceptation is empty || supplierAcceptation.verifySignature() == false:
        evidence = createEvidence(supplier)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may check for any external service provider or supplier if an active acceptance exists.

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
HR-06.2H	ActiveAcceptation	[true, false]	==	True	Boolean	Identity

3.6.1.6 Technique for HR-06.3H requirement

HR-06.3H: The [non-disclosure and confidentiality] agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored.

Assumptions: We assume that a list of current users and their role assignments are available through a user management system, such as Active Directory¹³.

Possible methods: To check compliance with this requirement, a CSP may compare the employees' role permissions with the respective users' non-disclosure and confidentiality agreements. This way, it can be verified that every user with access permission to CSC data has accepted the agreements.

Pseudocode

```
users = getUsers ()
agreements = getAgreements()

for user in users:
    if 'ReadCSCData' is in user.permissions:
        if user.Id is not in agreements:
            // create a non-compliant assessmentResult
            createAssessmentResult(evidence, false)
```


Metrics

A metric in this context may check if a user who has access to CSC data, also has an active agreement:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
HR-06.3H	NoCSCAccess WithoutAgreement	[true, false]	==	True	Boolean	Identity

3.6.1.7 Technique for AM-01.4H requirement

AM-01.4H: The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.

Assumptions: We assume that the process that performs the inventory is a custom program that runs, for example, on a dedicated cloud resource such as a virtual machine. We also assume that the generated inventory is stored in a database, e.g., an SQL database.

Possible methods

- Technique to *implement* the process: Different possibilities exist to implement a process that creates a resource inventory (we focus on large cloud providers like Azure and AWS). First, the available service APIs can be used to list all types of resources, like virtual machines, networks, etc. Second, an Infrastructure-as-Code template can be exported which describes the resources in a standardized format. Please note, however, that the responses always depend on the access rights of the requesting client, so it needs *read*-rights on all resources.
- Technique to *monitor* the process: To guarantee that the process is performed regularly, and the inventory therefore is up-to-date, the CSP may monitor the health of the resource the process runs on. In addition, tests can be performed that create a new resource and check whether it appears in the inventory.

Pseudocode

```
vm = getInventoryVirtualMachine()

If vm.status != "running"
    evidence = createEvidence(vm)
    // create a non-compliant assessmentResult
    createAssessmentResult(evidence, false)
else
    newVm = createVm()
inventory = database.get(inventoryTable)
    if newVM not in inventory
        evidence = createEvidence(vm)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may define the uptime of the inventory resource:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
AM-01.4H	HealthyInventory	[true, false]	==	true	Boolean	VirtualMachine

3.6.1.8 Technique for AM-03.4H requirement

AM-03.4H: The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.

Assumptions: Approvals of hardware (de-)commissioning are documented in a table form, such as an Excel sheet. Approvals include a cryptographic signature of the approver.

Possible methods: To check compliance with this requirement, the approval document needs to be checked for the appropriate approvers, i.e., if the cryptographic signatures have been done by an appropriate employee.

Pseudocode

```

allowedApprovers = getAllowedApprovers()
approvalSignatures = getSignaturesFromApprovalDoc()

for signature in approvalSignatures:
    if signature.Identity not in allowedApprovers:
        evidence = createEvidence(signature)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)

```

Metrics

A metric in this context may check if every approver is in the list of allowed approvers.

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
AM-03.4H	AllowedApprovers	[true, false]	==	true	Boolean	Identity

3.6.1.9 Technique for AM-04.1H requirement

AM-04.1H The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored.

Assumptions: We assume that the commitments are documented via an online platform that, e.g., provides trainings to employees and documents the commitments. We also assume that the platform requires authentication, making the commitments trustworthy. Furthermore, we assume that a list of current users is available through a user management system, like Active Directory.

Possible methods: To check this requirement, the commitments to the policies and procedures for acceptable use and safe handling of assets in the given situation simply need to be checked against an up-to-date list of users.

Pseudocode:

```
commitments = getPolicyCommitments()
userList = getUserList()
for user in userList:
    if user not in commitments:
        evidence = createEvidence(user)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may assess how many commitments are missing:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
AM-04.1H	MissingCommitments	[0, ...]	<=	0	Integer	Identity

Alternative metrics may include a temporal overview, e.g., of how many users have not given the commitment on average, or how long it takes for the average user to complete it once registered as a new user.

3.6.1.10 Technique for PS-02.8H requirement

PS-02.8H: The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored.

Assumptions: We assume that the physical accesses are logged in a database, e.g., a SQL table. We also assume that a current user list is available through a user management system, like Active Directory¹³.

Possible methods: To check this requirement, it is necessary to retrieve the accesses, as well as the list of users. All accesses that have been made by a certain user are then filtered out. All the user's roles can then be checked for their inclusion in the access in question.

Pseudocode

```
accesses = getPhysicalAccessesToNonPublicAreas()
userList = getUserList()
for user in userList:
    for role in user.roles:
        for access in accesses.filter(user):
            if access not in role.permissions:
                evidence = createEvidence(user)
                // create a non-compliant assessmentResult
                createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may define an upper limit for users that (try to) access sensitive areas without permission, e.g., to trigger an alert:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
PS-02.8H	MaximumSensitive-AccessRequests	[0, ...]	<=	0	Integer	Identity

3.6.1.11 Technique for OPS-02.2H requirement

OPS-02.2H: The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards.

Assumptions: The “safeguards” mentioned in the requirement refer to safeguards that ensure compliance with the Service Level Agreement (SLA). SLAs may define numerous aspects, including availability, performance, security, and support. We focus here on the availability of certain resource types, like storages and compute resources, since the availability of such resources is an essential part of any cloud-related SLA.

Possible methods: To check compliance with this requirement, the CSP may access the asset inventory regularly and compare different states.

Pseudocode

```
SLAServices = getServicesWithAvailabilitySLA()
for service in SLAServices:
    isHealthy = performHealthCheck()
    if not isHealthy:
        evidence = createEvidence(service)
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may assess the overall uptime of a service:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
OPS-02.2H	SLAServiceAvailable	[0, ..., 100]	>=	99	Integer	CloudService

3.6.1.12 Technique for IAM-03.2H requirement

IAM-03.2H: The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application.

Assumptions: We assume that a list of current users and their properties, like authentication attempts, is available through a user management system, like Active Directory¹³. Furthermore, the CSP must implement the mentioned policy, which specifies risks for different types of

accounts, their access rights and authentication mechanisms. We assume that such a policy is in place and is mapped to a maximum number of failed authentication attempts allowed.

Possible methods: To check compliance with this requirement, a CSP can query the API of the user management system regularly to retrieve information about a user's account type and failed authentication attempts, and compare the results against the maximum defined in the policy. Also, a health check of the blocking mechanism may be meaningful to check for compliance.

Pseudocode

```
users = listUsers()
policy = getAuthenticationPolicy()

for user in users:
    if failedAuthenticationAttempts != 0:
        // compare with policy
        allowedFailedAuthenticationAttempts = policy.get(user.type)
        if failedAuthenticationAttempts > allowedFailedAuthenticationAttempts:
            // create a non-compliant assessmentResult
            createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may check the number of failed authentications for a given user.

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
IAM-03.2H	FailedAuthentications	[0, ...]	<=	3	Integer	Identity

3.6.1.1 Technique for IAM-03.5H requirement

IAM-03.5H: The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application.

Assumptions: We assume that a list of current users/accounts and their properties, like their status (e.g., active/blocked/revoked), is available through a user management system, like Active Directory. Furthermore, the CSP must implement a policy which specifies the allowed period of inactivity after which the mechanism shall become active.

Possible methods: To check compliance with this requirement, a CSP may first retrieve the allowed value of inactivity from the specified policy. Then, the list of user accounts can be retrieved and if revoked accounts are found, their inactivity period can be compared to the policy's value.

Pseudocode

```
users = listUsers()
policy = getPolicy()
```

for user in users:

```
    if user.status == "revoked" and user.inactivityPeriod > policy.allowedInactivityPeriod:
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may check how long blocked accounts have been inactive. If, for example, the policy defines the respective allowed period as 30 days long, the metric can be defined as follows:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
IAM-03.5H	InactivityPeriod-RevokedAccounts	[0, ...]	<=	30	Integer	User

3.6.1.1 Technique for IM-02.5H requirement

IM-02.5H: The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures.

Assumptions: We assume that security incidents are reported in a business process that can be queried automatically about the processing state of an incident. Example steps of such a system that could be monitored can be the analysis of the incident, containment, eradication, and recovery.

Possible methods: To monitor the execution of the steps mentioned above, the business process system, for example Jira, can be queried regularly to check if processed incidents have gone through all necessary steps of the process. Additionally, using a pre-defined maximum time frame, it can be checked whether any incident has stayed too long in one of the steps.

Pseudocode

```
processedIncidents = listProcessedIncidents()
```

for incident in processedIncidents:

```
    if length(incident.history) < 4:
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

```
// for any step X in the business process
incidentsInStepX = listIncidentsInStepX()
```

for incident in incidentsInStepX:

```
    if incident.lastChange > 24 hours:
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
```

Metrics

A metric in this context may define an upper limit for the time an incident may stay in one a step of the process:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
IM-02.5H	IncidentProcessTime	[0, ...]	<=	24	Integer	ProcessingTime

3.6.1.1 Technique for INQ-03.4H requirement

INQ-03.4H: The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.

Assumptions: We assume that investigators use normally administrated user accounts, e.g., managed in an Active Directory¹³.

Possible methods: To check compliance with this requirement, one possible technique is to monitor *all* access requests to the cloud system, and especially to the evidence and assessment results. In this way, the accesses by investigator users are also logged.

Pseudocode

```
accessLoggingEnabled = getAccessRequestLoggingConfiguration()
```

```
if not accessLoggingEnabled:
```

```
    // create a non-compliant assessmentResult
```

```
    createAssessmentResult("AccessRequestLogging", false)
```

Metrics

A metric in this context may check if the access request logging system is enabled:

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
INQ-03.4H	AccessRequestLoggingEnabled	[true, false]	==	True	Boolean	Logging

3.6.1.2 Technique for PSS-04.2H requirement

PSS-04.2H: An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails.

Assumptions: We assume that the CSP checks integrity via cryptographic signatures, and we assume that the CSP has defined a policy which specifies allowed signatories.

Possible methods: To verify compliance with this requirement, a CSP may check if the compute resources in operation, like virtual machines, serverless functions, and containers, are running images; if this is the case, it can be checked if the image is signed, and the signature can be

verified. Note that the report mentioned in the requirement may be generated by another MEDINA component.

Pseudocode

```
computeResources = listComputeResources()
allowedSignatories = listAllowedSignatories()

for resource in computeResources:
    if resource.image.signature.signatory not in allowedSignatories:
        // create a non-compliant assessmentResult
        createAssessmentResult(evidence, false)
        // alert the CSC
        alertCSC(resource)
```

Metrics

A metric in this context may check if a compute resource runs an image that is integrity-verified (for example, using Docker Content Trust for containers).

Requirement ID	Metric ID	Scale	Operator	Target Value	Target Value Type	Resource Type
PSS-04.2H	IntegrityVerified	[true, false]	==	true	Boolean	Compute

4 Coverage of EUCS requirements by the MEDINA Evidence Management Tools

This section presents the final coverage of the high-level assurance requirements that the draft candidate version of the EUCS scheme [3] qualifies as “continuous (automated monitoring)”, by the *MEDINA Evidence Management tools* described in section 3.

The selected requirements are a list of 34 EUCS high-level requirements (also known as “the 34”) that meet this condition and are documented in D2.2 [17]. For completeness, a summary of these requirements is also provided in Table 2¹⁴.

Table 2. Summary of the 34 selected requirements from the August 2022 draft candidate EUCS [3]

Req.ID	Requirement
OIS-02.4H	“The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.”
ISP-03.5H	“The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.”
HR-03.4H	“All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.”
HR-04.3H	“The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program.”
HR-05.2H	“The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure.”
HR-06.2H	“The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored.”
HR-06.3H	“The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored.”
HR-06.5H	“The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored.”
AM-01.4H	“The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.”
AM-03.4H	“The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.”

¹⁴ It should be noted that the EUCS requirements referred in this document correspond to a draft version of the ENISA certification scheme and are not intended for being used outside the context of MEDINA.

Req.ID	Requirement
AM-04.1H	"The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored."
PS-02.8H	"The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored."
OPS-02.2H	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."
OPS-05.3H	"The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities."
OPS-07.2H	"In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP."
OPS-09.2H	"When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup."
OPS-12.1H	"The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation."
OPS-12.2H	"The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H)."
OPS-13.1H	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data."
OPS-18.6H	"The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC."
OPS-21.1H	"The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements."
IAM-03.1H	"The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons."
IAM-03.2H	"The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access

Req.ID	Requirement
	rights and authentication mechanisms, and automatically monitor its application.”
IAM-03.5H	“The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application.”
IAM-03.6H	“The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant.”
CCM-04.1H	“The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored.”
CCM-05.1H	“The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights.”
PM-04.7H	“The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling).”
PM-04.8H	“The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action.”
IM-02.5H	“The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures.”
CO-03.5H	“Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions.”
CO-03.6H	“The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP’s subject matter experts for immediate assessment and action.”
INQ-03.4H	“The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.”
PSS-04.2H	“An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails.”

Appendix D: EUCS Requirements coverage per tool within the MEDINA Evidence Management Tool details the specific coverage of the 34 high-level requirements from Table 2 for each of the *MEDINA Evidence Management Tools* described in section 3, namely *Clouditor*, *Codyze*, *Wazuh*, *VAT*, *AMOE* and *GEC*.

Table 3 shows a summary of this coverage at the time of writing this deliverable. The aim is to show the current level of compliance of the MEDINA KPIs, in particular KPI 1.1 and KPI 1.2 (see deliverable D2.2 [17]).

The structure of Table 3 is as follows:

- Each row corresponds to a EUCS high-level requirement listed in Table 2.

- The “Type” column identifies the type of requirement: technical (*tech*) or organizational (*org*). It should be noted that the requirement is considered organizational if it involves the monitoring of a static policy document.
- The “Coverage” column shows the level of coverage of the requirement by the *MEDINA Evidence Management Tools* described in section 3. The background colour means:

Green

MEDINA Evidence Management Tools cover the requirement to some extent (i.e., at least one metric has been implemented).

Orange

There is a plan or idea to implement the requirement by any of the *MEDINA Evidence Management Tools*, but it has not yet been realised.

Red

It is not possible to cover the requirement due to its nature.

Table 3. Summary of the final coverage of the *MEDINA Evidence Management Tools* for the 34 high level requirements from the draft candidate EUCS [3]

Category	Control	Req.ID	Type	Coverage
Organizational Information Security	OIS-02 SEGREGATION OF DUTIES	OIS-02.4H	Tech	
Information Security Policies	ISP-03 EXCEPTIONS	ISP-03.5H	Tech	
Human Resources	HR-03 EMPLOYEE TERMS AND CONDITIONS	HR-03.4H	Tech & Org	
	HR-04 SECURITY AWARENESS AND TRAINING	HR-04.3H	Tech	
	HR-05 TERMINATION OR CHANGE IN EMPLOYMENT	HR-05.2H	Tech	
	HR-06 CONFIDENTIALITY AGREEMENTS	HR-06.2H	Tech	
		HR-06.3H	Tech	
		HR-06.5H	Tech & Org	
Asset Management	AM-01 ASSET INVENTORY	AM-01.4H	Tech	
	AM-03 COMMISSIONING AND DE-COMMISSIONING	AM-03.4H	Tech	
	AM-04 ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS	AM-04.1H	Tech & Org	
Physical Security	PS-02 PHYSICAL SITE ACCESS CONTROL	PS-02.8H	Tech & Org	
Operational Security	OPS-02 CAPACITY MANAGEMENT – MONITORING	OPS-02.2H	Tech	
	OPS-05 PROTECTION AGAINST MALWARE – IMPLEMENTATION	OPS-05.3H	Tech	
	OPS-07 DATA BACKUP AND RECOVERY – MONITORING	OPS-07.2H	Tech	
	OPS-09 DATA BACKUP AND RECOVERY – STORAGE	OPS-09.2H	Tech	
	OPS-12 LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	OPS-12.1H	Tech	
		OPS-12.2H	Tech	
	OPS-13 LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION	OPS-13.1H	Tech	

Category	Control	Req.ID	Type	Coverage
	OPS-18 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	OPS-18.6H	Tech	
	OPS-21 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	OPS-21.1H	Tech	
Identity, Authentication and Access Control Management	IAM-03 LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	IAM-03.1H	Tech	
		IAM-03.2H	Tech & Org	
		IAM-03.5H	Tech & Org	
		IAM-03.6H	Tech	
Change and Configuration Management	CCM-04 APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	CCM-04.1H	Tech & Org	
	CCM-05 PERFORMING AND LOGGING CHANGES	CCM-05.1H	Tech & Org	
Procurement Management	PM-04 MONITORING OF COMPLIANCE WITH REQUIREMENTS	PM-04.7H	Tech	
		PM-04.8H	Tech	
Incident Management	IM-02 PROCESSING OF SECURITY INCIDENTS	IM-02.5H	Tech	
Compliance	CO-03 INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	CO-03.5H	Tech & Org	
		CO-03.6H	Tech	
Dealing with Investigation Requests from Government Agencies	INQ-03 CONDITIONS FOR ACCESS TO OR DISCLOSURE OF DATA IN INVESTIGATION REQUESTS	INQ-03.4H	Tech	
Product Safety and Security	PSS-04 IMAGES FOR VIRTUAL MACHINES AND CONTAINERS	PSS-04.2H	Tech	

From Table 3, we can conclude that at the time of writing this deliverable the *MEDINA Evidence Management Tools* **fully cover 32 of the 34 EUCS requirements** identified in Table 2. Furthermore, **there is an ongoing working for covering another requirement** identified in Table 2 until the end of the MEDINA project. Summarizing, **there is only one requirement that is not covered by the *MEDINA Evidence Management Tools*.**

Taking this into consideration, we can calculate the current level of achievement for the following MEDINA KPIs:

- **KPI 1.1: “Provide realizable metrics for at least 70% of the technical measures referenced in EUCS-High assurance requiring ‘continuous (automated)’ monitoring”.**
 - Considering results from Table 3, the 34 identified requirements are considered to be of a technical nature. *MEDINA Evidence Management Tools* cover around **94.1 % (32/34)** of the technical requirements and there is an ongoing working to cover another **2.9 % (1/34)**, resulting in a 97.0%.
 - Summarizing, **KPI 1.1 has been achieved at 94.11%, which is much higher than the 70% coverage target.**
- **KPI 1.2: “Provide a concrete proposal for semi-automated evaluation of metrics related to at least 50% of the organizational measures in EUCS-High assurance requiring ‘continuous (automated)’ monitoring”.**

- Considering results from Table 3, 9 of the 34 requirements identified are considered to be organizational. *MEDINA Evidence Management Tools* cover **100.0% (9/9)** of the organizational requirements.
- Summarizing, **KPI 1.2 has been achieved at 100.0%, which is much higher than the 50% coverage target.**

5 MEDINA Evidence Trustworthiness Management System

This section presents the final version of the *MEDINA Evidence Trustworthiness Management System*, designed, and developed in Task 3.5 and based on the theoretical analysis gathered in D4.3 [7]. The description included in this section contains much information in common with D3.2 [4] with the final aim of providing a self-contained section that facilitates the reader's understanding.

5.1 Functional Description

Blockchain technology has started to be considered as a suitable technology for trustworthy purposes [18], [19], [20], [21] as it promises a transparent, secure, and affordable solution to audit trails. First, Blockchain eliminates the need of a central authority for maintaining data records as it decentralizes the information in a distributed network. Furthermore, Blockchain guarantees immutability of the recorded information as it is “copied” in a distributed network. Another key aspect is that information recorded in a Blockchain is digitally signed by its creator so the origin can always be traced back.

Although Blockchain integrity, decentralization, and non-repudiation inherent features make it a suitable technology for audit trails, its use is still not widespread, and its usability is not user-friendly. Nowadays, a Blockchain client is needed for interacting with a Blockchain. This is usually a limiting requirement as nowadays it is not common for users to have a Blockchain client deployed in their systems. That is why a graphical and web-based tool to access the information recorded in the Blockchain in a user-friendly way is highly recommended, making Blockchain totally transparent for external users (for example, auditors) and providing a graphical mechanism to verify the information records in the Blockchain about evidence and assessment results provided by the *Orchestrators*. This way, anyone with permission (authentication is needed), could check the information recorded in the Blockchain without any kind of Blockchain client (Blockchain will be totally transparent).

The Blockchain based *MEDINA Evidence Trustworthiness Management System*, provides a secure mechanism for MEDINA to maintain an audit trail of evidence and assessment results. The *MEDINA Evidence Trustworthiness Management System* is implemented in **Smart Contracts** backbone by a common **Blockchain network** for all the MEDINA framework instances, providing the following **functionalities**:

- Includes the logic for all *Orchestrator* instances in MEDINA to **provide the required information to be audited** (about evidence and assessment results).
- Provides **long-term information recording**, thanks to the inherent advantages of Blockchain (integrity, decentralization, authenticity...).
- Includes the logic for external users to **access MEDINA's audited information** (about evidence and assessment results) **in a graphical and user-friendly way**.

5.1.1 Fitting into overall MEDINA Architecture

Figure 11 shows how the Blockchain-based *MEDINA Evidence Trustworthiness Management System* fits into the overall MEDINA architecture. It provides a common service of trustworthy records to be able to perform manual or automated inspections if needed while guaranteeing the integrity of information. On the one hand, considering the MEDINA components, only the *Orchestrator(s)* will provide information related to evidence and assessment results. On the other hand, compliance manager auditors will be able to consume information recorded in the Blockchain by means of the web-based interface of the *MEDINA Evidence Trustworthiness Management System* (Blockchain viewer and the automatic verification service).



5.1.1 Component card

Component Name	MEDINA Evidence Trustworthiness Management System		
Main functionalities	<p>The component provides the following functionalities:</p> <ul style="list-style-type: none"> • Maintains an improved audit trail of evidence and assessment results. • Provides a manual and automatic way of verification of evidence and assessment results integrity. • 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). 		
Sub-components Description	<p>Blockchain client, to be executed on the <i>Orchestrator</i> for providing the information (evidence/assessment results) to be saved on the Blockchain.</p> <p>Smart contract, deployed on Blockchain nodes, for information (evidence/assessment results) writing and reading operations as well as events generation indicating the provision of new information.</p> <p>Viewer tool, for subscription to the Blockchain based events and notification to the different viewer clients.</p> <p>Graphical viewer client, for gathering and showing all the information saved on the Blockchain (and be able to manually verify it, without needing any interaction with the Blockchain).</p> <p>Automatic verification service, for evidence and assessment results integrity automatic check.</p>		
Main logical Interfaces	Interface name	Description	Interface technology
	Blockchain client	It provides: i) the required evidence and assessment results to be saved on the Blockchain, and ii) a way to obtain or check the evidence and assessment results saved on the Blockchain.	REST API
	Graphical Viewer Client	It provides a GUI to manually check evidence and assessment results saved on the Blockchain.	WEB
	Automatic Verification Service	It provides a GUI for automatic verification of the integrity of evidence and assessment results.	WEB
Requirements Mapping	<p>List of requirements covered by this component (see D5.2 [1]):</p> <p>ETM.01, ETM.02, ETM.03, ETM.04, ETM.05</p>		

<p>Interaction with other components</p>	<table> <tr> <th>Interfacing Component</th><th>Interface Description</th></tr> <tr> <td>Orchestrator</td><td>The orchestrator will provide (and check, if needed) the information (evidence/assessment results) to be saved on the Blockchain by means of the Blockchain client interface.</td></tr> <tr> <td>Auditors</td><td>The auditors will check the information saved on the Blockchain by means of the graphical viewer client interface (manual way) or the automatic verification service interface (automatic way).</td></tr> </table>	Interfacing Component	Interface Description	Orchestrator	The orchestrator will provide (and check, if needed) the information (evidence/assessment results) to be saved on the Blockchain by means of the Blockchain client interface.	Auditors	The auditors will check the information saved on the Blockchain by means of the graphical viewer client interface (manual way) or the automatic verification service interface (automatic way).
Interfacing Component	Interface Description						
Orchestrator	The orchestrator will provide (and check, if needed) the information (evidence/assessment results) to be saved on the Blockchain by means of the Blockchain client interface.						
Auditors	The auditors will check the information saved on the Blockchain by means of the graphical viewer client interface (manual way) or the automatic verification service interface (automatic way).						
<p>Relevant sequence diagram/s (*)</p>	<p>Evidence and assessment results recording:</p> <pre> sequenceDiagram participant Orchestrator participant BC_Client participant Network_node participant Viewer participant ViewerClient Note over Orchestrator: Normal previous Operation loop Repeat process n times Orchestrator->>BC_Client: Evidence Hash Orchestrator->>BC_Client: Trustworthy Evidence (hash) BC_Client->>Network_node: write_evidence(trustworthy evidence) Network_node->>Viewer: Event write_evidence(organizationID) Viewer->>ViewerClient: create_topic_if_needed(organizationID) Viewer->>ViewerClient: subscribe_if_needed(organizationID) Viewer->>ViewerClient: Publish write_evidence(organizationID) Viewer->>ViewerClient: Notify write_evidence(organizationID) end loop Repeat process n times Orchestrator->>BC_Client: Assessment Result Hash Orchestrator->>BC_Client: Trustworthy Assessment (hash) BC_Client->>Network_node: write_assessment(trustworthy assessment) Network_node->>Viewer: Event write_assessment(organizationID) Viewer->>ViewerClient: create_topic_if_needed(organizationID) Viewer->>ViewerClient: subscribe_if_needed(organizationID) Viewer->>ViewerClient: Publish write_assessment(organizationID) Viewer->>ViewerClient: Notify write_assessment(organizationID) end </pre>						

	<p>Evidence and assessment results integrity verification:</p> <pre> sequenceDiagram participant Orchestrator participant BC_Client participant Network_node participant Monitor participant MonitorClient participant AutomaticVerification participant Auditor loop Manual Check of evidence trust Orchestrator->>BC_Client: get_evidence(evidenceID) BC_Client->>Auditor: evidenceID Auditor->>Auditor: Obtain evidence hash Auditor->>MonitorClient: Look for evidenceID details in Blockchain MonitorClient->>Auditor: Blockchain evidence Hash Auditor->>Auditor: Compare both hashes. Auditor-->>BC_Client: Validation result: true/false end loop Manual Check of assessment results trust Orchestrator->>BC_Client: get_assessment(assessmentID) BC_Client->>Auditor: assessmentID Auditor->>Auditor: Obtain assessment hash Auditor->>MonitorClient: Look for assessmentID details in Blockchain MonitorClient->>Auditor: Blockchain assessment Hash Auditor->>Auditor: Compare both hashes Auditor-->>BC_Client: Validation result: true/false end loop Automatic Check of evidence trust Orchestrator->>AutomaticVerification: check_evidence(evidenceID) AutomaticVerification->>BC_Client: evidence BC_Client->>Auditor: evidence Auditor->>Auditor: Evidence Hash Auditor->>MonitorClient: get evidence recorded in Blockchain (evidenceID) MonitorClient->>Auditor: Blockchain evidence Hash Auditor->>Auditor: Compare both hashes. Auditor-->>AutomaticVerification: Validation result: true/false end loop Automatic Check of assessment results trust Orchestrator->>AutomaticVerification: check_assessment(assessmentID) AutomaticVerification->>BC_Client: assessmentID BC_Client->>Auditor: assessmentID Auditor->>Auditor: assessment Hash Auditor->>MonitorClient: get assessment recorded in Blockchain (assessmentID) MonitorClient->>Auditor: Blockchain assessment Hash Auditor->>Auditor: Compare both hashes. Auditor-->>AutomaticVerification: Validation result: true/false end </pre>
Current TRL ¹⁵	TRL4
Target TRL ¹⁶	TRL5
Programming language	Solidity, NodeJS, React
License	Proprietary. Copyright by TECNALIA.
WP and task	WP3, Task 3.5 WP4, Task 4.2
MEDINA Workflows	WF2 - Preparation of MEDINA Components, WF5 - EUCS Compliance Assessment, and WF7 - EUCS –Report on ToC Certificate (see D5.4 [22])

(*) A more readable version of the Sequence Diagram can be found in section 2.3.4.

¹⁵ TRL value before validation

¹⁶ TRL value after validation

5.1.2 Requirements

Below is the collection of requirements (described in D5.2 [6]) related to the *MEDINA Evidence Trustworthiness Management System* and a description of how and to what extent these requirements are implemented at this point of development.

Requirement id	ETM.01
Short title	Trustworthiness of evidence
Description	The evidence orchestrator must integrate reasonable safeguards for guaranteeing the trustworthiness of collected evidence.
Status	Fully implemented

The trustworthiness of evidence is guaranteed thanks to the design of the *MEDINA Evidence Trustworthiness Management System*. Two key points: (i) Blockchain is used as trustworthy storage. Information recorded on the Blockchain cannot be tampered, so information integrity is guaranteed; (ii) Instead of recording evidence, evidence hashes/checksums are recorded for avoiding sensitive data disclosure; hashes are considered sufficiently secure (reasonable safeguards) as it is almost impossible to obtain the same hash for two different sets of data. The interested reader is referred to deliverable D4.3 [7] for more details.

Requirement id	ETM.02
Short title	Transmission of evidence checksums
Description	The evidence orchestrator should integrate a Ledger client that stores checksums of evidence in a DLT.
Status	Fully implemented

A Blockchain client has been provided for the *MEDINA Orchestrator* to interact with the Blockchain and provide a way to be able to register evidence and assessment results hashes/checksums in the Blockchain. The Blockchain client has been integrated with the *Orchestrator*.

Requirement id	ETM.03
Short title	Trustworthiness guaranteeing capabilities
Description	Enable trustworthiness guaranteeing capabilities by extracting checksums from DLT and comparing with current checksums to detect modifications.
Status	Fully implemented

The *MEDINA Evidence Trustworthiness Management System* provides user-friendly manual (through the Blockchain viewer) and an automatic way (through the automatic verification service) to verify the evidence and assessment results integrity.

Requirement id	ETM.04
Short title	Tamper-Resistance
Description	The developed tool must provide a tamper-proof way of storing evidence in the considered attacker model.
Status	Fully implemented

A risk assessment study was carried out in deliverable D4.3 [7] to identify the main security risks for evidence integrity. Blockchain was considered a suitable technology for providing tamper-proofs of evidence. The *MEDINA Evidence Trustworthiness Management System* records information related to evidence on the Blockchain.

Requirement id	ETM.05
Short title	Tamper-Resistance

Description	The DAT must provide a tamper-proof way of storing audit information in the considered attacker model.
Status	Fully implemented

A risk assessment study was carried out in deliverable D4.3 [7] to identify the main security risks for audit information (assessment results) integrity. Blockchain was considered a suitable technology for providing tamper-proofs of assessment results. The *MEDINA Evidence Trustworthiness Management System* records information related to assessment results on the Blockchain.

5.2 Technical Description

This section describes the technical details of the *MEDINA Evidence Trustworthiness Management System*, including the prototype architecture, the different components, and the main technical specifications.

5.2.1 Prototype architecture

Figure 12 shows the architecture of the Blockchain-based *MEDINA Evidence Trustworthiness Management System*.

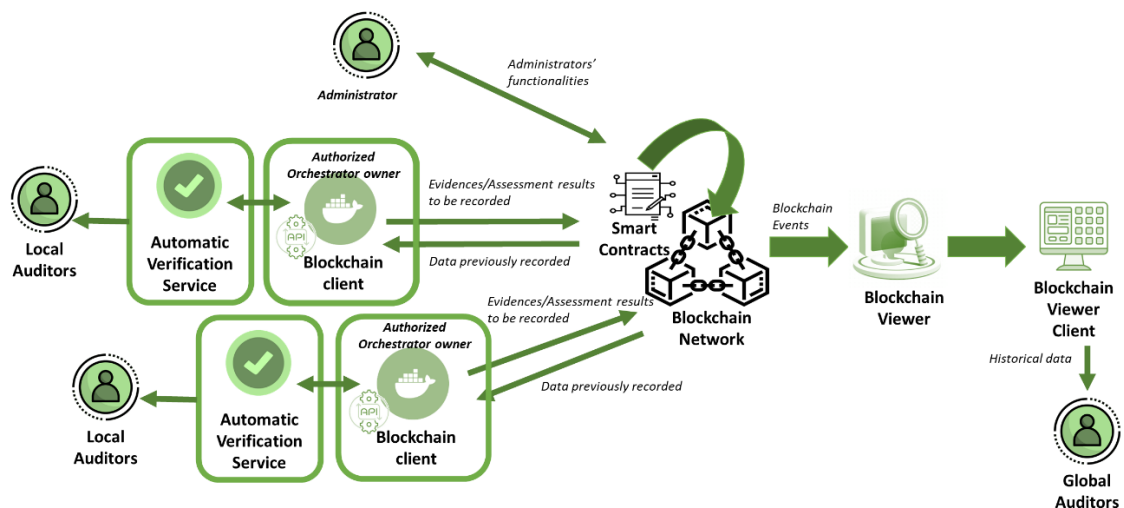


Figure 12. *MEDINA Evidence Trustworthiness Management System* (source: *MEDINA's own contribution*)

The architecture is composed of six main elements:

- **Blockchain network.** A Blockchain network has been configured with three nodes deployed in TECNALIA servers. The Blockchain network has been offered as a service by TECNALIA to validate the system solution; however, in real deployments, additional nodes from different companies will be recommended for improving the governance of the Blockchain network. All the information provided by the *Orchestrator* to the *MEDINA Evidence Trustworthiness Management System* will be recorded in all the nodes of the Blockchain network, thus ensuring the integrity of the recorded information.
- **Smart Contracts.** The *MEDINA Evidence Trustworthiness Management System* functionalities have been implemented in Smart Contracts deployed in the Blockchain network (previous element). Smart Contracts are programs typically used to automate the execution of certain actions, guaranteeing that all actors can have immediate certainty of the outcome. Like the information, the Smart Contracts definition is also recorded in all nodes of the Blockchain, ensuring the integrity and security of execution.

The *MEDINA Evidence Trustworthiness Management System* functionalities include the registration of data in the Blockchain (evidence and assessment results) to be verified, as well as the use of this previously registered data for integrity verification. In addition, Blockchain-based events are also generated to feed the Blockchain viewer.

- **Blockchain Client.** Every *Orchestrator* using the functionalities of the *MEDINA Evidence Trustworthiness Management System* needs a Blockchain client to interact with the Blockchain (wallet management functionalities, transactions generation, etc.). To facilitate integration and deployment, this Blockchain client will be deployed on all the *Orchestrator* instances as a Docker image that exposes an API REST to interact with it.
- **Blockchain viewer.** A component that listens for Blockchain events from the Smart Contracts and normalises and categorises the details for proper consumption from the Blockchain viewer client. The Blockchain viewer allows to isolate external users from the need to have a Blockchain client to consume information recorded on the Blockchain.
- **Blockchain viewer Client:** A client that consumes the normalised and categorised information from the Blockchain viewer.
- **Automatic verification service:** An automatic verification tool for current and recorded evidence and assessment results has been included in the *MEDINA Evidence Trustworthiness Management System* to provide auditors a user friendly and automatic way to verify the integrity of evidence and assessment results. This service exposes a graphical interface to improve usability.

5.2.2 Description of components

This section describes the six components that appear in the architecture of the *MEDINA Evidence Trustworthiness Management System* (see Figure 12).

5.2.2.1 Blockchain network

The Blockchain network considered for the *MEDINA Evidence Trustworthiness Management System* is **Quorum** [23]. This selection was based on the comparative study carried out inside WP4, where different Blockchain technologies were analysed, concluding that Quorum is the most suitable one (for more details, the interested reader may refer to deliverable D4.3 [7]).

The Quorum Blockchain network has been deployed at TECNALIA for prototype purposes; three Quorum Blockchain nodes form the test Blockchain network; however, as mentioned in section 5.2.1, in real deployments, more nodes from different organizations are needed to improve the decentralization and governance of the Blockchain network. These additional nodes need to be permissioned to be part of the Blockchain network, maintaining the network state, executing Smart Contracts, and verifying transactions. Figure 13 shows the architecture of each Quorum node.

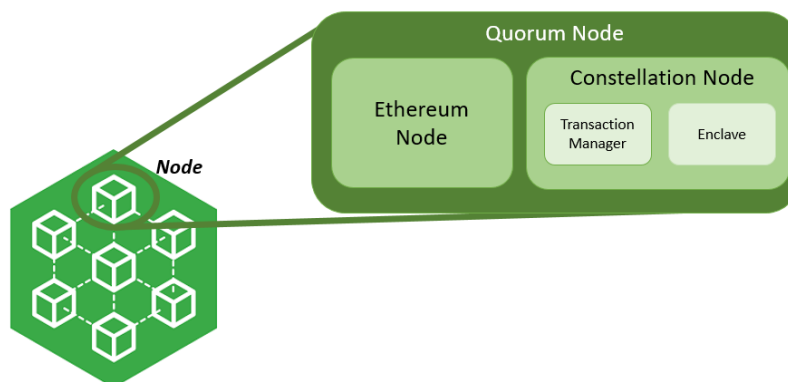


Figure 13. Quorum Blockchain node architecture (source: MEDINA's own contribution)

Quorum [23] is a private Blockchain network created by JP Morgan as a fork of the public Ethereum. It stands out for its high maturity level (being a fork of Ethereum means a widely proven background) which reuses existing technology and maintains sync with upcoming versions of Ethereum. Its main advantages are:

- Advanced Smart Contracts. In Quorum, Smart Contracts are based on Solidity language, allowing all the logic of a complete “Turing machine”.
- No cryptocurrency. The *MEDINA Evidence Trustworthiness Management System* does not require any cryptocurrency. For this reason, it is not necessary to complicate the operation of the Blockchain network. In this sense, Quorum stands out because of its high simplicity.
- Voting based consensus. Quorum leverages a faster voting-based consensus algorithm [24] which does not require large processing features in the Blockchain nodes. This consensus algorithm is lighter.
- Private network. Quorum only allows permissioned nodes to participate; it is a private network.
- High scalability level. Quorum is scalable in terms of participants and activities.

The Quorum nodes communicate with Blockchain clients and other Blockchain nodes using the Constellation peer-to-peer system based on secure messages [25]. This module is formed of two components:

- Transaction Manager: it communicates the different Quorum nodes by orchestrating private transactions (sending/receiving encrypted payloads among them). It uses the Enclave for cryptographic operations.
- Enclave: It executes encryption and decryption operations.

All information provided by the *MEDINA Orchestrators* to the *MEDINA Evidence Trustworthiness Management System* (evidence and assessment results) and the Smart Contracts with the specific *MEDINA Evidence Trustworthiness Management System* functionality will be recorded in all Quorum nodes.

5.2.2.2 Smart Contracts

The Smart Contracts deployed in the Blockchain network include all the intelligence (functionalities) for the *MEDINA Evidence Trustworthiness Management System*. The main functionalities are:

User management

There are two kinds of users:

- **Administrators.** These actors are those who can authorize or de-authorize *Orchestrators* to access the *MEDINA Evidence Trustworthiness Management System*. Administrators can also define new administrators or remove existing ones. The default administrator in the system for prototype purposes is “TECNALIA”.
- **Authorized *Orchestrators*’ owners.** These users shall have been authorized by an existing administrator to use the *MEDINA Evidence Trustworthiness Management System* (for example, XLAB, FHG, etc.). Each of these users will own “one” *MEDINA Orchestrator* which can be then registered in the system (there will be just one *Orchestrator* associated to each authorized *Orchestrator* owner due to the access control policies implemented in the Smart Contract). The information associated to each *Orchestrator* can only be retrieved by its owner. Thus, although the Blockchain network will be common to several authorized *Orchestrator* owners (information associated with

different *Orchestrators* will be recorded in the same Blockchain network), each authorized *Orchestrator* owner will only have access to the information associated to its own registered *Orchestrator*.

Blockchain addresses are used in the Blockchain based *MEDINA Evidence Trustworthiness Management System* for users' identity purposes (the Blockchain address will be the user identifier).

Administrators' functionalities

Administrators can obtain general information about the current status of the *MEDINA Evidence Trustworthiness Management System* (only administrators can execute the following set of functionalities):

- Register a new administrator (the new administrator *id* is needed).
- Remove an existing administrator (the administrator *id* is needed).
- Check if a specific user *id* is an administrator (the administrator *id* is needed).
- Get the number of administrators in the system.
- Authorize a new *Orchestrator* owner (the new *Orchestrator* owner *id* is needed).
- De-authorize an existing *Orchestrator* owner (the *Orchestrator* owner *id* is needed).
- Check if a specific *Orchestrator* owner *id* is an authorized *Orchestrator* owner (the *Orchestrator* owner *id* is needed).
- Get the total number of authorized *Orchestrator* owners in the system.
- Get the total number of registered *Orchestrators* in the system.
- Get all the registered *Orchestrators* *ids* in the system (administrators can only see the registered *Orchestrator id*, but not the information provided during the registering process by the authorized *Orchestrator* owner).

Authorized *Orchestrator* owners' functionalities

Authorized *Orchestrator* owners can register *Orchestrators*. This registration process considers the following data model for each *Orchestrator* identification:

- **id:** This is the internal *id* used to identify the *Orchestrator* inside the *MEDINA Evidence Trustworthiness Management System*. It is automatically generated by the Smart Contract considering its Blockchain address (this is unique).
- **owner:** It refers to the authorized *Orchestrator* owner *id* who has registered the *Orchestrator*. As above, it refers to the Blockchain address of the authorized *Orchestrator* owner, as it is considered the user identifier. It is automatically provided by the Smart Contract.
- **timestamp:** It refers to the timestamp in seconds since the epoch of the *Orchestrator* registering process. It is automatically generated by the Smart Contract.

The functionalities related to the *Orchestrators*' owners are:

- Register a new *Orchestrator* (only one *Orchestrator* per authorized *Orchestrator* owner).
- Get the registered *Orchestrator id*.
- Get the associated authorized *Orchestrator* owner *id*.
- Get the registered *Orchestrator* registration timestamp.
- Add new evidence information (details following the trustworthy evidence data model shown in Figure 14 are needed).
- Get a specific evidence information (the specific evidence *id* is needed).
- Get all the added evidence *ids* associated to this *Orchestrator*.

- Add new assessment result information (details following the trustworthy assessment result data model shown in Figure 14 are needed).
- Get a specific assessment result information (the specific assessment result id is needed).
- Get all the added assessment result ids associated to this *Orchestrator*.
- Check the validity of the hash for specific evidence (the specific evidence id and the evidence hash are needed).
- Check the validity of the hash for a specific assessment result (the specific assessment result id and the assessment result hash are needed).
- Check the validity of the hash for a specific assessment compliance result (the specific assessment result id and the assessment compliance result hash are needed).

```
address id;  
address owner;  
uint256 creationTimestamp;  
  
uint256[] evidencesIds;  
struct Evid {  
    uint256 id;  
    bytes32 valueHash;  
    uint256 toolId;  
    uint256 resourceId;  
    uint256 cspId;  
    uint256 timestamp;  
}  
mapping(uint256 => Evid) public evid;  
  
uint256[] assessmentsIds;  
struct Assess {  
    uint256 id;  
    bytes32 securityAssessmentHash;  
    bytes32 complianceHash;  
    uint256[] associatedEvidencesId;  
    uint256 metricId;  
    uint256 timestamp;  
}  
mapping(uint256 => Assess) public assess;
```

Figure 14. MEDINA Trustworthiness Management System data model

If they are not authorized users, they will not be able to use the system as it is restricted by the Smart Contracts design.

Administrators are responsible for authorizing the *Orchestrators'* owners to use the *MEDINA Evidence Trustworthiness Management System*. For this purpose, *Orchestrator* owners need to make a "registration request" to notify the administrators that they want to use the *MEDINA Evidence Trustworthiness Management System*. This notification includes the user identifier (Blockchain address) and a contact email to reply to. Once the notification is received by the administrators, they manually analyse whether the *Orchestrator* owner should be authorized or not. If yes, the authorized *Orchestrator* owner will receive feedback by email with the username and password needed to access the Blockchain viewer client.

Events generation

Every time an operation is executed in the Smart Contract, a Blockchain based event is generated to feed the Blockchain monitor. The Blockchain based events to be generated include (but are not limited to):

- A new administrator is registered.
- An existing administrator is removed.

- A new *Orchestrator* owner is authorized to use the system.
- An existing *Orchestrator* owner is de-authorized to use the system.
- A new *Orchestrator* is registered by its *Orchestrator* owner.
- New evidence information is provided.
- New assessment result information is provided.

5.2.2.3 Blockchain client

Orchestrators need the Blockchain client to interact with the Blockchain network in general, and with the functionalities of the *MEDINA Evidence Trustworthiness Management System* implemented by means of Smart Contracts, in particular. For this purpose, the main functionalities of the Blockchain client are as follows.

Blockchain account management

Every authorized *Orchestrator* owner interacting with the *MEDINA Evidence Trustworthiness Management System* requires a Blockchain account. The account is formed by a Blockchain address, which clearly identifies the user inside the Blockchain network (in fact, it will be considered as the *Orchestrator* owner id in the system because it is unique), and an associated private key, only known by the *Orchestrator* owner (it should be securely kept). The Blockchain account is usually managed by means of a “wallet” included as part of the Blockchain client implemented in MEDINA in order to make users’ interaction with the Blockchain network easier (and transparent of any Blockchain dependency).

In this context, the functionalities available in the Blockchain client related to the Blockchain accounts are:

- Create a new Blockchain account. A new address and its associated private key are automatically generated.
- Get the address associated to a specific private key (for validation purposes).
- Add a specific Blockchain account to the Blockchain client wallet (the private key is needed). Only one account can be added to the wallet in MEDINA (this is a limitation defined for MEDINA).
- Get the Blockchain address added to the wallet (for validation purposes). The Blockchain address previously added to the system Blockchain wallet is obtained.
- Ask the administrators for authorization of a specific Blockchain address (associated to a specific *Orchestrator* owner) to use the *MEDINA Evidence Trustworthiness Management System*.

Blockchain transactions creation

Orchestrators need to generate Blockchain transactions in order to send them to the Blockchain and be understood by the Smart Contracts deployed on the Blockchain. The Blockchain client automatically creates the required Blockchain transaction for executing (calling) all the functionalities available in the *MEDINA Evidence Trustworthiness Management System* Smart Contracts. For this purpose, the Blockchain client internally uses the Web3.js library¹⁷.

API REST for external interaction

The Blockchain component exposes an API REST in order to allow the *MEDINA Orchestrators* to easily interact with the Blockchain client for the functionalities previously described.

¹⁷ <https://web3js.readthedocs.io/en/v1.5.2/>

Figure 15 shows the different endpoints available on the API through Swagger. For more details on the API, please refer to *Appendix C: MEDINA Evidence Trustworthiness Management System API description*.

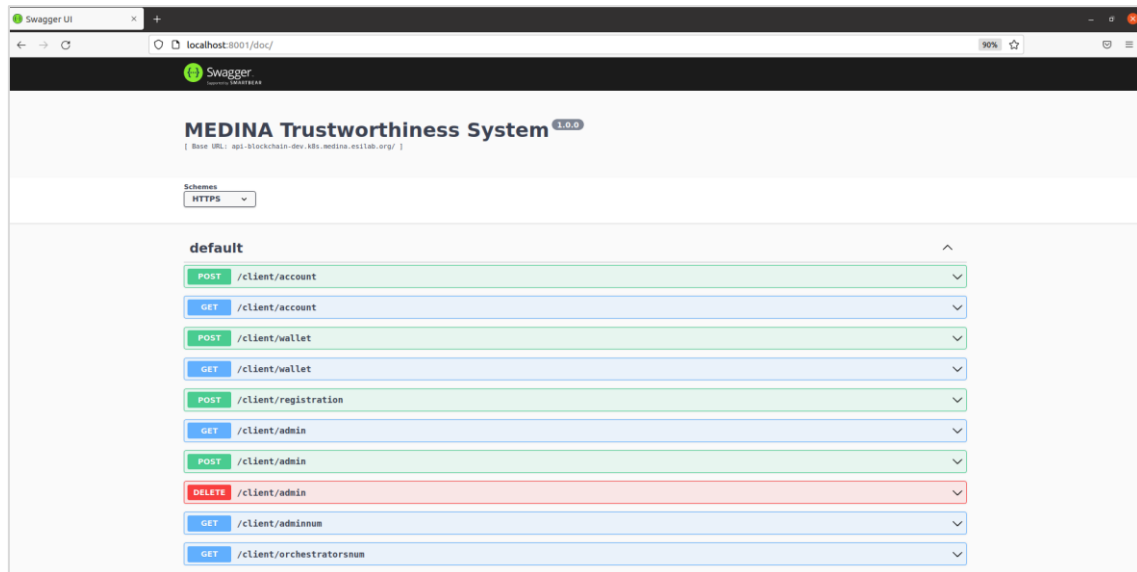


Figure 15. POSTMAN collection for validating Blockchain client API

In addition, the automatic verification service described in 5.2.2.1 also interacts with the Blockchain client API for obtaining the evidence and assessment results recorded in the Blockchain necessary for the automatic verification of the integrity of the real evidence and assessment results.

5.2.2.4 Blockchain viewer

The Blockchain viewer listens to Blockchain based events generated by the Smart Contracts, notifying about new administrators and *Orchestrators'* owners in the system, as well as new evidence or assessment results recorded in the *MEDINA Evidence Trustworthiness Management System*. It provides a mechanism for external users (for example, external auditors, external security engineers, etc.) to verify evidence/assessment results recorded in the Blockchain in a manual way. Figure 16 shows the internal architecture of the Blockchain viewer.

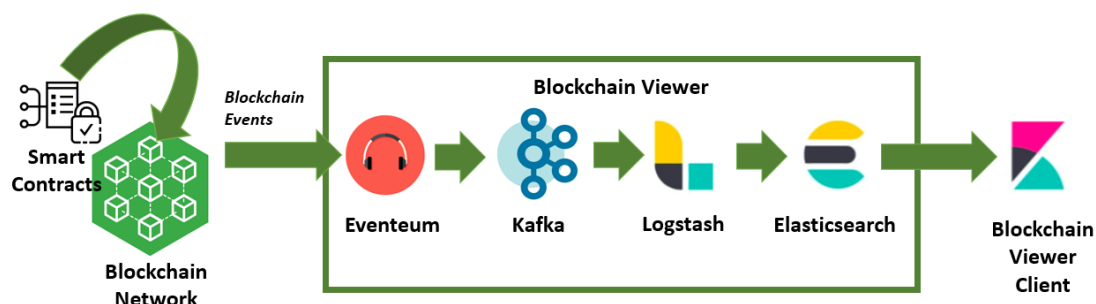


Figure 16. Blockchain viewer architecture (source: MEDINA's own contribution)

The Blockchain viewer is composed of four main elements:

- **Eventum** [26]. It is the component which bridges the Smart Contracts deployed in the Blockchain network with the *MEDINA Evidence Trustworthiness Management System* functionality and the Blockchain Viewer. As it has been explained in 5.2.1, the Smart

Contracts automatically generate Blockchain events that will be listened by Eventum. Eventum will then use Kafka for transmitting them to Logstash. For listening to the events, it is necessary to be subscribed to events from the specific Smart Contract addresses (every Smart Contract has a Blockchain address, which identifies itself in the Blockchain). In addition, the format of the specific events must be also indicated to Eventum (event id, event parameters order, event parameters type).

- **Apache Kafka** [27]. It is the intermediate platform used to distribute Blockchain events between Eventum and Logstash. Kafka uses message queues to provide an asynchronous communications way; this means that the sender (Eventum) and the receiver (Logstash) of the message do not need to interact with the message queue at the same time.
- **Logstash** [28]. It is a log management tool used in the Blockchain viewer for collecting all the events received from Eventum using Kafka queues and normalising them in a common format before routing them again to Elasticsearch to be processed.
- **Elasticsearch** [29]. It is a distributed search and analysis engine, which allows to store, index and process information. It receives Blockchain event data from the Logstash service and categorizes it in four different categories: users, *Orchestrators*, evidence, and assessment results. The information stored in Elasticsearch can be recreated from scratch at any time in case of a security incident resulting in a fully reliable source of information. Elasticsearch exposes an API REST for accessing the information.

5.2.2.5 Blockchain viewer client

There could be several options to consume data from the Blockchain viewer. However, **Kibana** [30] has been considered the best option due to its high compatibility with Elasticsearch as well as the large number of graphical capabilities that it offers, which would highly improve the usability of the system. Kibana is a graphical interface which displays the information from Elasticsearch in real time and through customised dashboards.

Authentication is required to access Kibana dashboards; in addition, different roles have been created for accessing different types of information in the *MEDINA Evidence Trustworthiness Management System*: administrators (“TECNALIA” in MEDINA) have access to all the registered evidence and assessment results from different *Orchestrators*. However, each authorized *Orchestrator* has a limited access only to its associated evidence and assessment results in order to avoid information disclosure.

For this purpose, Kibana provides three security features [31]:

- Spaces, allowing the definition of different “tenants” for each user.
- Roles, allowing the definition of different privileges (different spaces access, for example).
- Users, associated to a specific role (and, consequently, a specific space). In MEDINA, there is an administrator user and one user for each *Orchestrator* (or MEDINA deployed instance).

Figure 17 shows the main dashboard for administrators, where a list of the different authorized *Orchestrator* owners appears with a link (shown in blue) to their associated dashboards. Additionally, a summary of the total number of administrators, authorized *Orchestrator* owners, registered *Orchestrators*, registered evidence, and registered assessment results in the *MEDINA Evidence Trustworthiness Management System* is shown. Finally, different filters have been included for improving the usability of the system: filter by role (administrator or *Orchestrator* owner) or filter directly by *Orchestrator* owner id. For each *Orchestrator*, all the authorized users have the same access privileges irrespective of their role, as defined in D5.4 [22].

Figure 18 shows the main dashboard for each *Orchestrator* owner. Here, the complete list of registered evidence (evidence hashes) and assessment results (assessment result hashes) is shown. This information is useful for manual verifications for auditors. Additionally, a summary of the total number of registered evidence and assessment results for the specific *Orchestrator* owner is shown. Finally different filters have been included for improving the usability of the system: filter by id, hash or associated metadata on the evidence and assessment results.

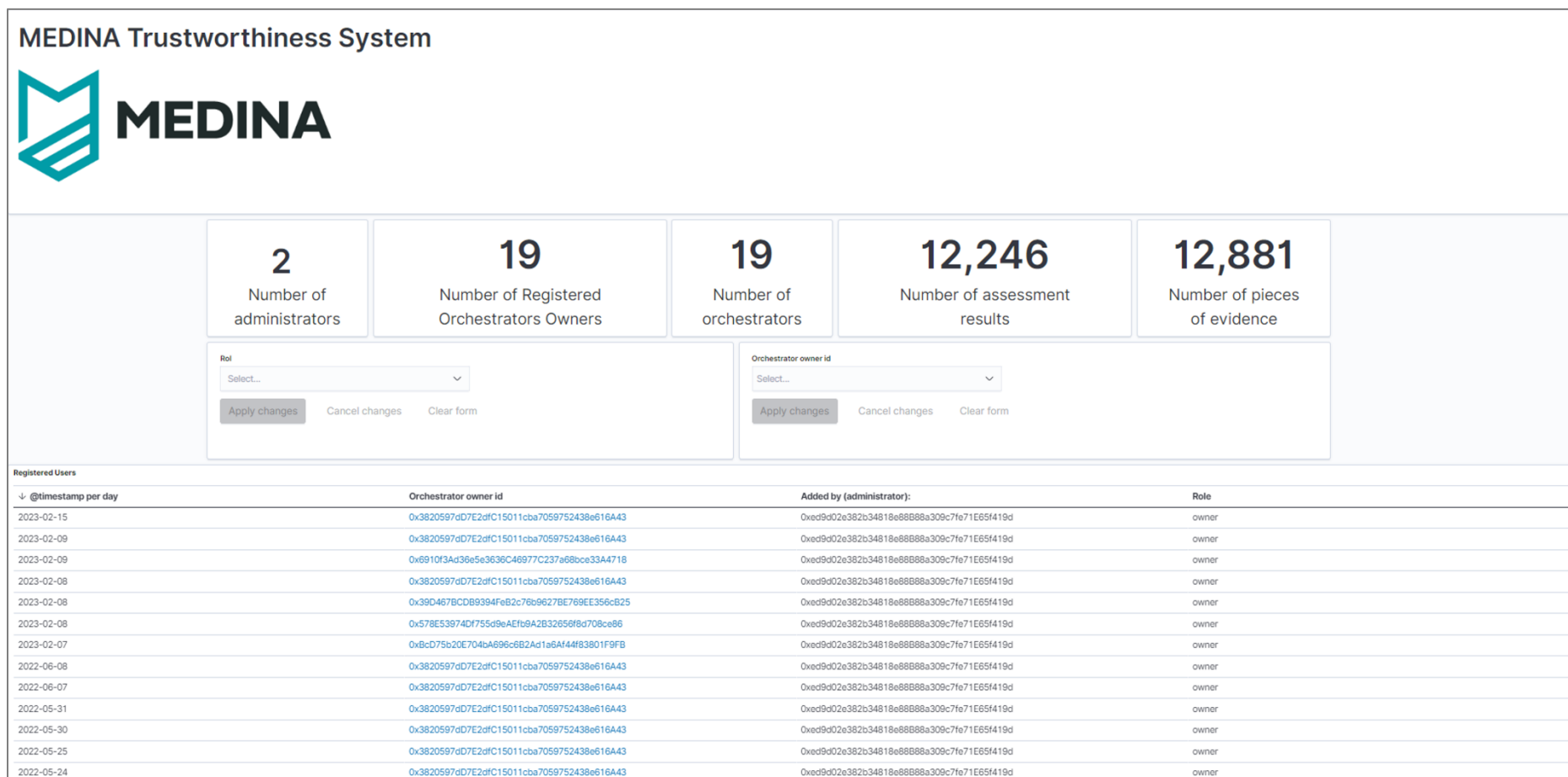



Figure 17. Blockchain viewer graphical interface for administrators

MEDINA Trustworthiness System



Number of evidences

Number of pieces of evidence
13,023

Number of assessment results

Number of assessment results
12,280

Look for specific:

Evidence id
Select...

Evidence Hash
Select...

Resource id
Select...

Tool id
Select...

CSP id
Select...

Apply changes
Cancel changes
Clear form

Registered evidences

Date per day	timestamp	Evidence id	Resource id	Tool id	CSP id	Hash
2023-02-15	1676457278988769372	b8629170-8ddb-4b0e-a7b0-47d5a101aa3f	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%40%F2X%00D%A4%2B%2C%2CP%40%D3X%1E%...
2023-02-15	1676457277955117497	a6ed113b-89bb-4273-9c73-09e9b2d8cc93	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%F5%DA%A1%E8%96%1B%5E5%40P%AB%CE%7%...
2023-02-15	1676457276930725267	d41c8323-8981-4fdb-9774-e6c6a7f8cd28	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%9A%24%C9%EE%9EE%98%B9w%AF%26%B0%C%...
2023-02-15	1676457275903431246	2a37436a-4584-4e1f-afee-8860e191a21e	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%D0%03%09%96%E9%C5%1Cp%A7%D8%9Bo%9F%...
2023-02-15	1676457274877751328	88d55270-12b2-4a5b-b15c-fc7c91049d	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	%9D%F67%A0%60%09%01g%C6%26%02%A2%CA%...
2023-02-15	1676457273853865836	a1747320-8d16-4c27-9aef-0626ad917a8e	/subscriptions/463cd324-9281-4ba1-b42d-ef90d...	Clouditor Evidences Collection	N/A	H%DCf%E7%B85%00%17%D1%E5%936%8A%C3z%...

Filter Assessment Results. Look for a specific:

Assessment Result id
Select...

Metric id
Select...

Assessment Result Hash
Select...

Compliance Hash
Select...

Apply changes
Cancel changes
Clear form

Registered Assessment Results

Date per day	timestamp	Assessment id	Metric id	Assessment Hash	Compliance Hash	Associated evidences
2023-02-15	1676459060172149348	61ab60c2-bdad-4221-8ec9-a73f25eddac3	AtRestEncryptionEnabled	%85%16B%A2%E0%A3%F8%7F%7C%5C%3B%84%...	%15%ESY%B6%AO-%402%BF%E8%D0%D3%BA%2...	5ff4081d-4aaf-4841-9581-aa883ddd835f
2023-02-15	1676458823291346173	2c67eb59-502c-4d40-bf60-7202c5c632ab	OSLoggingEnabled	%DEL-%DF%4F8 %9C%94%F4WPrtOf%85k%00...	7%CCo%0D~z,%3C%3A0%82%EE%7B%5Db%...	5e237f69-5f3f-45d5-9493-bd8abab85b77
2023-02-15	1676458759386442634	974ecba0-15b6-4204-857b-ac305f4d0a26	AtRestEncryptionEnabled	%F5%BB%ED%AE%97%FEG%00b%81%09%60%99...	%15%ESY%B6%AO-%402%BF%E8%D0%D3%BA%2...	0c5adf1d-8d3b-4a56-82d4-dae70eaa987
2023-02-15	167645845927986421	b492f28f-b29f-4759-91a2-d449cddea13f	AtRestEncryptionEnabled	%A4%94%B9%06%12%E7r%11%0A%233%D9%DD...	%15%ESY%B6%AO-%402%BF%E8%D0%D3%BA%2...	436ebd15-273f-4f58-a8c6-0745082317b5

Figure 18. Blockchain viewer graphical interface for Orchestrator owners

5.2.2.1 Automatic verification service

In addition to the manual way of accessing the hashes of evidence and assessment results (and additional information), auditors demand an automatic way of verifying the integrity of evidence and assessment results. The automatic verification service fulfils this objective by providing auditors with a graphical tool for automatic validation of evidence and assessment results from the *Orchestrator* against the information recorded on the Blockchain.

The automatic verification service allows the integrity verification of evidence and assessment results. Figure 19 shows the “home” page of this service.

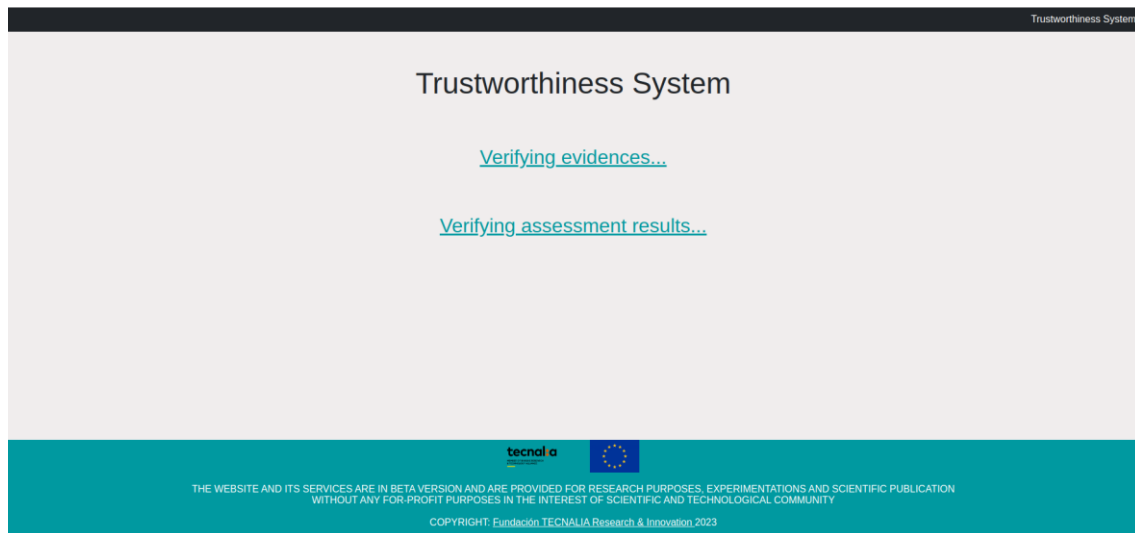


Figure 19. Automatic verification service home page

Both for evidence and assessment results, the only information to be provided by auditors is the ID that identifies the piece of evidence or the assessment result. This information is provided in a form shown in Figure 20.

Figure 20. Automatic verification service form

The automatic verification service will automatically obtain the evidence or assessment result from the *Orchestrator* and calculate its hash. At the same time, the service will interact with the Blockchain client to obtain the piece of evidence or assessment result hash previously recorded on the Blockchain. Both hashes are automatically compared, and the result of the integrity check

is shown to the auditor. Figure 21 and Figure 22 show a correct and incorrect integrity verification check, respectively.

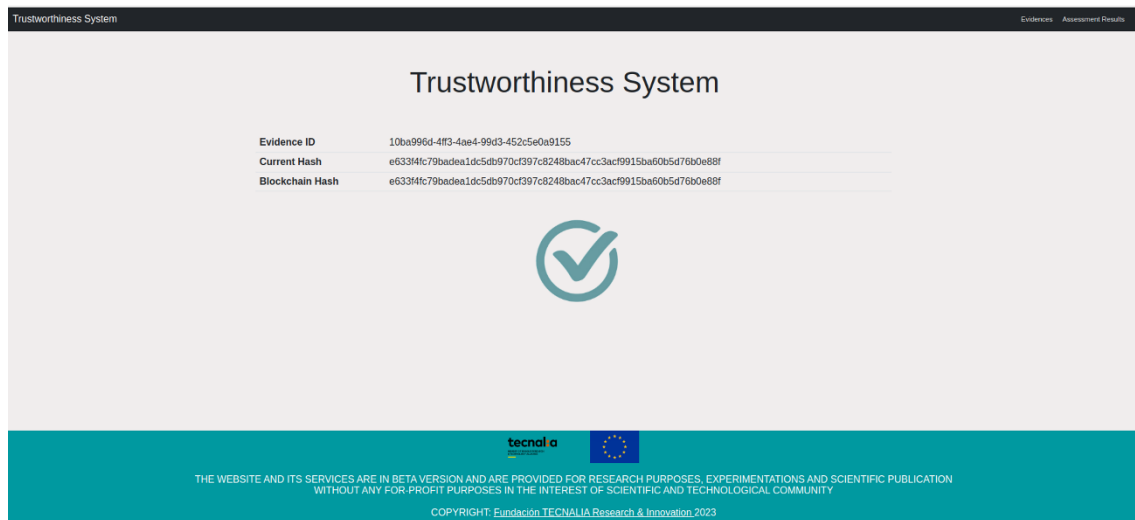


Figure 21. Automatic correct integrity verification service

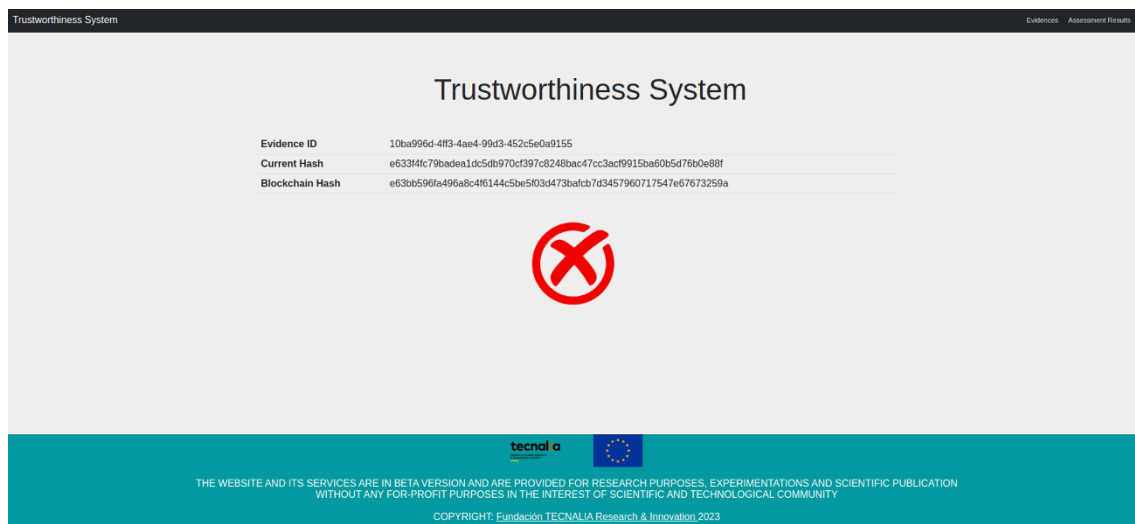


Figure 22. Automatic incorrect integrity verification service

5.2.3 Technical specifications

Table 4 shows the main technical specifications of the *MEDINA Evidence Trustworthiness Management System*.

Table 4. *MEDINA Evidence Trustworthiness Management System* technical specifications

DEVELOPMENT	
Type	Software
Operating Systems	Windows or Linux
Databases	Blockchain (Quorum) and MongoDB
GUI	Through Kibana (viewer client) and React (automatic verification service)
Programming language	Go, Solidity, JavaScript, Scripting, React, Nodejs

Development Environment	Solidity, Elastic Stack, npm
INSTALLATION AND DEPLOYMENT	
Software Requirements	Docker engine and its supporting packages
Hardware Requirements	Hardware virtualization support
Containerization	Docker
Communications	Secure HTTP (HTTPS)
EXECUTION	
Execution Time	It depends on the network stability
Execution Frequency	Asynchronous

5.3 Delivery and Usage

This section describes the information needed for the installation and use of the *MEDINA Evidence Trustworthiness Management System*. Besides, it also details the licensing information and related packages and repositories.

5.3.1 Package information

Only the Blockchain client and the automatic verification service need to be provided, as the rest of the *MEDINA Evidence Trustworthiness Management System* components are provided as a service from TECNALIA's premises. Both components are packaged as a docker image.

5.3.2 Installation instructions

Only the Blockchain client and the automatic verification service need to be installed, as the rest of the *MEDINA Evidence Trustworthiness Management System* components are provided as a service from TECNALIA 's premises.

The installation process (from the *Orchestrator* owner premises) is as follows (the same process should be followed for both components).

```
sudo docker login optima-medina-docker-dev.artifact.tecnalia.com (and enter
your username and password; registration in Orein is needed in advance)

sudo docker pull optima-medina-docker-dev.artifact.tec-
nalia.com/wp3/t35/blockchain:latest

sudo docker run -d -p 8001:8001 -name medina_blockchain optima-medina-
docker-dev.artifact.tecnalia.com/wp3/t35/blockchain:latest
```

5.3.3 User Manual

The *Orchestrator* is the component which needs to use the Blockchain client to provide evidence and assessment results to the *MEDINA Evidence Trustworthiness Management System*. Once the docker image is running (after following the installation steps in section 5.3.2), the *Orchestrator* needs the following:

1. A Blockchain account needs to be generated and added to the Blockchain wallet (inside the Blockchain client) for each *Orchestrator* owner through a POST to the /client/account endpoint and a POST to the /client/wallet endpoint of the Blockchain client API.
2. Request Authorization of the *Orchestrator* owner in the *MEDINA Evidence Trustworthiness Management System* through a POST to the /client/registration endpoint of the Blockchain client API. This way, TECNALIA will automatically receive an

- email with the Blockchain id (account) to be authorized in the system. TECNALIA will manually authorize the Blockchain account (*Orchestrator* owner) and will generate the credentials needed for accessing the Blockchain viewer (user and password).
3. Once the *Orchestrator* owner is authorized, the *Orchestrator*, as technical component, needs to be registered in the system through a POST to the `/client/orchestrator` endpoint. From this moment, all the authorized *Orchestrator* owners' functionalities from the *MEDINA Evidence Trustworthiness Management System* can be executed. The interested reader may refer to *Appendix C: MEDINA Evidence Trustworthiness Management System API description* to see the available functionalities: provide evidence or assessment results; get the list of registered evidence or assessment results ids; get the information of a specific evidence or assessment result id; check the hashes of a specific evidence or assessment result.
 4. Additionally, the API also includes additional endpoints for admin purposes, as TECNALIA (as administrator) could make *Orchestrator* owners administrators of the system, if needed.

In addition, the correct sequence of steps for testing and validating all the functionalities from the web-based Blockchain viewer client (Kibana) is as follows:

1. Login in the system is required (only authenticated users can access the dashboard) (<https://medina.bclab.dev>; [internal use only - authentication is required])
2. The main dashboard associated to the specific user is automatically displayed. Here, the list of evidence or assessment results can be consulted, or filters can be applied as needed.

Finally, the automatic verification service provides a graphical way for verifying the integrity of evidence and assessment results from the *Orchestrator* against their values when recorded on the Blockchain. The flow is as follows:

1. Select the type of information to verify: either evidence or assessments result.
2. Provide the ID of the information to verify (either evidence ID or assessment result ID). This ID is unique and identifies the evidence or assessment result.
3. The current and recorded hash values for the specific information ID are automatically provided as well as the integrity verification result.
4. This process can be repeated as many times as needed.

5.3.4 Licensing information

Proprietary. Copyright by TECNALIA.

5.3.5 Download

This section is not applicable. All the components of the *MEDINA Evidence Trustworthiness Management System* are provided as a service from TECNALIA and TECNALIA owns a proprietary license, so no source code can be provided.

5.4 Advancements within MEDINA

This section reports on the progress implemented in the *MEDINA Evidence Trustworthiness Management System* component from November 2022 to April 2023 (formal end of WP3). In particular:

- The automatic verification service has been designed and implemented.
- The automatic verification service has been integrated within the MEDINA framework.

- The *MEDINA Evidence Trustworthiness Management System* has been integrated with the MEDINA keycloak authentication system following the authorization requirements defined in D5.4 [22].
- The *MEDINA Evidence Trustworthiness Management System* has been extensively tested.

5.5 Limitations and Future Work

The main limitation in the current development of the *MEDINA Evidence Trustworthiness Management System* prototype is related to the Blockchain network. For MEDINA, a Blockchain network based on three nodes has been deployed at TECNALIA for prototype purposes. However, in real deployments, more nodes and from more organizations are needed to guarantee suitable decentralization and governance of the Blockchain network.

Taking this into consideration, the definition and creation of a suitable Blockchain network for the *MEDINA Evidence Trustworthiness Management System* is needed as future work, either by creating a new network from different organizations or by taking advantage of existing ones, such as those provided by the European Blockchain Services Infrastructure (EBSI) [33].

6 Checklist for the Self-assessment of EUCS security requirements

In response to Article 54 recital (g) of the EUCSA [34] which states that “A European cybersecurity certification scheme shall include at least the following elements [...] (g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;” EUCS [35] has defined an evidence-based assessment approach that is to be used solely for the basic level of assurance.

The proposed evidence-based conformity assessment approach states that the evaluation does not require a “full-fledged audit of the cloud service to be certified” [35] but is more oriented towards “facilitating a controlled environment for providing limited assurance while keeping the associated cost for certification affordable for smaller CSP’s” [35] and follows a checklist-oriented approach.

The process to be followed is similar to the one a CSP would need to follow in order to get certified, where it would need to create the application request, define the scope of certification, create the audit plan, execute the assessment procedures, analyse the results, issue the assurance report, review the evaluation, and obtain the certification.

The difference here is that in the basic level of assurance, the CSP itself, and not an external or third-party auditor, can create and carry out the audit plan and execute the assessment procedures, also analysing the results, which are sent to the CAB for further analysis and audits. Figure 23 shows a simplified version of this process.

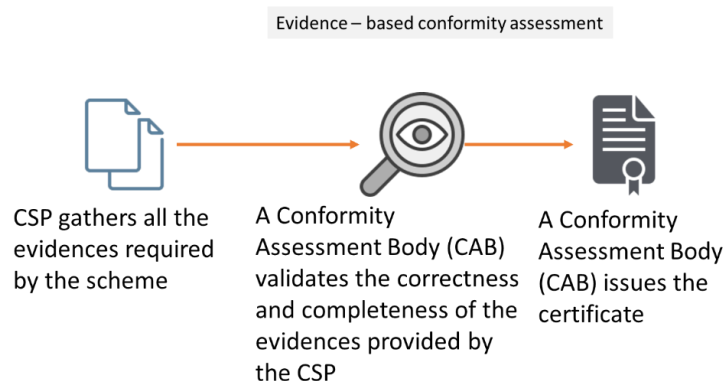


Figure 23. Evidence-based conformity assessment (adapted from [35])

Hence, the challenge here is: how to guide CSPs, especially smaller ones, in this evidence-based conformity assessment methodology? In fact, checklists could be not yet available, or they need to be complemented (e.g., they do not show examples of evidence that can be delivered and can be considered valid to demonstrate the compliance of a requirement).

The main goal of the checklists elaborated in MEDINA (a.k.a. “MEDINA Questionnaires”) is therefore to develop an assessment model for EUCS requirements that can be understood by less experienced compliance managers. The main target users of the *MEDINA Questionnaires* are small CSPs. However, auditors and CABs could also adopt it as guidance and benefit from them.

MEDINA Questionnaires are based on the experience of the auditors and consultants that have worked in the checklists, with feedback incorporated from the CSPs that participated in MEDINA, as well as from literature. The questions are extracted directly from the EUCS requirements themselves. They have been split for understandability reasons into multiple questions, that is,

from one requirement multiple questions have been created. However, the number of overall questions is important as this self-assessment model must not be very heavy and difficult to use.

In addition to the questions, a very important aspect that has been included in the design of the *MEDINA Questionnaires* is **evidence**. ISO 9000 defines evidence as the data supporting the existence or verity of something [36]. In MEDINA, two types of evidence are distinguished:

- **Technical evidence:** data supporting the compliance of a technical requirement or measure. Examples: protocol version, password length.
- **Organizational evidence:** data supporting the compliance of an organizational requirement. Example: existence of a policy and/or procedure document.

Hence, the *MEDINA Questionnaires* identify some examples of evidence that the CSP shall submit to the CAB for the evaluation assessment. The evidence examples shown are not meant to be an exhaustive list but just a guidance.

The *MEDINA Questionnaires* are supported in a spread sheet, where the first sheet shows the index of categories (see Figure 24), and each of the other sheets are associated with an EUCS Category. Figure 25 shows an excerpt of the checklist for the “Operational Security” category. The checklists have a tabular form with the following structure:

- **ControlID:** id of the EUCS control coming from the draft candidate version of the EUCS scheme August 2022 [3].
- **Control:** description of the control coming from the draft candidate version of the EUCS scheme August 2022.
- **ReqID:** id of the requirement coming from the draft candidate version of the EUCS scheme August 2022.
- **Requirement:** description of the requirement coming from the draft candidate version of the EUCS scheme August 2022.
- **Question ID:** unique identified of each question, related to each requirement.
- **Statement / Question:** question that the CSP should answer in the evaluation to comply with the requirement as requested in the scheme.
- **Evidence:** the document, section of a document, or any kind of information that the CSP is required to provide in order to prove that the requirement is properly implemented in accordance with what it is required. The list provided is not meant to be exhaustive but rather an indication of what kind of information is expected to be provided.



MEDINA
MEDINA Questionnaires

EUCS Controls - SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES

- ▶ A1. Organizational Information Security
- ▶ A2. Information Security Policies
- ▶ A3. Risk Management
- ▶ A4. Human Resources
- ▶ A5. Asset Management
- ▶ A6. Physical Security
- ▶ A7. Operational Security
- ▶ A8. Identity, Authentication and Access Control Mgmt
- ▶ A9. Cryptography and Key Management
- ▶ A10. Communication Security
- ▶ A11. Portability and Interoperability
- ▶ A12. Change and Configuration Management
- ▶ A13. Development of Information Systems
- ▶ A14. Procurement Management
- ▶ A15. Incident Management
- ▶ A16. Business Continuity
- ▶ A17. Compliance
- ▶ A18. User Documentation
- ▶ A19. Dealing with Investigation Requests from Government Agencies
- ▶ A20. Product Safety and Security

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

Figure 24. Summary of the EUCS categories in the MEDINA Questionnaires

A7. Operational Security												
Dom	Category	Objective	Control	Control objective	ReqID	Requirement	Level	Question	Statement/Questions	Val	Evidence	Comm
A7	OPERATIONAL SECURITY	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against	OPS-01	CAPACITY MANAGEMENT - PLANNING		The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.		Q1-OPS-01.1B	Does the CSP define procedures to plan for capacities and resources (personnel and IT resources)?	50	- Capacity plan - Specific capacity procedures	
			OPS-01				Basic	Q2-OPS-01.1B	Do procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload?	50	- Capacity plan (encompasses future capacity requirements) - Specific capacity procedures	
			OPS-01				Basic	Q3-OPS-01.1B	Does the CSP implement procedures to plan for capacities and resources (personnel and IT resources)?	100	- Capacity plan audit	
			OPS-01			The CSP shall meet the requirements included in contractual agreements with CSCs regarding the provision of the cloud service in case of capacity	Basic	Q1-OPS-01.2B	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of capacity bottlenecks?	50	- Monitoring reports - Contractual agreements - Non-conformities to the contract (if there are non-compliances)	
			OPS-01				Basic	Q2-OPS-01.2B	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of IT resources outages?	NA	- Monitoring reports - Non-conformities to the contract/SLA (if there are non-compliances) - Contractual agreements	
			OPS-02	CAPACITY MANAGEMENT - MONITORING		The capacities of critical resources such as personnel and IT resources are monitored.	Basic	Q1-OPS-02.1B	Does the CSP document technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	50	- Multidimensional QoS prediction methods	
			OPS-02				Basic	Q2-OPS-02.1B	Does the CSP implement technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure	50	- Service level agreement - SLA compliance report	
			OPS-02				Basic	Q3-OPS-02.1B	Does the CSP define organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure	100	- Multi-dimensional QoS measures	
			OPS-02				Basic	Q4-OPS-02.1B	Does the CSP implement organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure	50	- Service level agreement - SLA compliance report	
			OPS-03	CAPACITY MANAGEMENT - CONTROLLING OF RESOURCES		The CSCs have the ability to manage the IT resources allocated to them in order to avoid overcrowding of resources and to achieve	Basic	Q1-OPS-03.1B	Does the CSP enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs?	100	- Contractual agreement - SLA - Privileges to use the monitoring and control tools	
			OPS-04	PROTECTION AGAINST MALWARE - POLICIES		Policies are defined that ensure the protection against malware of IT equipment related to the cloud service	Basic	Q1-OPS-04.1B	Does the CSP define policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering the use of system-specific protection mechanisms?	100	- Documented policies and procedures	
			OPS-04			The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects: (1) Use of system-specific protection mechanisms; (2) Operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the	Basic	Q2-OPS-	Does the CSP implement policies and procedures	50	- System-specific protection	

Figure 25. Excerpt of the checklist for the Operational Security category

The first version of the MEDINA Questionnaires was released in D3.1 [4]. The checklists included 532 questions and were related to the 220 basic assurance level requirements defined in the draft candidate EUCS version published in December 2020 [35].

In the second version of the *MEDINA Questionnaires*, reported in D3.2 [4], the number of questions as well as the formulation evolved. Questions and evidence were reviewed and updated with respect to the description of the EUCS requirements defined, first in the basic level of assurance of the candidate EUCS November 2021 and second in the basic level of assurance of the draft candidate version of the EUCS scheme August 2022 [3]. Also, checklists for the substantial and high level of assurance requirements were elaborated and included in the *MEDINA Questionnaires*. The answers provided by a CSP to questions at a given level of assurance can be used to assess the compliance at a higher level; this feature has been used in the implementation of the scorecard functionality described below.

In the final version of the *MEDINA Questionnaires*, the checklists for the substantial and high assurance level requirements have been revised and updated. Table 5 shows the number of requirements in the draft candidate version of the EUCS scheme August 2022 and the final number questions elicited for each level of assurance (basic, substantial, and high). *Appendix E: Self-assessment Questionnaires for EUCS basic requirements* includes the checklist corresponding to the requirements of the EUCS basic level of assurance.

Table 5. Coverage of EUCS requirements by the MEDINA Questionnaires

	Number of EUCS requirements [3]	Number of elicited questions in MEDINA Questionnaires
Basic level of assurance	220	498
Substantial level of assurance	351	865
High level of assurance	427	1009

Table 6 shows the final number of questions that have been elicited for each Category of controls in the EUCS, as well as the number of requirements in each Category, for the three levels of assurance (basic, substantial, and high).

Table 6. Coverage of EUCS requirements by the MEDINA Questionnaires for each EUCS category

EUCS Category	Basic		Substantial		High	
	# of Req.	# of Quest.	# of Req.	# of Quest.	# of Req.	# of Quest.
A1.Organisation of Information Security	6	15	7	22	8	26
A2.Information Security Policies	10	26	13	31	15	34
A3.Risk Management	10	27	11	27	12	29
A4.Human Resources	16	36	22	58	23	74
A5.Asset Management	9	14	11	20	15	30
A6.Physical Security	12	35	21	48	27	55
A7.Operational Security	33	66	52	125	65	155
A8.Identity, Authentication and Access Control Management	21	46	49	98	56	116
A9.Cryptography and Key Management	5	18	9	25	10	26
A10.Communication Security	15	38	21	52	26	55
A11.Portability and Interoperability	8	16	11	20	13	24
A12.Change and Configuration Management	8	20	11	32	18	45
A13.Development of Information Systems	11	20	27	65	32	66
A14.Procurement Management	13	26	14	57	21	66
A15.Incident Management	14	33	20	45	24	55
A16.Business Continuity	3	10	9	47	10	48
A17.Compliance	5	14	10	29	15	35
A18.User Documentation	11	17	14	31	15	34
A19.Dealing with Investigation Requests from Government Agencies	5	9	6	10	7	11
A20.Product Safety and Security	5	12	13	23	15	25
	220	498	351	865	427	1009

The *MEDINA Questionnaires* also incorporate a **scorecard functionality** for each EUCS Category, that shows the level of compliance of the security controls in that Category. The level achieved by each security control in the scorecard is calculated as an average of the level of compliance indicated by the CSP on the set of questions associated with that security control (see Figure 25). The following options are available to indicate the degree of compliance with a question:

- 100% => Fully supported
- 50% => Partially supported
- 0% => Not supported at all
- N.A. => Not applicable

We have implemented a scorecard for each level of assurance (basic, substantial, and high), so that the CSP can see at a glance the compliance of all controls for each level, and an overall scorecard that shows a comparison of compliance at control level for the three levels of assessment. Figure 26 shows the scorecards for the self-assessment of controls in the “Operational Security” category.

In addition, the *MEDINA Questionnaires* also provide three overall scorecards showing the level of compliance of all EUCS Categories for the corresponding basic, substantial, and high levels of assurance. Figure 27 shows an example of a scorecard indicating the overall level of compliance of a self-assessment for the basic level of assurance.



Figure 26. Scorecards for the Operational Security category in MEDINA Questionnaires

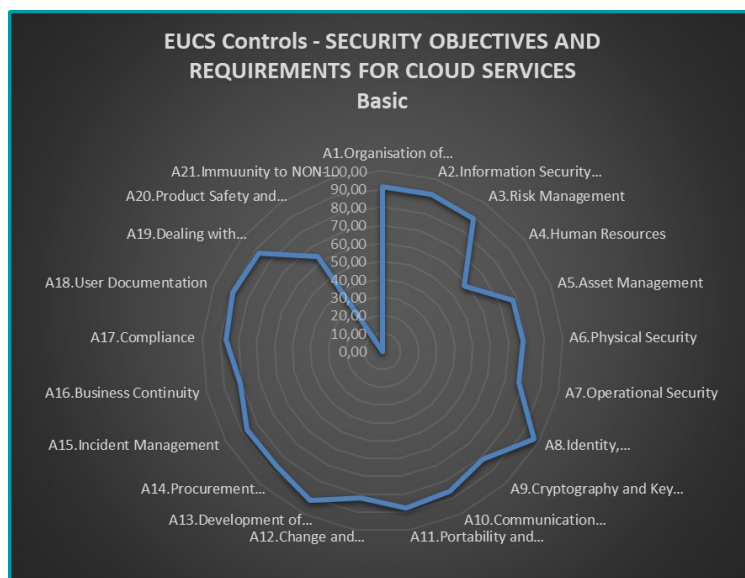


Figure 27. Overall scorecard in MEDINA Questionnaires

Finally, as reported in D2.2 [17], the checklists defined for the assessment of the EUCS requirements at the basic, substantial, and high levels of assurance have been integrated in the MEDINA *Catalogue of Controls and Metrics*. In this way, CSPs could have a more flexible tool to answers questions in a more automated way, storing the results electronically, and providing immediate and visual feedback.

The CSP can select the assurance level for the assessment, and then provide answers to several questions to check compliance with each of the requirement involved (see Figure 28). It also allows entering comments related to a question and textual references to locate the evidence supporting the answer given. The tool provides a summary dashboard with quantitative values to reflect the degree of compliance for each control. The authorization and filtering capabilities implemented in the Catalogue allow auditors to access the self-assessment questionnaires and enter non-conformities for each non-compliant requirement.

MEDINA Catalogue v0.0.1-SNAPSHOT

Home Entities Questionnaires Administration

Questionnaire

Security Category navigator

Categories

- A1: Organisation of Information Security
- A2: Information Security Policies
- A3: Risk Management
- A4: Human Resources
- A5: Asset Management
- A6: Physical Security
- A7: Operational Security
- A8: Identity, Authentication and Access Control Management
- A9: Cryptography and Key Management
- A10: Communication Security
- A11: Portability and Interoperability
- A12: Change and Configuration Management
- A13: Development of Information Systems
- A14: Procurement Management

A1: Organisation of Information Security Current Security Category

Choose a Control: OIS-01 OIS-02 OIS-03 OIS-04 Security Control navigator

OIS-01: The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service. Current Security Control

OIS-01.B: The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service. Requirement

Questions

Q1: Has the CSP an information security management system (ISMS) documented?

☐ Fully supported.
☐ Partially supported.
☐ Not supported at all.
☐ Not applicable.

Evidence:

Comments:

Q2: Does the CSP implement an information security management system (ISMS)?

☐ Fully supported.
☐ Partially supported.
☐ Not supported at all.
☐ Not applicable.

Evidence:

Comments:

Q3: Does the CSP maintain an information security management system (ISMS)?

☐ Fully supported.
☐ Partially supported.
☐ Not supported at all.
☐ Not applicable.

Evidence:

Comments:

Figure 28. Integration of the checklist of the MEDINA Questionnaires in the Catalogue of controls and metrics (Source D2.2 [17])

The source code of the *Catalogue of Controls and Metrics* is available at the public GitLab repository of the MEDINA project¹⁸.

¹⁸ <https://git.code.tecnalia.com/medina/public/catalogue-of-controls>

7 Conclusions

This document presents the architecture of the *MEDINA Evidence Management Tools* [KR4], which comprises the integration of *Clouditor*, *Codyze*, *Wazuh*, the *Vulnerability Assessment tool (VAT)*, the *Assessment and Management of Organisational Evidence (AMOE)*, the *Generic Evidence Collector (GEC)* and finally the *MEDINA Evidence Trustworthiness Management System*, which aims at ensuring that all evidence and assessment results collected by the previous tools are secured. This is achieved by means of smart contracts.

The deliverable starts by introducing the architecture, data model and sequence diagrams of the *MEDINA Evidence Management Tools*, extending the models and explanations already presented in D5.2 [1].

The document then deepens into the main ideas and motivation for the further development of the tools that comprise the *MEDINA Evidence Management Tools*, even if the technical details of the implementation are provided in D3.6 [2]. Furthermore, the coverage of the requirements of assurance level high coming from the draft candidate version of the EUCS scheme August 2022 [3] has been matched with the different tools comprising the *MEDINA Evidence Management Tools*. Please note that the EUCS requirements referred in this deliverable correspond to a draft version of the ENISA catalogue and are not intended for being used outside the context of MEDINA.

Furthermore, the functional and technical details of the *MEDINA Evidence Trustworthiness Management System*, how it fits into MEDINA, the architecture of the prototype, the description of the prototype and how it is delivered has also been presented. The system is based on Smart Contracts and is currently deployed on a Blockchain network in TECNALIA.

Finally, and although MEDINA mostly focuses on the automated monitoring and the high assurance level of the EUCS, CSPs may struggle in assessing EUCS requirements, especially the smaller CSPs. The checklists presented in section 6 can guide CSPs in their self-assessment activities by showing what kind of evidence they should provide to CABs when conducting the third-party assessment.

8 References

- [1] MEDINA Consortium, “D5.2 MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v2,” 2022.
- [2] MEDINA Consortium, “D3.6 Tools and techniques for collecting evidence of technical and organisational measures - v3,” 2023.
- [3] ENISA, “EUCS – Cloud Services Scheme,” Draft version provided by ENISA (August 2022) - not intended for being used outside the context of MEDINA, 2022.
- [4] MEDINA Consortium, “D3.2 Tools and techniques for the management of trustworthy evidence-v2,” 2022.
- [5] MEDINA Consortium, “D5.1 MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v1,” 2021.
- [6] MEDINA Consortium, “D5.2 MEDINA requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy - v2,” 2022.
- [7] MEDINA Consortium, “D4.3 Tools and Techniques for the Management and Evaluation of Cloud Security Certifications-v3,” 2023.
- [8] MEDINA Consortium, “D6.2 Use cases specification and evaluation methodology-v2,” 2021.
- [9] Fraunhofer AISEC, “CLOUDITOR - Continuous Cloud Assurance,” [Online]. Available: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/Whitepaper_Clouditor_Feb2017.pdf. [Accessed April 2023].
- [10] MEDINA Consortium, “D2.5 Specification of the Cloud Security Certification Language-v3,” 2023.
- [11] Fraunhofer AISEC, “CODYZE - Static code analysis tool,” April 2023. [Online]. Available: <https://github.com/Fraunhofer-AISEC/codyze>.
- [12] “w3af,” [Online]. Available: <http://w3af.org/>. [Accessed April 2023].
- [13] OWASP Foundation, “OWASP Zed Attack Proxy (ZAP),” [Online]. Available: <https://owasp.org/www-project-zap/>. [Accessed April 2023].
- [14] “Nmap,” [Online]. Available: <https://nmap.org/>. [Accessed April 2023].
- [15] Wazuh Inc., “Wazuh,” [Online]. Available: <https://wazuh.com/>. [Accessed April 2023].
- [16] I. Kunz, A. Schneider and C. Banse, “Privacy Smells: Detecting Privacy Problems in Cloud Architectures,” in *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020.
- [17] MEDINA Consortium, “D2.2 Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v2,” 2023.

- [18] A. Ahmad, M. Saad, M. Bassiouni and A. Mohaisen, "Towards blockchain-driven, secure and transparent audit logs," in *15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018.
- [19] J. Chen, "Certchain: Public and efficient certificate audit based on blockchain for tls connections," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, 2018.
- [20] J. Dai, "Three essays on audit technology: audit 4.0, blockchain, and audit app," Rutgers University-Graduate School-Newark, 2017.
- [21] A. M. Rozario and C. Thomas, "Reengineering the audit with blockchain and smart contracts," *Journal of emerging technologies in accounting*, vol. 16, no. 1, pp. 21-35, 2019.
- [22] MEDINA Consortium, "D5.4 MEDINA integrated solution-v2," 2023.
- [23] Consensys, "Build on Quorum, the complete open source blockchain platform for business," 2021. [Online]. Available: <https://consensys.net/quorum/>. [Accessed April 2023].
- [24] K. Li, H. Li, H. Wang, H. An, P. Lu, P. Yi and F. Zhu, "PoV: an efficient voting-based consensus algorithm for consortium blockchains," *Frontiers in Blockchain*, vol. 3, no. 11, 2020.
- [25] Consensys, "Constellation," 2021. [Online]. Available: <https://github.com/ConsenSys/constellation>. [Accessed April 2023].
- [26] GitHub, "Eventum source code," 2021. [Online]. Available: <https://github.com/eventum/eventum>. [Accessed April 2023].
- [27] Apache, "APACHE KAFKA," 2021. [Online]. Available: <https://github.com/eventum/eventum>. [Accessed April 2023].
- [28] Logstash. [Online]. Available: <https://www.elastic.co/es/logstash/>. [Accessed April 2023].
- [29] Elasticsearch B.V., "Elasticsearch," [Online]. Available: <https://www.elastic.co/es/what-is/elasticsearch>. [Accessed April 2023].
- [30] Elasticsearch B.V., "Kibana," [Online]. Available: <https://www.elastic.co/es/kibana/>. [Accessed April 2023].
- [31] Elastic, "Securing Access to Kibana," [Online]. Available: <https://www.elastic.co/guide/en/kibana/current/tutorial-secure-access-to-kibana.html>. [Accessed April 2023].
- [32] I. Williams, "Cross-chain blockchain networks, compatibility standards, and interoperability standards: The case of european blockchain services infrastructure. In *Cross-Industry Use of Blockchain Technology and Opportunities for the Future*," *IGI Global*, pp. 150-165, 2020.
- [33] European Commission;, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52," June 2019. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>. [Accessed April 2023].

- [34] ENISA, "EUCS – Cloud Services Scheme," [Online]. Available: <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>. [Accessed April 2023].
- [35] International Standards Organization, "ISO 9000:2015 - Quality management systems — Fundamentals and vocabulary".
- [36] Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven Deep Dive," 2020.
- [37] Cloud Security Alliance, "State of Cloud Security Concerns, Challenges, and Incidents," 2021.
- [38] J. Montes, A. Sánchez, B. Memishi, M. S. Pérez and G. Antoniu, "GMonE: A complete approach to cloud monitoring," in *Future Generation Computer Systems*, 29(8), 2026-2040, 2013.
- [39] K. A. Torkura, M. I. Sukmana, F. Cheng and C. Meinel, "Continuous auditing and threat detection in multi-cloud infrastructure," in *Computers & Security*, 2021.
- [40] K. A. Torkura, M. I. Sukmana, T. G. H. Strauss, F. Cheng and C. Meinel, "CSBAuditor: Proactive Security Risk Analysis for Cloud Storage Broker Systems," in *IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 2018, 2018.
- [41] Palo alto networks,, "Prisma cloud," [Online]. Available: <https://www.paloaltonetworks.com/resources/datasheets/cloud-security-posture-management>. [Accessed April 2023].
- [42] D. Knoblauch and C. Banse, "Reducing Implementation Efforts in Continuous Auditing Certification Via an Audit API," in *IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Napoli, 2019.
- [43] Balbix, "What to know about Vulnerability Scanners and Scanning Tools," [Online]. Available: <https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/>. [Accessed April 2023].
- [44] Rapid7, "Appspider," [Online]. Available: <https://www.rapid7.com/products/appspider/>. [Accessed April 2023].
- [45] PortSwigger Ltd., "Burp Suite," [Online]. Available: <https://portswigger.net/burp>. [Accessed April 2023].
- [46] Tenable Inc., "Nessus," [Online]. Available: <https://www.tenable.com/products/nessus>. [Accessed April 2023].
- [47] Qualys Inc., "Web Application Scanning," [Online]. Available: <https://www.qualys.com/apps/web-app-scanning/>. [Accessed April 2023].
- [48] Greenbone Networks, "OpenVAS," [Online]. Available: <https://www.openvas.org/>. [Accessed April 2023].

- [49] Sarosys LLC, "Arachni Scanner," [Online]. Available: <https://www.arachni-scanner.com/>. [Accessed April 2023].
- [50] M. S. Bernardo Damele Assumpcao Guimaraes. [Online]. Available: <https://sqlmap.org/>. [Accessed April 2023].
- [51] "XXSer (Cross Site "Scripter")," [Online]. Available: <https://xssec.03c8.net/>. [Accessed April 2023].
- [52] OWASP Foundation, "Vulnerability Scanning Tools," [Online]. Available: https://owasp.org/www-community/Vulnerability_Scanning_Tools. [Accessed April 2023].
- [53] A. Mudgerikar, P. Sharma and E. Bertino, "Edge-Based Intrusion Detection for IoT devices," *ACM Transactions on Management Information Systems*, vol. 11, no.4, 2020.
- [54] C. Livadas, R. Walsh, D. Lapsley and W. Strayer, "Using Machine Learning Techniques to Identify Botnet Traffic," in *31st IEEE Conference on Local Computer Networks*, 2006.
- [55] T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection," *Information Sciences*, vol. 177, no. 18, pp. 3799-3821, 2007.
- [56] C. Schneider, A. Barker and S. Dobson, "A survey of self-healing systems frameworks," *Software: Practice and Experience*, pp. 1375-1398, 2014.
- [57] Cisco Systems, "Snort," [Online]. Available: <https://www.snort.org/>. [Accessed April 2023].
- [58] The Open Information Security Foundation, "Suricata," [Online]. Available: <https://suricata.io/>. [Accessed April 2023].
- [59] The Zeek Project, "Zeek," [Online]. Available: <https://zeek.org/>. [Accessed April 2023].
- [60] Ossec Project Team, "Ossec," [Online]. Available: <https://www.ossec.net/>. [Accessed April 2023].
- [61] Google LLC, "VirusTotal," [Online]. Available: <https://www.virustotal.com/>. [Accessed April 2023].
- [62] "Wikipedia - Question answering," [Online]. Available: https://en.wikipedia.org/wiki/Question_answering. [Accessed April 2023].
- [63] "Dida.do blog - BERT for question answering part 2 (BERT-SQuAD)," [Online]. Available: <https://dida.do/blog/bert-for-question-answering-part-2>. [Accessed April 2023].
- [64] "Github - Bert-SQuAD," [Online]. Available: <https://github.com/kamalkraj/BERT-SQuAD>. [Accessed April 2023].
- [65] "Huggingface - BERT base cased squad2," [Online]. Available: <https://huggingface.co/deepset/bert-base-cased-squad2>. [Accessed April 2023].
- [66] "Wikipedia - BERT (language model)," October 2021. [Online]. Available: [https://en.wikipedia.org/wiki/BERT_\(language_model\)](https://en.wikipedia.org/wiki/BERT_(language_model)). [Accessed April 2023].

9 Appendix A: Current state of practice of Tools and Techniques in Management of Evidence

9.1 Assessment of security performance configuration of cloud workloads

Cloud environments are fast-changing and can become vulnerable to attacks if not configured correctly. These configuration changes may be hard to detect and include manual configuration changes as well as configuration changes based on upgrades. According to a study [37] about the top threats to cloud computing by the Cloud Security Alliance (CSA) from 2020, two of the top threats to cloud services are misconfiguration and inadequate change control (Top 2) as well as insecure interfaces and APIs (Top 7).

Cloud configuration checking tools can be used to detect these misconfigurations. According to a further study of the CSA from 2021 regarding the state of cloud security both Cloud Provider tools and third-party tools for configuration checking are used about equally often [38]. Furthermore, the study also states that the dominant public cloud platforms in the market are Microsoft Azure, Amazon Web Services and Google Cloud Platform.

Various approaches, architectures, and implementation for cloud security monitoring have been proposed in the last decade. For example, GMonE [39] was one of the first general-purpose cloud monitoring systems. A more recent approach has been proposed by Torkura et al. [40]. They combine cloud monitoring with state transition analysis to build a continuous threat assessment tool for multi-cloud systems. Similar to *Cloudditor* [9], this tool, called CSBAuditor [41], uses Cloud APIs to discover existing resources. The results are then compared to the resources' expected states, i.e., via state transition analysis. It also further analyses the results using a dedicated risk analysis component. In comparison to *Cloudditor*, however, it does not implement an ontology-based discovery. While this approach is a compact concept and implementation of a multi-cloud auditing tool, MEDINA rather aims at building a modular framework that automates parts of the certification process, e.g., of the EUCS. Since CSBAuditor implements some of the features that are needed in the MEDINA framework, e.g., cloud resource discovery, it could in parts be adapted to fit the MEDINA design requirements (e.g., APIs).

9.1.1 Cloud-Native Configuration Monitoring

Azure Security Center and Azure Policies

The cloud computing service of Microsoft Azure provides the *Azure Security Center*¹⁹ allowing to monitor various resources deployed within the cloud. One way to improve the monitoring is to use *Azure Policy*²⁰ which is a service that lets users create policies. Using these policies helps to comply with the imposed regulations of the company. They can be used to deny the deployment of resources beforehand or give alerts (e.g., in the *Azure Security Center*) about the current state of the deployed resources. There is the option to use pre-built policies or to produce customized policies depending on the specific needs of the respective user.

Although the *Security Center* accompanied with *Azure Policies* provides a good and visualized presentation of the current state of the cloud environment, there are two downsides using this

¹⁹ <https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction>

²⁰ <https://docs.microsoft.com/en-us/azure/governance/policy/overview>

approach. First, the capabilities to monitor resources depend on the expressiveness and scope of the *Azure Policy* language. The main limitation of using Azure’s monitoring services, however, is to be tied to Azure. A multi-cloud monitoring approach is not possible using Azure’s service exclusively.

By exploiting the respective CSP APIs, *Clouditor* leverages the maximum potential to access information about cloud resources and the ability to monitor multiple cloud services simultaneously – based on the ontology used in MEDINA.

AWS Config, Security Hub

Similar to Azure, Amazon Web Services (AWS) provides its own services for monitoring AWS’ resources as well. Two options for checking the state of deployed resources are *AWS Config*²¹ and the *AWS Security Hub*²². The same limitations as for *Azure* arise here: being tied to expressiveness of these services and limited to resources of AWS. In addition, the service *AWS Config* cannot be used for free.

As accessing the CSP via its offered APIs is free of charge and the *Clouditor* is offered as an open-source tool under the Apache 2.0 license, the *Clouditor* can be freely used, modified, and distributed under the terms of the license. In addition, the advantages of using *Clouditor* for *Azure* apply.

9.1.2 Commercial tools

There are also commercial tools for monitoring the configurations of one or more cloud computing services. One example is Prisma Cloud [42], a multi-cloud solution for continuous monitoring of cloud configurations. However, such tools are mostly costly and not open source. Since they are not open source, they lack flexibility in use and therefore cannot be easily integrated into a framework like MEDINA.

Secureframe²³ is a commercial offering that promises continuous compliance with various standards, including ISO 27001 and GDPR (but not the EU CS). It also offers integration to several cloud platforms, such as AWS and Google Cloud. It is, however, unclear to which extent Secureframe automatically covers the standards’ requirements and how its architecture is designed.

9.1.3 Standardized template export

Another way to discover resource configurations is to leverage the APIs for exporting an IaC (Infrastructure-as-Code) template. It allows to retrieve templates for resources deployed in the cloud service. Such a template provides a comprehensive view about the configuration of the respective cloud resource. In addition to the more holistic discovering provided with the general APIs of the respective cloud service providers, we foresee to implement the discovery via these IaC APIs as well, to obtain a quick overview of the cloud resources’ configuration. The export is possible in both Azure and AWS.

Another approach that aims at standardizing evidence gathering from cloud workloads has been proposed by Knoblauch and Banse [43]. They propose a standardized audit API that can be queried by the evidence gathering tool in any system, but which moves the implementation effort to the cloud provider and/or the cloud service provider: either the API responses have to be

²¹ <https://aws.amazon.com/es/config/>

²² https://aws.amazon.com/security-hub/?nc1=h_ls

²³ <https://secureframe.com/>

implemented by the service provider or the cloud provider needs to adopt them. This proposal is therefore better suited in customized systems rather than standard cloud systems.

9.2 Security assessment of computing infrastructure

This section describes the state of the art of tools used for assessing the security of infrastructural elements such as (virtual) machines and networks. Two types of tools are presented: tools for proactively detecting vulnerabilities (vulnerability assessment) and tools for reactively detecting breaches (intrusion detection). In the scope of MEDINA, these tools are used to obtain evidence about fulfilment of specific requirements by monitoring the state of infrastructure's security, or offered to be used by CSPs to satisfy certain requirements and communicate the fulfilment of these requirements to MEDINA.

9.2.1 Vulnerability assessment

Vulnerability assessment comprises identifying, quantifying, and ranking potential vulnerabilities in computer systems, networks, and applications, and is a critical component of vulnerability and risk management in any company. Vulnerability scanners are automated tools that can aid in the process of identifying vulnerabilities, by checking for security weaknesses or abnormalities in the networks, systems, or applications. Based on the scope of their scanning targets, they are classified as network-based, host-based, wireless, application, and database scanners [44], where a single tool with multiple capabilities (e.g. Nmap [14]) can fall into more than one category. Application vulnerability scanners are further divided into two groups depending on their testing method. Dynamic application security testing (DAST) tools test software in its operational state by using the provided interfaces of running programs to insert specially crafted test inputs, intended to verify the correctness of the program's responses and find error patterns that could indicate security vulnerabilities. DAST scanners do not require application's source code or other data about the software internal operation (black-box testing). On the other hand, static application security testing (SAST) scanners analyse the software's source code and do not require the tested application to be in a running state.

Among the most used DAST tools are web application vulnerability scanners that scan websites for vulnerabilities such as cross-site scripting (XSS), SQL injection, path traversal, and various insecure server configuration errors. Examples of such tools include AppSpider [45], Burp Suite [46], Nessus [47], Qualys [48] (offered as a service), and open-source tools: OpenVAS [49], Arachni [50], OWASP ZAP [13], and w3af [12]. Beside the general web application scanners, other DAST tools focus on specific vulnerabilities: sqlmap [51] (detecting SQL vulnerabilities) and XXSer [52] (cross-site scripting). DAST scanning tools can be used manually in penetration testing or in an automated way, where the results are later examined by an expert. A comprehensive list of DAST scanners is provided by OWASP [53].

Vulnerability Assessment Tools included in MEDINA (described in section 3.3) combine multiple open-source DAST scanners in a scanning automation framework in order to extend the scope of scanning and enable scheduling of automated scans, alerting, and basic vulnerability management.

9.2.2 Intrusion detection

Intrusion Detection Systems (IDSs) are software applications that can detect and analyse active attacks or threats in the monitored infrastructure. Depending on the scope of monitoring, IDSs can monitor a single machine, its configurations, files, and applications (host-based IDS, HIDS), or analyse traffic on a network to detect anomalous activity or attacks (network-based IDS, NIDS). Based on the detection technique used, IDSs are grouped into signature-based and anomaly-based. Signature-based IDSs use databases of known attacks or malware patterns and

simply look for matches in files or traffic they monitor. Anomaly-based IDSs on the other hand use models, built by monitoring the normal system operation and identify anomalies based on deviations from the normal operation. These are more sophisticated and normally use machine learning methods to train their models and classify application logs, behavioural features, files, or network streams into either normal or potentially harmful (malicious). Because host-based IDSs rely on detecting anomalous behaviour, they can also detect new types of threats, while signature-based IDSs are typically more accurate at detecting known threats, but are incapable of detecting previously unseen malware or new types of attacks (0-days) due to their different fingerprints (patterns).

Recent research in intrusion detection methods focuses on improving the machine learning methods for anomaly based IDSs. Various system-level data is utilized to profile the normal system behaviour and detect abnormalities using supervised or unsupervised machine-learning approaches [54]. Some techniques in research focus on specific attack classification (e.g., denial-of-service attacks) [55] while others are devoted to detection of anomalous traffic without classifying the type of attacks [56].

In order to extend the effectiveness of an intrusion detection system, its detection functionality can be combined or integrated with inspectors and actuators. While the detector is capable of detecting anomalies or threats, inspector software enables review of generated alerts by experts, and actuators can (automatically) perform actions to change the system configuration in order to avoid (further) damage by the detected threat. Multi-module solutions that integrate capabilities of sensors, detectors, inspectors, and actuators exist as well, solutions with the widest capabilities are typically Security Information and Event Management systems (SIEMs) [57].

Two examples of popular IDS tools are Snort [58] and Suricata [59], both signature-based network IDSs. Suricata, the more modern of the pair, supports hardware-accelerated high-bandwidth network captures and decoding of application layer data. Zeek [60] (previously known as Bro-IDS) is a network IDS with prevention capabilities that beside pattern-matching also offers some anomaly detection functionalities with the help of its powerful scripting language. Concerning host-based IDSs, one of the most popular open-source tools is OSSEC [61]. It runs on all major operating systems and consists of a server – agent architecture, where agents (lightweight components installed on monitored hosts) deliver information about detected events to the server that manages the agents. Detection capabilities of OSSEC include file integrity monitoring, collection and analysis of application and system logs, rootkit detection, as well as integration with anti-malware software and APIs (e.g., VirusTotal [62]). *Wazuh*, also used in MEDINA, is another open-source HIDS that is based on OSSEC, but includes additional functionalities, especially regarding possible integrations with other software. *Wazuh* is integrated with the ELK stack (storing logs and events into an Elasticsearch [29] database and providing a user-facing UI through Kibana [30]), includes a restful API for management, as well as improved detection capabilities with added rulesets. Detection rulesets also include basic evaluation of compliance with some controls of specific regulations or standards like GDPR and PCI DSS. *Wazuh* can also retrieve certain data about cloud infrastructure through integrations with Amazon AWS and Microsoft Azure clouds.

9.3 Information of data flows in cloud applications

The security and compliance of cloud applications depend on the secure configuration of interfaces for data exchange and processing of information. Thereby, the full software and application stack must be examined. The security of a cloud application depends equally on the security of interactions between components as well as vulnerability free implementations in

software. For each granularity, tools are available that support developers and cloud application designers in developing secure applications.

On the highest level, a cloud application consists of a set of services that in its entirety provides the functionality of a cloud application. As a complex system composed of multiple components the secure configuration of each component must be ensured. Tools like Terrascan²⁴, Chef InSpec²⁵, Snyk²⁶ or Anchore²⁷ can identify security problems in Infrastructure as Code specifications. These includes misconfigurations or violations against best practices that increase the chance of having vulnerable cloud applications. Part of these checks are based on descriptions how a secure configuration should look like. These in turn are mapped in some cases onto policies. As a result, they can validate compliance to standards like HIPAA, PCI DSS, NIST and CIS benchmarks.

A second class of tool can check if used components are up to date and free of vulnerability. This class of tools often provides some form of container or VM scanner. It checks if used programs and libraries in a container/VM contain outdated software or software with vulnerabilities. Tools like these are, for example, Grype²⁸, Clair²⁹ and Trivy³⁰.

Finally, source code of developed software that is deployed as a component of a cloud application must be developed using secure coding practices. Part of these practices is the use of static security application testing tools. These tools are often included in CI/CD pipelines and scan source code for vulnerable software patterns. Well known tools include products from SonarSource like SonarQube³¹, Flawfinder³², Semgrep³³ or CodeQL³⁴ by GitHub. They often contain rules that identify when certain software patterns represent vulnerabilities or violate best coding practices. They may also include softer rules from software engineering that try to reduce the complexity of source code and enforce documentation. These tools help developers to identify problems in their code and fix them before the code is deployed as a production application.

Codyze belongs to this last class of tools. It scans code and identifies potential pitfalls in the use of software libraries that cause vulnerabilities. However, where most of the previous tools stop the analysis, *Codyze* tries to map low-level code properties to high-level security requirements from control frameworks like ENISA EUCS [35]. Thus, *Codyze* tries to conclude that the presence of some software properties and absence of vulnerability qualifies a software to comply with control frameworks like ENISA EUCS.

²⁴ <https://www accurics.com/developers/terrascan/>

²⁵ <https://community.chef.io/tools/chef-inspec>

²⁶ <https://snyk.io/>

²⁷ <https://anchore.com/>

²⁸ <https://github.com/anchore/grype>

²⁹ <https://github.com/quay/clair>

³⁰ <https://github.com/aquasecurity/trivy>

³¹ <https://www.sonarqube.org/>

³² <https://dwheeler.com/flawfinder/>

³³ <https://semgrep.dev/>

³⁴ <https://codeql.github.com/>

10 Appendix B: Assessment of Organizational Measures using NLP

Audits, even those carried out at regular intervals, require many hours of time to find a wide variety of evidence documents. According to the knowledge of MEDINA partners, this is particularly noticeable in the area of organisational requirements. These are various types of evidence documents that have to be found by CSPs. This evidence can consist of screenshots, pictures, log files, configurations, or others. Thus, an extensive manual analysis is currently necessary. Because of the wide variety of different problems, there exists almost no automation as far as MEDINA partners know. Moreover, it is difficult to automate the analysis due to the large variety of evidence types.

To fulfil MEDINA's goal of the assessment of organisational measures, the AMOE tool will be used to extract evidence based on metrics from certain documents linked to the organisational measures and process them in a pipeline to prepare them for assessment. The evidence information is to be retrieved from a wide variety of document types. This can be done by separating certain types of documents and then processing them accordingly, for example through natural language processing (NLP) for natural language-based text documents, or through differential analysis, which uses a golden standard, for other documents.

A possible method to extract evidence or check for compliance is to compare a document to a previous state or predefined template. The difference analysis depends again on the type of input. Images could be compared by analysing the difference of pixels or apply optical character recognition and compare the text. Alternatively, the bits of the documents could be compared directly, as for the other methods as well, so the result highly depends on the goal of the assessment. For textual documents, sentence-level differential analysis could be applied (including manual checking of highlighted differences), word embeddings and semantic similarities could also be utilized. The following sections provide more details to possible approaches for evidence management.

10.1 Document types and methods

The process involves a wide variety of document types. Such documents can be images, .xlsx, .docx, .md, .txt or even .pdf files. This makes a standardised methodology for the extraction of evidence correspondingly difficult. Different document forms can also occur within these file formats. For example, a Word document can contain tabular text as well as full text. This makes this task even more complex as this structure and context is lost when only the text is considered. Therefore, in order to find a way to extract the evidence, the files must first be divided into categories that can be handled in different ways. Furthermore, document sections need to be handled separately if the structure varies (e.g., text, table, figure, diagrams...).

A selection of requirements from the EUCS marked as organisational within the MEDINA project, can be used as a basis for this task's experiments. For this, it is necessary to create metrics and map them to these organisational requirements. These metrics can be used to design specific queries to extract the audit-relevant information from evidence documents. Some metrics might need specific input from the CSP to make the query complete, which could allow to transform an organisational measure to a technical, assessable measure.

10.1.1 Dataset

Building a dataset to fulfil all requirements of a security scheme is difficult, as every CSP and every service can produce different types of accepted (=compliant) evidence. At the moment of writing this document, this data set is not yet available. Therefore, one of the main first steps of this task is to gather all evidence documents that could be relevant for successfully reaching the compliance status to a security scheme. To get a generic dataset, the documents should reflect

the real-world evidence of CSPs. In a joint effort, exemplary documents and the evidence could be provided by Bosch, Fabasoft and Nixu.

10.1.2 Natural language text documents

Text-based evidence will often be provided in the form of .docx documents or .pdf documents containing human-readable text. Here, however, it is often difficult to obtain the required information with classical information extraction and is usually connected with manual searching for the corresponding sentence passages, automated, predefined queries, and queries with a predefined structure. For this reason, it is necessary to try NLP approaches to solve this problem. One such NLP option is a *question answering* [63] system.

A question-answering system is an intelligent system that can answer questions asked on the basis of a natural language text document. There are question-answering systems for the extraction of word phrases (e.g.: BERT-SQUAD [64] [65]) as well as for the prediction of yes/no questions. This system can be tested on the official BERT-SQUAD site of huggingface [66]. Such a system is built, for example, on top of a neural network like Bert [67]. Bert is a neural network that can understand human-readable documents by pre-training large amounts of data. This network was retrained with questions and answers in order to be able to answer questions from a given document.

A question answering system can be used, for example, to investigate the current approach for monitoring the security of office buildings. For this, we need to query the document containing the information that includes how the floors are currently secured. The result would be a corresponding extracted text phrase from the given document. This extraction includes a certain degree of confidence. If the confidence is high enough, the result can be compared with a list of possible results. If the result is present in the list, the metric is fulfilled.

The disadvantage of such a system is that it always tries to find a corresponding answer to a question. For example, to the question: "Where is the Eiffel Tower located?" it would also try to find the most likely answer. If the following input text is used: "Fabasoft has its headquarters in Linz", the network will probably give Linz as the answer.

As it can be seen from this example, the correctness of a neural network cannot be guaranteed. Also, model answers to yes/no questions might not be accurate enough, so further research has to be considered here to determine whether such systems provide high quality output usable for this task. However, the model provides a confidence level, which can be considered before using the output for assessment. The extracted evidence with the respective confidence is passed on to Clouditor for further processing and assessment. Thus, it can be decided there whether a manual check is necessary, or the confidence is sufficient. In this case, the result of the network can be used to speed up the manual testing process.

10.2 Information extraction from log files

Classical information extraction methods can be used to query for information from log files. Depending on the structure of the log file this can be done using regular expressions (RegEx) or XPath queries or extraction from JSON files. As this is straight forward process, we do not intend to use NLP methods for this type of documents.

10.3 Difference analysis

One way of checking documents can also be a simple difference comparison. Here, it is necessary that an existing checked and already audited document is available. This checked document can now be compared with a more recent version. If there is no change, or only an irrelevant change,

this document does not have to be further approved. Furthermore, the manual review of documents can be facilitated with the help of a difference analysis.

However, in order to be able to carry out such a difference analysis, a distinction must again be made between document types. Furthermore, thresholds have to be researched that determine whether the change is irrelevant and how manual reviews can influence the assessment.

10.3.1 Difference analysis on images

A simple approach here would be to compare the image to predefined (e.g., accepted in a previous audit) evidence image. The difference on pixel level can be calculated. If the difference is 0, the second image is identical to the first and does not have to be checked manually.

However, if a change has been made, a manual check must now be carried out. To simplify this check, the difference analysis can be used to display the change more easily. This can be found by subtracting the first image from the second image. The difference can then be presented to the user as additional information or be highlighted in the original images.

The described approaches will be probably too simple, as different ratios, contrast etc. of images are not considered. Hence, further research should be conducted. However, we do not expect to have a large quantity of evidence images (despite some screenshots). Screenshots or other images could be checked in other ways, as the source document will be some form of a text document, or the image can be OCRed (OCR: Optical Character Recognition) and then treated as such.

10.3.2 Difference analysis on textual documents

If the text content is identical to a document that has already been checked, the document to be compared is automatically compliant. However, if this is not the case, a sentence-level differential analysis could be performed to facilitate a manual review. This will highlight new sentences.

10.3.3 Bytewise Comparison

To compare two generic files, one can resort to a bytewise comparison. Before comparing the two files, the header must not be considered, as this information is usually changed when the file is saved. A bytewise comparison can now be carried out on the remaining data. The difference analysis for manual difference inspection (by human) only makes limited sense, as the difference cannot always be displayed visually in a meaningful way. As this would be a rather low-level approach, we do not expect to provide much to a working prototype, still it is considered here for completeness.

10.3.4 Difference analysis using document features

For this purpose, it is necessary to extract features from these already audited documents that allow similarity comparisons on the document corpus. In order to compare text, it is necessary that an algorithm can remotely “understand” the text. For this, a vectorisation of the text is necessary. Word embeddings or sentence embeddings can be used. Such embeddings can also be generated by neural networks. Semantic similarities are also considered here.

One of the easiest ways to compare images is to use the pixel values as a feature vector. However, it is important to note that the pixels must be contained in the exact same points on the image (resolution, contrast, etc.).

With the extracted features it is now possible to calculate similarity metrics. For example, cosine similarity can be used for this purpose. Cosine Similarity outputs a score between 0 and 1. If the

result is 1 both documents are very likely identical. Closer to 0 means that both documents are not very similar.

A limitation can be seen, for example, if a sentence in a bigger original document is changed just slightly. For example: "The floor is alarmed" to "The floor is not alarmed". Semantically, there is a big difference, but the similarity score only changes slightly. To address this problem, one can combine the similarity score with querying.

11 Appendix C: MEDINA Evidence Trustworthiness Management System API description

The Blockchain client deployed on the MEDINA *Orchestrator* exposes the following API:

11.1 Blockchain account Management

- <https://medina.bclab.dev/client/account>
 - Description: Create a new Blockchain account.
 - Method: POST.
 - Parameters: None.
 - Responses: 200 (OK), 403 (Application error).
 - Output (example):

```
{
  "ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72"825",
  "pr"va"eKey": "0x4a2ac221aef1a96c7dc13b2e5f552fc55939054a451e2e25131d079b"885b81a"
}
```

- <https://medina.bclab.dev/client/account?privatekey=0x4a2ac221aef1a96c7dc13b2e5f552fc55939054a451e2e25131d079b885b81a>
 - Description: Get address associated to a private key.
 - Method: GET.
 - Parameters: privatekey.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error).
 - Output (example):

```
{
  "ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72"825",
  "pr"va"eKey": "0x4a2ac221aef1a96c7dc13b2e5f552fc55939054a451e2e25131d079b"885b81a"
}
```

- <https://medina.bclab.dev/client/wallet?privatekey=0x4a2ac221aef1a96c7dc13b2e5f552fc55939054a451e2e25131d079b885b81a>
 - Description: Add account to wallet.
 - Method: POST.
 - Parameters: privatekey.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "walle"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"
}
```

- <https://medina.bclab.dev/client/wallet>
 - Description: Get account added to the wallet.
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 403 (Application error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "walle"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"
}
```

- <https://medina.bclab.dev/client/registration>
 - Description: Authorization request.
 - Method: POST.
 - Parameters: address.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error).
 - Output (example):

```
{
```

```
"s"at"s": "OK",  
"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"  
}
```

11.2 Blockchain transactions generation: General system management

- <https://medina.bclab.dev/client/admin?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>
 - Description: Add a new administrator.
 - Method: POST.
 - Parameters: address.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
 - Output (example):

```
{  
  "s"at"s": "OK",  
  "walle"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"  
}
```

- <https://medina.bclab.dev/client/admin?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>
 - Description: Remove an existing administrator.
 - Method: DEL.
 - Parameters: address.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
 - Output (example):

```
{  
  "s"at"s": "OK",  
  "walle"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"  
}
```

- <https://medina.bclab.dev/client/admin?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>
 - Description: Check if an id is administrator.
 - Method: GET.
 - Parameters: address.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
 - Output (example):

```
{  
  "s"at"s": "OK",  
  "is"dmin": "true"  
}
```

- <https://medina.bclab.dev/client/authorizedowner?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>
 - Description: Authorize an owner to use the *MEDINA Evidence Trustworthiness Management System*.
 - Method: POST.
 - Parameters: address.
 - Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
 - Output (example):

```
{  
  "s"at"s": "OK",  
  "authorizedowne"ad"ress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"  
}
```

- <https://medina.bclab.dev/client/authorizedowner?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>

- Description: Deauthorize an owner to use the *MEDINA Evidence Trustworthiness Management System*.
- Parameters: address.
- Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "authorizedowneraddress": "0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825"
}
```

- <https://medina.bclab.dev/client/authorizedowner?address=0x45a224EF8e9f8350eaf0fE123CbAb5ae3a72c825>

- Description: Check if an id is an authorized owner.
- Method: GET.
- Parameters: address.
- Responses: 200 (OK), 400 (parameter error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "isauthorizedowner": "true"
}
```

- <https://medina.bclab.dev/client/adminnum>

- Description: Get the number of administrators in the system.
- Method: GET.
- Parameters: None.
- Responses: 200 (OK), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "adminnum": "3"
}
```

- <https://medina.bclab.dev/client/authorizedownersnum>

- Description: Get the number of authorized owners in the system.
- Method: GET.
- Parameters: None.
- Responses: 200 (OK), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "authorizedownersnum": "4"
}
```

- <https://medina.bclab.dev/client/orchestratorsnum>

- Description: Get the number of *Orchestrators* registered in the system.
- Method: GET.
- Parameters: None.
- Responses: 200 (OK), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "orchestratorsnum": "5"
}
```

- <https://medina.bclab.dev/client/orchestrators>

- Description: Get the *Orchestrators* ids (addresses) registered in the system.
- Method: GET.
- Parameters: None.

- Responses: 200 (OK), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "s"at"s": "OK",
  "orchestratorsa"dr"sse":
  "0x55456e0Bd0E46Ec4276Eac51cfC281D39e2cd449,0xF2c6cF607dCbF1Bf4E885ae6099eC7cF1Cc0ac51,0
  x2B09939744d8c8Be9e23d05C1D04552F203B06D3,0xA3929a5dC7B0DAdB25004443F77bd9C47b56F4A4,0x0
  dE4b77C6683Bd29fAa3fa8FCDdCEf1b"F3aef8b"
}
```

11.3 Blockchain transactions generation: Orchestrator's functionalities

- <https://medina.bclab.dev/client/orchestrator>
 - Description: Register an *Orchestrator* in the trustworthy management system.
 - Method: POST.
 - Parameters: None.
 - Responses: 200 (OK), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK",
}
```

- <https://medina.bclab.dev/client/orchestrator/id>
 - Description: Get the *Orchestrator* id (address).
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK", "id": "0x0dE4b77C6683Bd29fAa3fa8FCDdCEf1b"F3aef8b"
}
```

- <https://medina.bclab.dev/client/orchestrator/owner>
 - Description: Get the *Orchestrator* owner.
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK", "owner": "0x45a224EF8e9f8350eaf0fE123CbAb5ae"a72c825"
}
```

- <https://medina.bclab.dev/client/orchestrator/creationtime>
 - Description: Get the *Orchestrator* creation time.
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "crea"io"Time": "16335876551"1352261"
}
```

- <https://medina.bclab.dev/client/orchestrator/evidence?id=1&hash=0x7465737400&tool=1&resource=2&csp=3>

- Description: Record a new evidence from the *Orchestrator*.
- Method: POST.
- Parameters: id, hash, tool, resource and csp.
- Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "evidenceId": "1",
  "evidenceHash": "0x7465737400000000000000000000000000000000000000000000000000000000",
  "evidenceTool": "1",
  "evidenceResource": "2",
  "evidenceCsp": "3"
}
```

- <https://medina.bclab.dev/client/orchestrator/evidence/{id}>

- Description: Get the evidence information of the provided evidence id.
- Method: GET.
- Parameters: None.
- Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "evidence": "1,0x7465737400000000000000000000000000000000000000000000000000000000,1,2,3,163358709970812276"
}
```

- <https://medina.bclab.dev/client/orchestrator/evidences>

- Description: Get the evidences ids registered from the *Orchestrator*.
- Method: GET.
- Parameters: None.
- Responses: 200 (OK), 401 (registration error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "evidenceIds": "0,1"
}
```

- [https://medina.bclab.dev/client/orchestrator/assessment?id=123&hashvalue=0x7465737400&hashcompliance=0x7465737400&evidences=\[1,2\]&metric=2](https://medina.bclab.dev/client/orchestrator/assessment?id=123&hashvalue=0x7465737400&hashcompliance=0x7465737400&evidences=[1,2]&metric=2)

- Description: Record a new assessment result from the *Orchestrator*.
- Method: POST.
- Parameters: id, result hash, compliance hash, associated evidences and metric.
- Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
- Output (example):

```
{
  "status": "OK",
  "assessmentId": "123",
  "assessmentHash": "0x7465737400000000000000000000000000000000000000000000000000000000",
}
```

[illegible]

- <https://medina.bclab.dev/client/orchestrator/assessment/{id}>
 - Description: Get the assessment result information of the provided assessment result id.
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

[illegible]

- <https://medina.bciab.dev/client/orchestrator/assessments>
 - Description: Get the assessment results ids registered from the *Orchestrator*.
 - Method: GET.
 - Parameters: None.
 - Responses: 200 (OK), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "ass"ss"ents": "123,456"
}
```

- <https://medina.bclab.dev/client/orchestrator/evidence/check>
 - Description: Check the recorded hash value for a specific evidence id.
 - Method: GET.
 - Parameters: id and hash.
 - Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "correctev"nc"hash": "true"
}
```

- <https://medina.bclab.dev/client/orchestrator/assessment/checkhash>
 - Description: Check the recorded result hash value for a specific assessment id.
 - Method: GET.
 - Parameters: id and result hash.
 - Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{
  "s"at"s": "OK",
  "correctassess"en"hash": "true"
}
```

- <https://medina.bclab.dev/client/orchestrator/assessment/checkcompliance>
 - Description: Check the recorded compliance hash value for a specific assessment id.
 - Method: GET.
 - Parameters: id and compliance hash.
 - Responses: 200 (OK), 400 (parameter error), 401 (registration error), 403 (Application error), 409 (account error).
 - Output (example):

```
{  
  "status": "OK",  
  "compliancehash": "true"  
}
```


12 Appendix D: EUCS Requirements coverage per tool within the MEDINA Evidence Management Tools

This section shows the current coverage of the 34 EUCS requirements identified in Table 2 for each of the tools within the *MEDINA Evidence Management Tools*. In addition, some of the tools also cover some additional requirements to the 34 EUCS requirements identified in Table 2. Please note that the EUCS requirements referred in this deliverable correspond to a draft version of the ENISA catalogue [3] and are not intended for being used outside the context of MEDINA.

The background colour in the “Coverage” column means:

- Green** The tool covers the requirement to some extent (i.e., at least one metric has been implemented).
- Orange** There is a plan or idea to implement the requirement by the tool, but it has not yet been realised.
- Red** It is not possible to cover the requirement due to its nature.

12.1 Cloudfitor

As shown in Table 7, *Cloudfitor* covers 11/34 EUCS requirements. 23/34 requirements are not possible to cover with *Cloudfitor's Cloud Evidence Collector* because some requirements are not related to cloud resources.

Table 7. Summary of Cloudfitor's coverage of the 34 EUCS high level requirements in Table 2

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

HR-06.3H	"The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored."	Tech	
HR-06.5H	"The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored."	Tech & Org	
AM-01.4H	"The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date."	Tech	
AM-03.4H	"The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored."	Tech	
AM-04.1H	"The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored."	Tech & Org	
PS-02.8H	"The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored."	Tech & Org	
OPS-02.2H	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."	Tech	
OPS-05.3H	"The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities."	Tech	
OPS-07.2H	"In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP."	Tech	
OPS-09.2H	"When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup."	Tech	
OPS-12.1H	"The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation."	Tech	
OPS-12.2H	"The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H)."	Tech	
OPS-13.1H	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data."	Tech	
OPS-18.6H	"The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC."	Tech	

OPS-21.1H	"The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements."	Tech	
IAM-03.1H	"The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons."	Tech	
IAM-03.2H	"The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application."	Tech & Org	
IAM-03.5H	"The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application."	Tech & Org	
IAM-03.6H	"The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant."	Tech	
CCM-04.1H	"The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored."	Tech & Org	
CCM-05.1H	"The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights."	Tech & Org	
PM-04.7H	"The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling)."	Tech	
PM-04.8H	"The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action."	Tech	
IM-02.5H	"The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures."	Tech	
CO-03.5H	"Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions."	Tech & Org	
CO-03.6H	"The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported"	Tech	

	to the appropriate CSP's subject matter experts for immediate assessment and action."		
INQ-03.4H	"The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01."	Tech	
PSS-04.2H	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."	Tech	

In addition, *Clouditor* also covers or has a plan to cover additional EUCS requirements beyond the 34 identified in Table 2. These additional requirements are listed in Table 8.

Table 8. Summary of additional requirements coverage of *Clouditor*

Req.ID	Requirement	Coverage
OPS-05.1B	"The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures."	
OPS-06.1S	"The CSP shall define and implement policies and procedures according to ISP-02 for data backup and recovery, covering at least the following aspects: (1)The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the CSCs and the CSP's operational continuity requirements for recovery time objective (RTO) and recovery point objective (RPO); (2) How data is backed up in encrypted, state-of-the-art form; (3) How backup data is stored, moved, managed, and disposed of; (4) How a CSC-initiated recovery or recovery test is performed; (5) Restricted access to the backed-up data and the execution of restores only by authorised persons; and (6) Tests of recovery procedures (cf. OPS-08)."	
OPS-13.1B	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its evaluation."	
OPS-13.2S	"The communication between the assets to be logged and the logging servers shall be authenticated, encrypted using state-of-the-art encryption and, when encryption is not feasible, shall be accessible only by authorised personnel."	
OPS-13.2H	"The communication between the assets to be logged and the logging servers shall be authenticated, encrypted using state-of-the-art encryption and, when encryption is not feasible, shall be accessible only by authorised personnel."	
OPS-13.3B	"Log data shall be deleted when no longer required for the purpose for which it was collected."	
OPS-13.4S	"The CSP shall implement technically supported procedures to fulfil requirements for log data access, storage and deletion restrictions, including access only for authorized users and systems and the enforcement of data retention periods."	
IAM-01.1B	"The CSP shall define role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on the business and security requirements of the CSP, in which at least the following aspects are covered: (1) Parameters to be considered for making access control decisions; (2) Granting and modifying access rights based on the "least-privilege" principle and on the "need to-know" principle; (3) Segregation of duties between managing, approving and assigning access rights; (4) Dedicated rules for users with privileged access; (5) Requirements for the approval and documentation of the management of access rights."	
IAM-06.5S	"The CSP shall require strong authentication (for example: multi-factor authentication) for accessing the administration interfaces used by the CSP."	

IAM-06.5H	"The CSP shall require strong authentication (for example: multi-factor authentication) for accessing the administration interfaces used by the CSP and those offered to the CSCs."	
IAM-07.1B	"The CSP shall define and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects: (1) The selection of mechanisms suitable for every type of account and each level of risk; (2) The protection of credentials used by the authentication mechanism; (3) The generation and distribution of credentials for new accounts; (4) Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and (5) Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules."	
CKM-01.1S	"The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described: (1) Usage of strong cryptographic mechanisms and secure network protocols, corresponding to the state of the art; (2) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; (3) Consideration of relevant legal and regulatory obligations and requirements; (4) Risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption."	
CKM-02.1B	"The CSP shall define and implement strong cryptographic mechanisms for the transmission of CSC data over public networks, in order to protect the confidentiality, integrity and authenticity of data."	
CKM-02.1S	"The CSP shall define and implement strong cryptographic mechanisms for the transmission of CSC data over public networks, in order to protect the confidentiality, integrity and authenticity of data."	
CKM-03.1B	"The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02."	
CKM-03.3S	"The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be established in accordance with applicable legal and regulatory obligations and requirements and contractually agreed with the CSC."	

12.2 Codyze

As shown in Table 9, *Codyze* covers 7/11 and has a plan to cover 1/34 EUCS requirements identified in Table 2. 26/34 requirements are not possible to cover with *Codyze* because they do not correspond to specific implementations in source code, but example, to runtime operations (e.g., ISP-03.5H, OPS-12.1H).

Table 9. Summary of *Codyze*'s coverage of the 34 EUCS high level requirements in Table 2

ReqID	Requirement	Type	Coverage
OIS-02.4H	"The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced."	Tech	
ISP-03.5H	"The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date."	Tech	

HR-03.4H	"All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees."	Tech & Org	
HR-04.3H	"The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program."	Tech	
HR-05.2H	"The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure."	Tech	
HR-06.2H	"The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored."	Tech	
HR-06.3H	"The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored."	Tech	
HR-06.5H	"The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored."	Tech & Org	
AM-01.4H	"The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date."	Tech	
AM-03.4H	"The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored."	Tech	
AM-04.1H	"The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored."	Tech & Org	
PS-02.8H	"The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored."	Tech & Org	
OPS-02.2H	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."	Tech	
OPS-05.3H	"The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities."	Tech	

OPS-07.2H	"In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP."	Tech	
OPS-09.2H	"When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup."	Tech	
OPS-12.1H	"The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation."	Tech	
OPS-12.2H	"The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H)."	Tech	
OPS-13.1H	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data."	Tech	
OPS-18.6H	"The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC."	Tech	
OPS-21.1H	"The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements."	Tech	
IAM-03.1H	"The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons."	Tech	
IAM-03.2H	"The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application."	Tech & Org	
IAM-03.5H	"The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application."	Tech & Org	

IAM-03.6H	"The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant."	Tech	
CCM-04.1H	"The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored."	Tech & Org	
CCM-05.1H	"The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights."	Tech & Org	
PM-04.7H	"The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling)."	Tech	
PM-04.8H	"The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action."	Tech	
IM-02.5H	"The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures."	Tech	
CO-03.5H	"Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions."	Tech & Org	
CO-03.6H	"The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP's subject matter experts for immediate assessment and action."	Tech	
INQ-03.4H	"The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01."	Tech	
PSS-04.2H	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."	Tech	

12.3 VAT

As shown in Table 10, VAT covers 2/34 requirements identified in Table 2, related to vulnerability scanning and automatic reporting as well as monitoring the system components. 32/34 requirements are not possible to cover with this tool.

Table 10. Summary of VAT's coverage of the 34 EUCS high level requirements in Table 2

Req.ID	Requirement	Type	Coverage
OIS-02.4H	"The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced."	Tech	
ISP-03.5H	"The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date."	Tech	
HR-03.4H	"All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees."	Tech & Org	
HR-04.3H	"The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program."	Tech	
HR-05.2H	"The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure."	Tech	
HR-06.2H	"The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored."	Tech	
HR-06.3H	"The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored."	Tech	
HR-06.5H	"The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored."	Tech & Org	
AM-01.4H	"The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date."	Tech	
AM-03.4H	"The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored."	Tech	
AM-04.1H	"The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored."	Tech & Org	
PS-02.8H	"The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored."	Tech & Org	

OPS-02.2H	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."	Tech	
OPS-05.3H	"The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities."	Tech	
OPS-07.2H	"In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP."	Tech	
OPS-09.2H	"When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup."	Tech	
OPS-12.1H	"The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation."	Tech	
OPS-12.2H	"The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H)."	Tech	
OPS-13.1H	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data."	Tech	
OPS-18.6H	"The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC."	Tech	
OPS-21.1H	"The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements."	Tech	
IAM-03.1H	"The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons."	Tech	

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

INQ-03.4H	"The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01."	Tech	
PSS-04.2H	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."	Tech	

12.4 Wazuh

As shown in Table 11, *Wazuh* covers 1/34 requirements, related to malware protection and automatic notification about malware threats. In the deliverable D3.2 [4], *Wazuh* covered two requirements (OPS-05.3H and OPS-21.1.H), all with metrics related to malware protection and automatic notification. Upon reviewing the metrics and requirements, it was decided that these metrics better correspond to only one requirement (OPS-05.3H). Thus, in the final iteration *Wazuh* covers only one requirement (OPS-05.3H). Other requirements cannot be covered with *Wazuh*.

Table 11. Summary of Wazuh's coverage of the 34 EUCS high level requirements in Table 2

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

HR-06.5H	"The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored."	Tech & Org	
AM-01.4H	"The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date."	Tech	
AM-03.4H	"The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored."	Tech	
AM-04.1H	"The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored."	Tech & Org	
PS-02.8H	"The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored."	Tech & Org	
OPS-02.2H	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."	Tech	
OPS-05.3H	"The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities."	Tech	
OPS-07.2H	"In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP."	Tech	
OPS-09.2H	"When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup."	Tech	
OPS-12.1H	"The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation."	Tech	
OPS-12.2H	"The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H)."	Tech	
OPS-13.1H	"The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data."	Tech	

OPS-18.6H	“The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC.”	Tech	
OPS-21.1H	“The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements.”	Tech	
IAM-03.1H	“The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons.”	Tech	
IAM-03.2H	“The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application.”	Tech & Org	
IAM-03.5H	“The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application.”	Tech & Org	
IAM-03.6H	“The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant.”	Tech	
CCM-04.1H	“The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored.”	Tech & Org	
CCM-05.1H	“The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights.”	Tech & Org	

PM-04.7H	"The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling)."	Tech	
PM-04.8H	"The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action."	Tech	
IM-02.5H	"The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures."	Tech	
CO-03.5H	"Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions."	Tech & Org	
CO-03.6H	"The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP's subject matter experts for immediate assessment and action."	Tech	
INQ-03.4H	"The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01."	Tech	
PSS-04.2H	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."	Tech	

12.5 AMOE

As shown in Table 12, *AMOE* covers 20/34 EUCS requirements. Other 14/34 requirements are not possible to cover with *AMOE* as they are not organisational, nor do they imply that monitoring a respective static policy document is necessary, i.e., they are focused on automatic monitoring that requires technical implementation.

Table 12. Summary of *AMOE*'s coverage of the 34 EUCS high level requirements in Table 2

Req.ID	Requirement	Type	Coverage
OIS-02.4H	"The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced."	Tech	
ISP-03.5H	"The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date."	Tech	
HR-03.4H	"All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production envi-	Tech & Org	

	ronment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.”		
HR-04.3H	“The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program.”	Tech	
HR-05.2H	“The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure.”	Tech	
HR-06.2H	“The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored.”	Tech	
HR-06.3H	“The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored.”	Tech	
HR-06.5H	“The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored.”	Tech & Org	
AM-01.4H	“The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.”	Tech	
AM-03.4H	“The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.”	Tech	
AM-04.1H	“The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02, and this commitment shall be automatically monitored.”	Tech & Org	
PS-02.8H	“The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these areas, and this logging shall be automatically monitored.”	Tech & Org	
OPS-02.2H	“The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards.”	Tech	
OPS-05.3H	“The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.”	Tech	
OPS-07.2H	“In order to check the proper application of these measures, the CSP shall automatically monitor the execution of data backups, and make available to the CSCs a service portal for monitoring the execution of backups when the CSC uses backup services with the CSP.”	Tech	

OPS-09.2H	“When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02), and shall be automatically monitored by the CSP to verify the execution of the backup.”	Tech	
OPS-12.1H	“The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation.”	Tech	
OPS-12.2H	“The CSP shall automatically monitor that event detection processes operate as intended on appropriate assets as identified in the asset classification catalogue (cf AM-05-1H).”	Tech	
OPS-13.1H	“The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation, and shall automatically monitor the aggregation and deletion of logging and monitoring data.”	Tech	
OPS-18.6H	“The CSP shall provide and promote, where appropriate, automatic update mechanisms for the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC.”	Tech	
OPS-21.1H	“The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards, and automatically monitor these system components for conformity with hardening requirements.”	Tech	
IAM-03.1H	“The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity, as defined in the policy of AIM-02, for user accounts, and automatically monitor its application. Such user accounts are: (1) Of employees of the CSP as well as for system components involved in automated authorisation processes; and (2) Associated with identities assigned to persons, identities assigned to non-human entities and identities assigned to multiple persons.”	Tech	
IAM-03.2H	“The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts, as defined in the policy of AIM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, and automatically monitor its application.”	Tech & Org	
IAM-03.5H	“The CSP shall document and implement an automated mechanism to revoke accounts that have been blocked by another automatic mechanism after a certain period of inactivity, as defined in the policy of AIM-02 for user accounts, and automatically monitor its application.”	Tech & Org	
IAM-03.6H	“The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant.”	Tech	

CCM-04.1H	"The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment, and the approval processes shall be automatically monitored."	Tech & Org	
CCM-05.1H	"The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment, and the changes in the production environment shall be automatically monitored to enforce these roles and rights."	Tech & Org	
PM-04.7H	"The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects: (1) Configuration of system components; (2) Performance and availability of system components; (3) Response time to malfunctions and security incidents; and (4) Recovery time (time until completion of error handling)."	Tech	
PM-04.8H	"The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the CSP for prompt assessment and action."	Tech	
IM-02.5H	"The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures."	Tech	
CO-03.5H	"Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions."	Tech & Org	
CO-03.6H	"The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP's subject matter experts for immediate assessment and action."	Tech	
INQ-03.4H	"The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01."	Tech	
PSS-04.2H	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."	Tech	

In addition, AMOE also covers additional EUCS requirements beyond the 34 identified in Table 2. These additional requirements are listed in Table 13.

Table 13. Summary of additional requirements coverage of AMOE

Req.ID	Requirement	Coverage
ISP-02.1H	"The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, and document them according to a uniform structure, including at least the following aspects: (1) Objectives; (2) Scope; (3) Roles and responsibilities within the organization, including staff competence requirements and the establishment of substitution rules; (4) Roles and dependencies on other organisations (especially CSCs and subservice	

	providers); (5) Steps for the execution of the security strategy; (6) Applicable legal and regulatory requirements.”	
AM-01.1H	“The CSP shall define and implement policies and procedures for maintaining an inventory of assets, which shall be performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle.”	
OPS-04.1H	“The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects: (1) Use of system-specific protection mechanisms; (2) Operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment; and (3) Operation of protection programs for employees’ terminal equipment.”	
OPS-06.1H	“The CSP shall define and implement policies and procedures according to ISP-02 for data backup and recovery, covering at least the following aspects: (1) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the CSCs and the CSP’s operational continuity requirements for recovery time objective (RTO) and recovery point objective (RPO); (2) How data is backed up in encrypted, state-of-the-art form; (3) How backup data is stored, moved, managed, and disposed of; (4) How a CSC-initiated recovery or recovery test is performed; (5) Restricted access to the backed-up data and the execution of restores only by authorised persons; and (6) Tests of recovery procedures (cf. OPS-08).”	
OPS-07.1H	“The CSP shall document and implement technical and organizational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06.”	
OPS-08.1H	“The CSP shall test the restore procedures at least annually, embedded in the CSP’s business continuity management, including tests assessing if the specifications for the RTO and RPO agreed with the customers are met.”	
OPS-08.3H	“The CSP shall thoroughly document restore tests, including the safe disposal of restored data.”	
OPS-09.1H	“The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location, selected upon criteria of distance, recovery times and impact of disasters on backup and main sites.”	
OPS-10.1H	“The CSP shall define and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility, covering at least the following aspects: (1) Definition of events that could lead to a violation of the protection goals; (2) Specifications for activating, stopping and pausing the various logs; (3) Information regarding the purpose and retention period of the logs; (4) Definition of roles and responsibilities for setting up and monitoring logging; (5) Definition of log data that may be transferred to CSCs and technical requirements of such log forwarding; (6) Information about timestamps in event creation; (7) Time synchronisation of system components; and (8) Compliance with legal and regulatory frameworks.”	
OPS-13.3H	“Log data shall be deleted when it is no longer required for the purpose for which they were collected.”	
OPS-17.1H	“The CSP shall define and implement, in accordance with ISP-02, policies and procedures, including technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service, covering at least the following aspects: (1) Regular identification of vulnerabilities; (2) Assessment of the severity of identified vulnerabilities; (3) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined case specific timelines; and (4) Handling of	

	system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.”	
OPS-19.1H	“The CSP shall perform at least monthly tests to detect publicly known vulnerabilities on the system components used to provide the cloud service, in accordance with policies for handling vulnerabilities (cf. OPS-17).”	
IAM-01.1H	“The CSP shall define role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on role-based access control and based on the business and security requirements of the CSP, in which at least the following aspects are covered: (1) Parameters to be considered for making access control decisions; (2) Granting and modifying access rights based on the “least-privilege” principle and on the “need to-know” principle; (3) Use of a role-based mechanism for the assignment of access rights; (4) Segregation of duties between managing, approving and assigning access rights; (5) Dedicated rules for users with privileged access; (6) Requirements for the approval and documentation of the management of access rights.”	
IAM-08.1H	“The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: (1) Non-reuse of credentials; (2) Trade-offs between entropy and ability to memorize; (3) Recommendations for renewal of passwords; (4) Rules on storage of passwords. (5) Recommendations on password managers (6) Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling.”	
CKM-01.1H	“The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described: (1) Usage of strong cryptographic mechanisms and secure network protocols, corresponding to the state of the art; (2) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; (3) Consideration of relevant legal and regulatory obligations and requirements; (4) Risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption.”	
CKM-02.1H	“The CSP shall define and implement strong cryptographic mechanisms for the transmission of all data over public networks, in order to protect the confidentiality, integrity and authenticity of data.”	
CKM-02.2H	“The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including employee authentication.”	
CKM-03.1H	“The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.”	
CKM-04.1H	“Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects: (1) Generation of keys for different cryptographic systems and applications; (2) Issuing and obtaining public-key certificates; (3) Provisioning and activation of the keys; (4) Secure storage of keys including description of how authorised users get access; (5) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; (6) Handling of compromised keys; and (7) Withdrawal and deletion of keys.”	
CS-01.1H	“The CSP shall document, communicate and implement technical safeguards that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems, in accordance with ISP-02, and based on the results of a risk analysis carried out according to RM-01.”	

CS-02.1H	“The CSP shall define and implement according to ISP-02 specific security requirements to connect within its network, including at least: (1) When the security zones are to be separated and when the CSCs are to be logically or physically segregated; (2) What communication relationships and what network and application protocols are permitted in each case; (3) How the data traffic for administration and monitoring are segregated from each other at the network level; (4) What internal, cross-location communication is permitted; and (5) what cross-network communication is allowed.”	
CS-03.1H	“The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment.”	
CS-05.1H	“The CSP shall document and implement separation mechanisms at network level for the data traffic of different CSCs.”	
PI-01.2B	“The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.”	
CCM-01.1H	“The CSP shall define and implement policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02, covering at least the following aspects: (1) Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals; (2) Requirements for the performance and documentation of tests; (3) Requirements for segregation of duties during planning, testing, and release of changes; (4) Requirements for the proper information of CSCs about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; (5) Requirements for the documentation of changes in the system, operational and user documentation; and (6) Requirements for the implementation and documentation of emergency changes, which must comply with the same level of security as normal changes. (7) Requirements for the handling of a change’s unexpected effects, including corrective actions.”	
IM-01.2H	“The CSP shall establish a Cyber Security Incident Response Team (CSIRT), which contributes to the coordinated resolution of security incidents.”	
IM-02.1H	“The CSP shall classify and prioritize security events that could constitute a security incident, and perform root-cause analyses for these events, using their subject matter experts and external security providers where appropriate.”	
IM-02.4H	“The CSP shall simulate the identification, analysis, and defence of security incidents and attacks at least once a year through appropriate tests and exercises.”	
IM-04.1H	“The CSP shall inform employees and external business partners of their contractual obligations to report all security events that become known to them and are directly related to the cloud service.”	
IM-04.3H	“The CSP shall define, publish and implement a single point of contact to report security events and vulnerabilities.”	
IM-05.1H	“The CSP shall periodically inform its CSCs on the status of the security incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual agreements.”	
IM-05.2H	“As soon as a security incident has been closed, the CSP shall inform the affected CSCs about the actions taken, according to the contractual agreements.”	
IM-07.1H	“The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents, in a way that could be used as evidence in court.”	
IM-07.4H	“The CSP shall establish an integrated team of forensic/incident responder employees specifically trained on evidence preservation and chain of custody management.”	

BC-01.1B	“The CSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure business continuity and contingency management.”	
BC-02.1H	“The policies and procedures for business continuity and contingency management shall include the need to perform a business impact analysis to determine the impact of any malfunction to the cloud service or enterprise, considering at least the following aspects: (1) Possible scenarios based on a risk assessment; (2) Identification of critical products and services; (3) Identification of dependencies, including processes (including resources required), applications, business partners and third-parties; (4) Identification of threats to critical products and services; (5) Identification of effects resulting from planned and unplanned malfunctions and changes over time; (6) Determination of the maximum acceptable duration of malfunctions; (7) Identification of restoration priorities; (8) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); (9) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and (10) Estimation of the resources needed for resumption.”	
BC-03.1H	“The CSP shall document and implement a business continuity plan and contingency plans to ensure continuity of the services, taking into account information security constraints and the results of the business impact analysis, based on industry accepted standards, and covering at least the following aspects: (1) Defined purpose and scope, including relevant business processes and dependencies; (2) Accessibility and comprehensibility of the plans for persons who are to act accordingly; (3) Ownership by at least one designated person responsible for review and approval; (4) Defined communication channels, roles and responsibilities including notification of the customers; (5) Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers); (6) List of standards being used; (7) Methods for putting the plans into effect; (8) Continuous process improvement; and (9) Interfaces to Security Incident Management.”	
CO-01.1H	“The CSP shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service.”	
CO-01.4H	The CSP shall document and implement a proactive approach for receiving up-to-date legal, regulatory and contractual requirements that affect the cloud service.”	
CO-02.1H	“The CSP shall define and implement policies and procedures for planning and conducting audits, made in accordance with ISP-02 and that would not interfere with the operation of the cloud service, addressing at least the following aspects: (1) Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the audit activities; (2) Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and (3) Logging and monitoring of activities.”	
DOC-01.1H	“The CSP shall make publicly available guidelines and recommendations to assist the cloud service users with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided, covering at least the following aspects, where applicable to the cloud service: (1) Instructions for secure configuration; (2) Information sources on known vulnerabilities and update mechanisms; (3) Error handling and logging mechanisms; (4) Authentication mechanisms; (5) Roles and rights policies including combinations that result in an elevated risk; (6) Services and functions for administration of the cloud service by privileged users, and (7) Complementary User Entity Controls (CUECs).”	

DOC-02.1H	“The CSP shall provide comprehensible and transparent information on: (1) Its jurisdiction; and (2) System component locations, including its subservice providers, where CSC data , meta-data, cloud service derived data and CSC account data is processed, stored and backed up; (3) System component locations, including for its subservice providers, where any CSP data is processed, stored, and backed up; (4) The locations from which administration and supervision may be carried out on the cloud service. (5) The locations from which the CSP conducts support operations for CSCs, including the list of operations that can be carried by support teams in each location.”	
-----------	--	--

12.6 Generic Evidence Collector (GEC)

As shown in Table 14, GEC covers 17/34 EUCS requirements.

Table 14. Summary of GEC's coverage of the 34 EUCS high level requirements in Table 2

Req.ID	Requirement	Type	Coverage
OIS-02.4H	“The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.”	Tech	
ISP-03.5H	“The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.”	Tech	
HR-03.4H	“All employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment, or any functional component thereof, and the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.”	Tech & Org	
HR-04.3H	“The CSP shall ensure that all employees complete the security awareness and training program defined for them on a regular basis, and when changing target group, and shall automatically monitor the completion of the security awareness and training program.”	Tech	
HR-05.2H	“The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps; the CSP shall automatically monitor the application of this procedure.”	Tech	
HR-06.2H	“The agreements shall be accepted by external service providers and suppliers when the contract is agreed, and this acceptance shall be automatically monitored.”	Tech	
HR-06.3H	“The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, and this acceptance shall be automatically monitored.”	Tech	
HR-06.5H	“The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement, and this acceptance shall be automatically monitored.”	Tech & Org	
AM-01.4H	“The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.”	Tech	

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

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

CO-03.6H	“The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP’s subject matter experts for immediate assessment and action.”	Tech	
INQ-03.4H	“The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.”	Tech	
PSS-04.2H	“An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails.”	Tech	

13 Appendix E: Self-assessment Questionnaires for EUCS basic requirements

13.1 Organization of Information Security

Table 15. Checklist for OIS basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	OIS-01.1B	The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service.	Q1-OIS-01.1B	Does the CSP have an information security management system (ISMS) documented?	- Documented Information Security Management System (ISMS)
				Q2-OIS-01.1B	Does the information security management system cover the operational units?	- ISMS scope (operational units)
				Q3-OIS-01.1B	Does the information security management system (ISMS), cover locations?	- ISMS scope (locations)
				Q4-OIS-01.1B	Does the CSP cover processes for providing the cloud service?	- ISMS scope (processes for providing the cloud service)
		OIS-01.2B	The CSP shall provide documented information of the ISMS applied to the cloud service.	Q1-OIS-01.2B	Does the CSP provide documented information of the ISMS applied to the cloud service?	- Documented information of the ISMS applied to the cloud service
OIS-02	SEGREGATION OF DUTIES	OIS-02.1B	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the CSC, covering at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the CSP: (1) Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); (2) Development, testing and release of changes (cf. DEV-01, CCM-01); and (3) Operation of the system components.	Q1-OIS-02.1B	Does the CSP perform a risk assessment as defined in RM-01?	- Documented risk assessment

				Q2-OIS-02.1B	Does the risk assessment address the accumulation of responsibilities or tasks in roles or individuals, with respect to the provision of the cloud service?	- Documented risk assessment (information related with the accumulation of responsibilities or tasks in roles or individuals, with respect to the provision of the cloud service)
				Q3-OIS-02.1B	Does the risk assessment cover administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01)?	- Documented risk assessment (information related with the administration of rights profiles, approval and assignment of access and access authorisations) - Documented risk assessment review record
				Q4-OIS-02.1B	Does the risk assessment cover development, testing and release of changes (cf. DEV-01, CCM-01)?	- Documented risk assessment (information related with development, testing and release of changes) - Documented risk assessment review record
				Q5-OIS-02.1B	Does the risk assessment cover the operation of the system components / assets?	- Documented risk assessment (information related with operation of the system components) - Documented risk assessment review record
		OIS-02.2B	The CSP shall implement the mitigating measures defined in the risk treatment plan, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	Q1-OIS-02.2B	Does the CSP implement the mitigating measures defined in the risk treatment plan?	- Quality records derived from the implementation of the defined Risk Assessment. The records shall include at least the following information: mitigation measure applied, linked requirement id and by whom.

OIS-03	CONTACT WITH AUTHORITIES AND INTEREST GROUPS	OIS-03.1B	The CSP shall stay informed about current threats and vulnerabilities	Q1-OIS-03.1B	Does the CSP stay informed about current threats and vulnerabilities?	- Subscriptions to Industry Reports & Storm Casts - Online Threat Intelligence investigation records
OIS-04	INFORMATION SECURITY IN PROJECT MANAGEMENT	OIS-04.1B	The CSP shall include information security in the project management of all projects that may affect the service, regardless of the nature of the project.	Q1-OIS-04.1B	Does the CSP include information security in the project management of all projects that may affect the service, regardless of the nature of the project?	- Project management documentation (information related with the information security)

13.2 Information Security Policies

Table 16. Checklist for ISP basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
ISP-01	GLOBAL INFORMATION SECURITY POLICY	ISP-01.1B	The CSP shall document a global information security policy covering at least the following aspects: (1) the importance of information security, based on the requirements of CSCs in relation to information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided (2) the security objectives and the desired security level, based on the business goals and tasks of the CSP (3) the commitment of the CSP to implement the security measures required to achieve the established security objectives; (4) the most important aspects of the security strategy to achieve the security objectives	Q1-ISP-01.1B	Is there a document describing the global information security policy?	- Global information security policy document

			(5) the organisational structure for information security in the ISMS application area.			
				Q2-ISP-01.1.B	Does the policy cover the importance of information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided?	- Global information security policy document (includes the importance of information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided)
				Q3-ISP-01.1.B	Does the policy cover the security objectives and the desired assurance and security level, based on the business goals of the Cloud Service Provider?	- Global information security policy document (includes the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider)
				Q4-ISP-01.1.B	Does the policy cover the commitment of the CSP to implement the security measures required to achieve the established security objectives?	- Global information security policy document (includes the commitment of the CSP to implement the security measures required to achieve the established security objectives)
				Q5-ISP-01.1.B	Does the policy cover the most important aspects of the security strategy to achieve the security objectives set?	- Global information security policy document (includes the most important aspects of the security strategy to achieve the security objectives set)
				Q6-ISP-01.1.B	Does the policy cover the organisational structure for information security in the cloud service application area?	- Global information security policy document (includes the organisational structure for information security in the ISMS application area)

		ISP-01.2B	The CSP's top management shall approve and endorse the global information security policy.	Q1-ISP-01.2B	Does the global information security policy or the organizational structure document establish who is the top management responsible for?	- Global information security policy document (establishes who is the top management responsible for) - Organizational structure
				Q2-ISP-01.2B	Does the top management approve and endorse the global information security policy?	- Top management signature of the global information security policy document
		ISP-01.3B	The CSP shall communicate and make available the global information security policy to employees and to CSCs.	Q1-ISP-01.3B	Does the CSP communicate and make available the global information security policy to all employees and CSCs?	- Intranet - Wallchart - Specific meetings minutes - etc.
				Q2-ISP-01.3B	Does the CSP communicate and make available the global information security policy to all external employees?	- Web - email - etc.
				Q3-ISP-01.3B	Does the CSP communicate and make available the global information security policy to all cloud service customers?	- Service contract - Web - email - etc.
ISP-02	SECURITY POLICIES AND PROCEDURES	ISP-02.1B	The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, and document them according to a uniform structure, including at least the following aspects: (1) Objectives, (2) Scope, (3) Roles and responsibilities within the organization, (4) Roles and dependencies on other organisations (especially CSCs and subservice providers), (5) Steps for the execution of the security strategy, (6) Applicable legal and regulatory requirements.	Q1-ISP-02.1B	Has the CSP identified all the relevant subject matters within the scheme?	- Specific document that includes information about the relevant subject matters within the scheme - Global information security policy - etc.
				Q2-ISP-02.1B	Does the CSP derive policies and procedures from the global information security policy for all relevant subject matters?	- Policies and procedures for each subject matter

				Q3-ISP-02.1B	Does the CSP document the policies and procedures derived from the global one following a uniform structure, including at least the following aspects? • Objectives; • Scope; • Roles and responsibilities within the organization; • Roles and dependencies on other organisations (especially cloud customers and subservice organisations); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements.	- Policies and procedures template - Policies and procedures for each subject matter
		ISP-02.2B	The CSP shall communicate and make available the policies and procedures to all employees.	Q1-ISP-02.2B	Does the CSP communicate and make available the policies and procedures to all internal employees?	- Intranet - Wallchart - Specific meetings minutes - etc.
				Q2-ISP-02.2B	Does the CSP communicate and make available the policies and procedures to all external employees?	- Web - email - etc.
		ISP-02.3B	The CSP's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies.	Q1-ISP-02.3B	Has the CSP defined the authorized bodies and its composition?	- Specific document that includes information about the authorized bodies and its composition
				Q2-ISP-02.3B	Are the security policies and procedures approved by the CSP's top management or by the authorized bodies?	- Top management or authorized bodies signature of the security policies and procedures

		ISP-02.4B	The CSP's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is modified, and when major changes may affect the security of the cloud service.	Q1-ISP-02.4B	Does every subject matter have an expert identified?	<ul style="list-style-type: none"> - Global information security policy document - Organizational structure - Another specific document
				Q2-ISP-02.4B	Every policy and procedure have been reviewed by the related expert at least annually, or when the global information security policy is updated, or when major changes may affect the security of the cloud service?	<ul style="list-style-type: none"> - Policies and procedures version control and change history
		ISP-02.5B	After a modification of procedures and policies, they shall be approved before they become effective, and then communicated and made available to employees.	Q1-ISP-02.5B	After an update of procedures and policies, have they been approved before they become effective?	<ul style="list-style-type: none"> - Signature of the new procedures and policies version
				Q2-ISP-02.5B	After an update of procedures and policies, have they been communicated and made available to internal and external employees?	<ul style="list-style-type: none"> - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
ISP-03	EXCEPTIONS	ISP-03.1B	The CSP shall maintain a list of exceptions, limited in time, to the security policies and procedures, including associated controls.	Q1-ISP-03.1B	Does the CSP maintain a list of exceptions to the security policies and procedures?	<ul style="list-style-type: none"> - List of exceptions to the security policies and procedures - Records of updates of the list of exceptions
				Q2-ISP-03.1B	Does the list of exceptions include associated controls?	<ul style="list-style-type: none"> - Associated controls in the list of exceptions
				Q3-ISP-03.1B	Are the exceptions defined limited in time?	<ul style="list-style-type: none"> - Time limitation for each exception
		ISP-03.2B	The list of exceptions shall be reviewed at least annually.	Q1-ISP-03.2B	Is the list of exceptions being reviewed at least annually?	<ul style="list-style-type: none"> - List of exceptions document version control and change history - List of exceptions document review record

13.3 Risk Management

Table 17. Checklist for RM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
RM-01	RISK MANAGEMENT POLICY	RM-01.1B	The CSP shall define policies and procedures for the cloud service in accordance with ISP-02 and OIS-01.1B for the following aspects: (1) Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners (2) Analysis of the probability and impact of occurrence and determination of the level of (3) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling (4) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners (5) Retain documented information of the activities to enable consistent, valid and comparable results.	Q1-RM-01.1B	Does the CSP define the policies and procedures for Risk management?	- Risk policy document - Risk management procedures
				Q2-RM-01.1B	Does the CSP define policies and procedures cover the identification of risks associated with the loss of confidentiality within the scope of the ISMS?	- Risk policy document (it includes the identification of risks associated with the loss of confidentiality within the scope of the ISMS) - Risk management procedures (includes the identification of risks associated with the loss of confidentiality within the scope of the ISMS)
				Q3-RM-01.1B	Does the CSP define policies and procedures cover the identification	- Risk policy document (includes the identification of risks)

					of risks associated with the loss of integrity within the scope of the ISMS?	associated with the loss of integrity within the scope of the ISMS) - Risk management procedures (includes the identification of risks associated with the loss of integrity within the scope of the ISMS)
				Q4-RM-01.1B	Does the CSP define policies and procedures cover the identification of risks associated with the loss of availability of information within the scope of the ISMS?	- Risk policy document (includes the identification of risks associated with the loss of availability of information within the scope of the ISMS) - Risk management procedures (includes the identification of risks associated with the loss of availability of information within the scope of the ISMS)
				Q5-RM-01.1B	Does the CSP document policies and procedures cover the identification of risks associated with the loss of authenticity of information within the scope of the ISMS?	- Risk policy document (includes the identification of risks associated with the loss of authenticity of information within the scope of the ISMS) - Risk management procedures (includes the identification of risks associated with the loss of authenticity of information within the scope of the ISMS)
				Q6-RM-01.1B	Does the CSP document policies and procedures cover the assignation of risk owners?	- Risk policy document (includes the assignation of risk owners) - Risk management procedures (includes the assignation of risk owners)
				Q7-RM-01.1B	Does the CSP define policies and procedures cover the analysis of the probability and impact of occurrence	- Risk policy document (includes the analysis of the probability and impact of occurrence and

					and determination of the level of risk?	determination of the level of risk) - Risk management procedures (includes the analysis of the probability and impact of occurrence and determination of the level of risk)
				Q8-RM-01.1B	Does the CSP define policies and procedures cover the evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling?	- Risk policy document (includes the evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling) - Risk management procedures (includes the evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling)
				Q9-RM-01.1B	Does the CSP define policies and procedures covers the handling of risks through measures?	- Risk policy document (includes the handling of risks through measures) - Risk management procedures
				Q10-RM-01.1B	Does the handling of risks through measures, includes the approval of authorisation and acceptance of residual risks by risk owners?	- Risk policy document - Risk management procedures (includes the handling of risks through measures)
RM-02	RISK ASSESSMENT IMPLEMENTATION	RM-02.1B	The CSP shall implement the policies and procedures covering risk assessment on the entire cloud service.	Q1-RM-02.1B	Does the CSP define policies and procedures cover the documentation of the activities implemented to enable consistent, valid and comparable results?	- Risk policy document (includes the documentation of the activities implemented to enable consistent, valid and comparable results) - Risk management procedures (includes the documentation of the activities implemented to enable consistent, valid and comparable results)

		RM-02.2B	The CSP shall make the results of the risk assessment available to relevant internal parties and relevant information shall be made available to defined external parties.	Q1-RM-02.2B	Does the CSP make the results of the risk assessment available to relevant stakeholders?	<ul style="list-style-type: none"> - Risk assessment results - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
		RM-02.3B	The CSP shall review and revise the risk assessment at least annually, and after each major change that may affect the security of the cloud service.	Q1-RM-02.3B	Does the CSP review and revise the risk assessment at least annually?	<ul style="list-style-type: none"> - Top management or authorized bodies signature of the risk assessment at least annually - records of this review in logs with dates
				Q2-RM-02.3B	Does the CSP review and revise the risk assessment after each major change that may affect the security of the cloud service?	<ul style="list-style-type: none"> - List of major changes - Top management or authorized bodies signature of the risk assessment after major changes
RM-03	RISK TREATMENT IMPLEMENTATION	RM-03.1B	The CSP shall prioritize risks according to their criticality.	Q1-RM-03.1B	Does the CSP shall prioritize risks according to their criticality?	<ul style="list-style-type: none"> - List of prioritized risks according to their criticality
		RM-03.2B	The CSP shall document and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them.	Q1-RM-03.2B	Does the CSP document a risk treatment plan to treat risks according to their priority level?	<ul style="list-style-type: none"> - Risk treatment plan according to their priority level
				Q2-RM-03.2B	Does the risk treatment plan contemplate the reducing or avoiding the risks through security controls, by sharing them, or by retaining them?	<ul style="list-style-type: none"> - Risk treatment plan (contemplates the reducing or avoiding the risks through security controls, by sharing them, or by retaining them)
				Q3-RM-03.2B	Does the CSP implement the defined risk treatment plan?	<ul style="list-style-type: none"> - Evidence of actions defined in the risk treatment plan
		RM-03.3B	The risk treatment plan shall reduce the risk level to a threshold that the risk owners deem acceptable (Residual Risk).	Q1-RM-03.3B	Does the risk treatment plan reduce the risk level to a threshold that the risk owners deem acceptable (Residual Risk)?	<ul style="list-style-type: none"> - Risk threshold evolution through time.

				Q2-RM-03.3B	Is it defined what a residual risk is?	- Formal and documented definition of "Residual Risk"
		RM-03.4B	The CSP shall make the risk treatment plan available to relevant internal parties with appropriately summarised and abstracted versions made available both internally and to authorized external parties.	Q1-RM-03.4B	Does the CSP make the risk treatment plan available to relevant internal parties with appropriately summarised and abstracted versions?	- Risk treatment plan - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q2-RM-03.4B	Are abstracted versions made available both internally and to authorized external parties?	
		RM-03.5B	If the CSP shares risks with the CSC, the shared risks shall be associated to Complementary User Entity Controls (CUECs) and described in the user documentation.	Q1-RM-03.5B	If the CSP shares risks with the CSC, are the shared risks associated to Complementary User Entity Controls (CUECs)?	- List of Complementary User Entity Controls for the risks shared with the CSC - Traceability between risks shared by CSP and Complementary User Entity Controls (CUECs)
				Q2-RM-03.5B	If the CSP shares risks with the CSC, are the shared risks described in the user documentation?	- User documentation including the description of the shared risks
		RM-03.6B	The CSP shall revise the risk treatment plan every time the risk assessment is modified.	Q1-RM-03.6B	Does the CSP review the risk treatment plan every time the risk assessment is revised?	- Risk treatment plan version control and change history - Risk treatment plan review record

13.4 Human Resources

Table 18. Checklist for HR basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
HR-01	HUMAN RESOURCE POLICIES	HR-01.1B	The CSP shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the cloud service in the production environment, and all positions with access to CSC data or system components.	Q1-HR-01.1B	Are the security-sensitive positions classified according to their level of risk?	- Competence Position Document or similar - Policy document (roles section)
				Q2-HR-01.1B	Are the IT administration positions included in that classification?	- Competence Position Document or similar (includes the administration positions)
				Q3-HR-01.1B	Are the cloud service provisioning positions included in that classification?	- Competence Position Document or similar (includes the cloud service provisioning positions)
				Q4-HR-01.1B	Are all the positions with access to cloud customer data included in that classification?	- Competence Position Document or similar (includes all the positions with access to cloud customer data)
				Q5-HR-01.1B	Are all the positions with access to system components / assets included in that classification?	- Competence Position Document or similar (includes all the positions with access to system components)
		HR-01.2B	The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement by employees to act ethically in their professional duties.	Q1-HR-01.2B	- Does there exist an overarching agreement containing rules to act ethically in professionals' duties?	Overarching agreement with rules to act ethically
				Q2-HR-01.2B	- Is this overarching agreement included in the internal employees' contract or in a dedicated code of conduct or ethics?	Internal employees' contracts or dedicated Code of Conduct/Ethics document

				Q3-HR-01.2B	- Is this overarching agreement included in the external employees' contract or in a dedicated code of conduct or ethics?	Internal employees' contracts or dedicated Code of Conduct/Ethics document
		HR-01.3B	The CSP shall define and implement a policy that describes actions to take in the event of violations of policies and procedures or applicable legal and regulatory requirements, including at least the following aspects: (1) Verifying whether a violation has occurred; and (2) Consideration of the nature and severity of the violation and its impact	Q1-HR-01.3B	- Has the CSP documented a policy that describes actions to take in the event of violations of policies and procedures or applicable legal and regulatory requirements?	- Documented Policy, section dedicated to violations, instructions, applicable legal and regulatory requirements
				Q2-HR-01.3B	- Does the documented policy include at least the following aspects? • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact	- Documented Policy (includes verifying whether a violation has occurred & Consideration of the nature and severity of the violation and its impact)
				Q3-HR-01.3B	Has the CSP communicated the policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements?	- Evidence related to the policy communication: - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q4-HR-01.3B	Are there evidence that the policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements has been implemented?	-Records related to the policy implementation such as warnings and signed documents in accordance with what it is defined in the policy for the different levels of violations
		HR-01.4B	If disciplinary measures are defined in this policy, then the employees of the CSP shall be	Q1-HR-01.4B	Does the policy that describes actions to take in the event of	- HR-03 Policy document

			informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.		violations of policies and instructions or applicable legal and regulatory requirements contain disciplinary measures?	
				Q2-HR-01.4B	Have the internal employees been informed about possible disciplinary measures?	Mechanisms used to inform internal employees about disciplinary methods: - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q3-HR01.4B	Have the external employees been informed about possible disciplinary measure?	- Mechanisms used to inform external employees about disciplinary methods - email - Wallchart - Specific meetings minutes - etc.
				Q4-HR01.4	Have the use of the disciplinary measures been appropriately documented?	- Documented disciplinary measures way of use
HR-02	VERIFICATION OF QUALIFICATION AND TRUSTWORTHINESS	HR-02.1B	The CSP shall assess the competence and integrity of all its employees with access to CSC data or system components under the CSP's responsibility, or who are responsible to provide the cloud service in the production environment before commencement of employment in a position classified in objective HR-01.	Q1-HR-02.1B	Does the CSP assess the competence and integrity of all its employees with access to CSC data or system components under the CSP's responsibility, or who are responsible to provide the cloud service in the production environment before commencement of employment in a position classified in objective HR-01?	- Documented assess results

		HR-02.2B	The CSP shall assess the competence and integrity of its employees of the CSP before commencement of employment in a position with a higher risk classification than their previous position within the company.	Q1-HR-02.2B	Does the CSP assess the competence and integrity of its employees of the CSP before commencement of employment in a position with a higher risk classification than their previous position within the company?	- Documented assess results
		HR-02.3B	The extent of the assessment shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks.	Q1-HR-02.3B	Is the extent of the assessment proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks?	- Assessment compliance review record
HR-03	EMPLOYEE TERMS AND CONDITIONS	HR-03.1B	The CSP shall ensure that all employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures.	Q1-HR-03.1B	Does the CSP ensure that all employees comply with all applicable information security policies and procedures?	- Employment terms and conditions - Audit results of internal employees
		HR-03.2B	The CSP shall ensure that the employment terms for all employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	Q1-HR-03.2B	Does the employment terms for all internal employees include a non-disclosure provision?	- Non-disclosure provision document included in the employment terms and conditions for internal employees
				Q2-HR-03.2B	Does the employment terms for all external employees include a non-disclosure provision?	- Non-disclosure provision document included in the employment terms and conditions for external employees
				Q3-HR-03.2	Does the non-disclosure provision cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized?	- Non-disclosure provision document included in the employment terms and conditions

		HR-03.3B	The CSP shall give a presentation of all applicable information security policies and procedures to employees before granting them any access to CSC data, the production environment, or any functional component thereof.	Q1-HR-03.3B	Has the CSP given a presentation of all applicable information security policies and procedures to internal employees before granting them any access to customer data, the production environment, or any component thereof?	- Information security policies and procedure presentation + delivery evidence
				Q2-HR-03.3B	Has the CSP given a presentation of all applicable information security policies and procedures to external employees before granting them any access to customer data, the production environment, or any component thereof?	- Information security policies and procedure presentation + delivery evidence
HR-04	SECURITY AWARENESS AND TRAINING	HR-04.1B	The CSP shall define a security awareness and training program that covers the following aspects: (1) Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; (2) Handling CSC data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; (3) Information about the current threat situation; and (4) Correct behaviour in the event of security incidents.	Q1-HR-04.1B	Has the CSP defined a security awareness and training program?	- Documented security awareness and training program

				Q2-HR-04.1B	Does the defined security awareness and training program contain at least the following topics? • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents.	- Security awareness and training program (includes Handling system components, Handling cloud customer data, Information about the current threat situation and Correct behaviour in the event of security incidents)
		HR-04.2B	The CSP shall review their security awareness and training program based on changes to policies and procedures and the current threat situation.	Q1-HR-04.2B	Is the security awareness and training program kept updated according to the changes to policies and instructions and the current threat situation?	- Documented history of the security and awareness training program with references to policies/instructions/threat situation
		HR-04.3B	The CSP shall ensure that all employees complete the security awareness and training program defined for them.	Q1-HR-04.3B	Have all the CSP employees received the defined security awareness and training program?	- Training delivery records
HR-05	TERMINATION OR CHANGE IN EMPLOYMENT	HR-05.1B	The CSP shall communicate to employees their ongoing responsibilities relating to information security when their employment is terminated or changed.	Q1-HR-05.1B	Does the CSP communicate to employees their ongoing responsibilities relating to information security when their employment is terminated or changed?	- Employee termination/position change document

		HR-05.2B	The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed.	Q1-HR-05.2B	Have the CSP defined a specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed?	- Documented specific procedure to revoke the access rights and process appropriately the accounts and assets of employees when their employment is terminated or changed
				Q2-HR-05.2B	Is this procedure applied to internal employees?	- Evidence of the new access rights and process appropriately the accounts and assets to internal employees
				Q3-HR-05.2B	Is this procedure applied to external employees?	- Evidence of the new access rights and process appropriately the accounts and assets to external employees
HR-06	CONFIDENTIALITY AGREEMENTS	HR-06.1B	The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers.	Q1-HR-06.1B	Does the CSP have non-disclosure or confidentiality agreements to rule the relationship between internal employees and external service providers and suppliers	- Documented Non-disclosure or confidentiality agreements to rule the relationship between internal employees and external service providers and suppliers
				Q2-HR-06.1B	Does the CSP ensure the agreement between internal employees and external service providers and suppliers based on the defined non-disclosure agreement?	- Signed non-disclosure or confidentiality agreements to rule the relationship between internal employees and external service providers and suppliers

13.5 Asset management

Table 19. Checklist for AM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
AM-01	ASSET INVENTORY	AM-01.1B	The CSP shall define and implement policies and procedures for maintaining an inventory of assets.	Q1-AM-01.1B	Does the CSP define policies and procedures for maintaining an inventory of assets?	- Documented policies and procedures
				Q2-AM-01.1B	Does the CSP implement the defined policies and procedures for maintaining an inventory of assets?	- Documented Inventory of assets
		AM-01.2B	The CSP shall record for each asset the information needed to apply the risk management procedure defined in RM-01.	Q1-AM-01.2B	Does the CSP record for each asset the information needed to apply the risk management procedure defined in RM-01?	- Documented Information needed for each asset to apply risk management in the inventory of assets
AM-02	ACCEPTABLE USE AND SAFE HANDLING OF ASSETS POLICY	AM-02.1B	The CSP shall define and implement policies and procedures as defined in ISP-02 for acceptable use and safe handling of assets. When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use.	Q1-AM-02.1B	Does the CSP define policies and procedures for acceptable use and safe handling of assets?	- Policies and procedures document - Global security policies
				Q2-AM-02.1B	When removable media is used in the technical infrastructure or for IT administration tasks, is this media dedicated to a single use?	- Policies and procedures document - Global security policies
AM-03	COMMISSIONING AND DECOMMISSIONING	AM-03.1B	The CSP shall define and implement a procedure for the commissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures.	Q1-AM-03.1B	Does the CSP define a procedure for the commissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures?	- Documented Hardware commissioning procedure

				Q2-AM-03.1B	Does CSP implement a procedure for the commissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures?	- Evidence related to procedure for the commissioning of hardware implementation: - HW commissioning records / Implementation checklist or equivalent
		AM-03.2B	The CSP shall define and implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, including the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies.	Q1-AM-03.2B	Does the CSP define a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures?	- Documented Hardware decommissioning procedure
				Q2-AM-03.2B	Does CSP implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures?	- Evidence related to procedure for the decommissioning of hardware implementation: - HW decommissioning records / Implementation checklist or equivalent
				Q3-AM-03.2B	Does the decommissioning procedure include the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies?	- Decommissioning Procedure -Evidence of procedure application in real cases
AM-04	ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS	AM-04.1B	The CSP shall ensure and document that all employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02.	Q1-AM-04.1B	Does the CSP ensure that internal and external employees are committed to the established policy and procedures related to assets commissioning and decommissioning?	-Evidence of actions to ensure employees commitment
AM-05	ASSET CLASSIFICATION AND LABELLING	AM-05.1B	The CSP shall document an asset classification schema that reflects for each asset the protection needs of the categories of information it may process, store, or transmit.	Q1-AM-05.1B	For every asset included in the Asset Inventory, has the CSP documented an asset classification scheme that reflects the protection needs of the	- Asset classification scheme in the Assets Inventory or in a separate document

					information it processes, stores, or transmits?	
		AM-05.2B	When applicable, the CSP shall label all assets according to their classification in the asset classification schema.	Q1-AM-05.2B	Has the CSP labelled (when applicable) each asset according to the asset classification scheme?	<ul style="list-style-type: none"> - List of assets linked to their labels / tags and other configuration information - Photograph (or other recording means) of the labelled assets - Asset classification Scheme

13.6 Physical security

Table 20. Checklist for PS basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
PS-01	PHYSICAL SECURITY PERIMETERS	PS-01.1B	The CSP shall define security perimeters in the buildings and premises related to the cloud service provided.	Q1-PS-01.1B	Does the CSP define security perimeters in the buildings related to the cloud service provided?	<ul style="list-style-type: none"> - Building plans - Security perimeter plans - A CSP shall establish secure areas to protect valuable information and assets that only authorized people can access
				Q2-PS-01.1B	Does the CSP define security perimeters in the premises related to the cloud service provided?	<ul style="list-style-type: none"> - Building plans - Security perimeter plans, identifying which are the ones concerning the cloud service
		PS-01.2B	The CSP shall define at least two security areas, with at least one sensitive area covering sensitive activities such as the buildings and premises hosting the information system for the provision of the cloud service, and at least one public area covering at least all remaining buildings and premises.	Q1-PS-01.2B	Does the CSP define a security area covering sensitive activities such as the buildings and premises hosting the information system for the provision of the cloud service?	<ul style="list-style-type: none"> - Documented security area plan, establishing the two security areas, as per the requirement and who has access to them and per which terms

				Q2-PS-01.2B	Does the CSP define a security public area covering at least all remaining buildings and premises?	-Documented security area plan
		PS-01.3B	The CSP shall define and implement a set of security requirements for each security area in a policy and procedures according to ISP-02.	Q1-PS-01.3B	Does the CSP define a set of security requirements for each security area in a policy according to ISP-02 (Information Security Policy)?	- Documented security requirements for each security area - Documented physical policy
				Q2-PS-01.3B	Does the CSP communicate the set of security requirements?	- Evidence related to the set of security requirements communication: - Intranet - Wallchart - Specific meetings minutes - etc.
PS-02	PHYSICAL SITE ACCESS CONTROL	PS-02.1B	The CSP shall define and implement policies and procedures according to ISP-02 related to the physical access control to the security areas matching the requirements defined in PS-01 and based on the principles defined in IAM-01.	Q1-PS-02.1B	Does the CSP define policies and procedures related to the physical access control to the security areas?	- Documented policies and procedures
				Q2-PS-02.1B	Does the CSP implement policies and procedures related to the physical access control to the security areas?	- Access control systems to prevent unauthorised access (i.e., EACS, intercoms, videophones, CCTV cameras, mechanical locking devices operated by keys or codes, etc.)
		PS-02.2B	The access control policy shall require at least one authentication factor for accessing any non-public area.	Q1-PS-02.2B	Does the access control policy require at least one authentication factor for accessing any non-public area?	- Authentication factors (i.e., Fingerprint, PIN, etc.)
		PS-02.3B	The access control policy shall describe the physical access control derogations in case of emergency.	Q1-PS-02.3B	Does the access control policy describe the physical access control derogations in case of emergency?	- Documented description of the physical access control derogations in case of emergency

		PS-02.4B	The CSP shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to the corresponding areas.	Q1-PS-02.4B	Does the CSP display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to the corresponding areas?	<ul style="list-style-type: none"> - Wall chats - Specific warning signals - etc.
		PS-02.5B	The CSP shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner so that it does not compromise the information security of the cloud service.	Q1-PS-02.5B	Does the CSP protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner so that it does not compromise the information security of the cloud service?	<ul style="list-style-type: none"> - CCTV (closed circuit television) Security System. - Access control systems. Access control systems serve to restrict entry only to authorized personnel. - Motion sensors. - Fibre optic detection systems. - Ground Radar Systems. - Microwave barriers. - Electrified fences. - Microphone cable fence disturbance sensors. - etc.
PS-03	WORKING IN NON-PUBLIC AREAS	PS-03.1B	The CSP shall define and implement policies and procedures according to ISP-02 concerning work in non-public areas.	Q1-PS-03.1B	Does the CSP define policies and procedures concerning work in non-public areas?	-Documented policies and procedures
				Q2-PS-03.1B	Does the CSP implement policies and procedures concerning work in non-public areas?	-Access control systems to prevent unauthorised access (i.e., EACS, intercoms, videophones, CCTV cameras, mechanical locking devices operated by keys or codes, etc.)
PS-04	EQUIPMENT PROTECTION	PS-04.1B	The CSP shall define and implement policies and procedures according to ISP-02 concerning the protection of equipment and including at least the following aspects: (1) Protecting power and communications cabling from interception, interference or damage;	Q1-PS-04.1B	Does the CSP define policies and procedures concerning the protection of equipment including protecting power and communications cabling from interception, interference or damage?	-Documented policies and procedures

			(2) Protecting equipment during maintenance operations; (3) Protecting equipment holding CSC data during transport.			
				Q2-PS-04.1B	Does the CSP implement policies and procedures concerning the protection of equipment including protecting power and communications cabling from interception, interference or damage?	<ul style="list-style-type: none"> - Power and telecommunications lines undergrounded - Power cables isolated - Installation of reinforced ducts and locked rooms or boxes at inspection and termination points - Electromagnetic shielding for cable protection - Access controlled to cable rooms and patch panels - etc.
				Q3-PS-04.1B	Does the CSP define policies and procedures concerning the protection of equipment including protecting equipment during maintenance operations?	-Documented policies and procedures
				Q4-PS-04.1B	Does the CSP implement policies and procedures concerning the protection of equipment including protecting equipment during maintenance operations?	<ul style="list-style-type: none"> - Service interval recommendations and supplier specifications - List of authorized maintenance personnel - Records of all failures, real or suspected, as well as all preventive and corrective maintenance - Maintenance requirements required by insurance policies

				Q5-PS-04.1B	Does the CSP define policies and procedures concerning the protection of equipment including protecting equipment holding CSC data during transport.	-Documented policies and procedures
				Q6-PS-04.1B	Does the CSP implement policies and procedures concerning the protection of equipment including protecting equipment holding CSC data during transport.	- Reliable transport or courier. It can also be an approved transport or courier, in agreement with the policies and procedures (see below) - List of authorized couriers - Procedures to verify the identity of couriers; - Packaging protect specifications - Records identifying the content of the media, the protection applied, as well as reflecting the moments of transfer to custodians and reception at destination.
		PS-04.2B	The CSP shall use encryption on the removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media	Q1-PS-04.2B	Does the CSP use encryption on the removable media intended to move between security areas?	- Compliant encryption algorithms and tools (i.e., Self-Encrypting USB Drives, Media Encryption Software, File Encryption Software) - Secure password management tool
				Q2-PS-04.2B	Does the CSP shall use encryption on the backup media intended to move between security areas?	- Backup software
				Q3-PS-04.2B	Is the level of encryption according to the sensitivity of the data stored on the media?	- Encrypted logs

PS-05	PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS	PS-05.1B	The CSP shall define and implement a set of requirements related to external and environmental threats in a policy according to ISP-02, addressing the following risks in accordance with the applicable legal and contractual requirements: (1) Faults in planning; (2) Unauthorised access; (3) Force majeure, including epidemiological risks; (4) Insufficient surveillance; (5) Insufficient air-conditioning; (6) Fire and smoke; (7) Water; (8) Power failure; and (9) Air ventilation and filtration.	Q1-PS-05.1B	Does the CSP define a set of security requirements related to external and environmental threats in a policy according to Information Security Policies (SP-02)?	- Documented policy
				Q2-PS-05.1B	Does the policy address fault in planning?	- Documented Policy & security requirements encompasses (faults in planning)
				Q3-PS-05.1B	Does the policy address unauthorised access?	- Documented Policy & security requirements encompasses (unauthorised access)
				Q4-PS-05.1B	Does the policy address insufficient surveillance?	- Documented Policy & security requirements encompasses (insufficient surveillance)
				Q5-PS-05.1B	Does the policy address insufficient air-conditioning?	- Documented Policy & security requirements encompasses (what to do when there is a lack of insufficient air-conditioning - e.g., high temperature)
				Q6-PS-05.1B	Does the policy address fire and smoke?	- Documented Policy & security requirements encompasses (fire and smoke)

				Q7-PS-05.1B	Does the policy address water?	- Documented Policy & security requirements encompasses (water)
				Q8-PS-05.1B	Does the policy address power failure?	- Documented Policy & security requirements encompasses (power failure)
				Q9-PS-05.1B	Does the policy address air ventilation and filtration?	- Documented Policy & security requirements encompasses (air ventilation and filtration)

13.7 Operational security

Table 21. Checklist for OPS basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
OPS-01	CAPACITY MANAGEMENT – PLANNING	OPS-01.1B	The CSP shall define and implement procedures to plan for capacities and resources (personnel and IT resources), which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.	Q1-OPS-01.1B	Does the CSP define procedures to plan for capacities and resources (personnel and IT resources)?	- Capacity plan - Specific capacity procedures
				Q2-OPS-01.1B	Do procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload?	- Capacity plan (encompasses future capacity requirements) - Specific capacity procedures
				Q3-OPS-01.1B	Does the CSP implement procedures to plan for capacities and resources (personnel and IT resources)?	- Capacity plan audit
		OPS-01.2B	The CSP shall meet the requirements included in contractual agreements with CSCs regarding the provision of the cloud service in case of capacity bottlenecks or personnel and IT resources outages.	Q1-OPS-01.2B	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of capacity bottlenecks?	- Monitoring reports - Contractual agreements - Non-conformities to the contract (if there are non-compliances)

				Q2-OPS-01.2B	Does the CSP meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of IT resources outages?	<ul style="list-style-type: none"> - Monitoring reports - Non-conformities to the contract/SLA (if there are non-compliances) - Contractual agreements
OPS-02	CAPACITY MANAGEMENT – MONITORING	OPS-02.1B	The CSP shall document and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement.	Q1-OPS-02.1B	Does the CSP document technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	<ul style="list-style-type: none"> - Multidimensional QoS prediction methods
				Q2-OPS-02.1B	Does the CSP implement technical safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	<ul style="list-style-type: none"> - Service level agreement - SLA compliance report
				Q3-OPS-02.1B	Does the CSP define organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	<ul style="list-style-type: none"> - Multi-dimensional QoS measures
				Q4-OPS-02.1B	Does the CSP implement organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement?	<ul style="list-style-type: none"> - Service level agreement - SLA compliance report
OPS-03	CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES	OPS-03.1B	The CSP shall enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs.	Q1-OPS-03.1B	Does the CSP enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs?	<ul style="list-style-type: none"> - Contractual agreement - SLA - Privileges to use the monitoring and control tools

OPS-04	PROTECTION AGAINST MALWARE – POLICIES	OPS- 04.1B	The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects: (1) Use of system-specific protection mechanisms; (2) Operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment; and (3) Operation of protection programs for employees' terminal equipment	Q1-OPS- 04.1B	Does the CSP define policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering the use of system-specific protection mechanisms?	-Documented policies and procedures
				Q2-OPS- 04.1B	Does the CSP implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering the use of system-specific protection mechanisms?	- System-specific protection mechanisms - System-specific protection mechanism deployment report - Audit report - policies and procedures
				Q3-OPS- 04.1B	Does the CSP document policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment?	-Documented policies and procedures
				Q4-OPS- 04.1B	Does the CSP communicate policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment?	-Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.

				Q5-OPS-04.1B	Does the CSP implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment?	<ul style="list-style-type: none"> - Operating protection programs on system components under the responsibility of the CSP - Operating protection programs deployment report - Audit report
				Q6-OPS-04.1B	Does the CSP document policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering operation of protection programs for employees' terminal equipment.	- Documented policies and procedures
				Q7-OPS-04.1B	Does the CSP document, communicate and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering operation of protection programs for employees' terminal equipment.	<ul style="list-style-type: none"> - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q8-OPS-04.1B	Does the CSP implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering the operation of protection programs for employees' terminal equipment.	<ul style="list-style-type: none"> - Operation of protection programs for employees' terminal equipment - Operation of protection programs for employees' terminal equipment deployment report - Audit report
OPS-05	PROTECTION AGAINST MALWARE – IMPLEMENTATION	OPS-05.1B	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures.	Q1-OPS-05.1B	Does the CSP deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment?	- Malware protection programs deployed

				Q2-OPS-05.1B	Is the deploy of malware protection according to policies and procedures?	- Documented policies and procedures for malware protection - Malware deployment report
OPS-06	DATA BACKUP AND RECOVERY – POLICIES	OPS-06.1B	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery.	Q1-OPS-06.1B	Does the CSP define policies and procedures according to ISP-02 for data backup and recovery?	- Documented policies and procedures
				Q2-OPS-06.1B	Does the CSP implement policies and procedures according to ISP-02 for data backup and recovery?	- A filled form or screenshot identifying which information was requested to be backed up, the requester, the date of request, the date when the backup was performed, the result of the backup procedure (successful / fail) and where the backup was stored. - A general schedule of the backup to be performed, identifying which information is planned to be backed up, the requester, the dates planned for backup, and where the backup must be stored
OPS-07	DATA BACKUP AND RECOVERY – MONITORING	OPS-07.1B	The CSP shall document and implement technical and organizational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06.	Q1-OPS-07.1B	Does the CSP document technical and organizational measures to monitor the execution of data backups?	- Documented technical and organizational measures
				Q2-OPS-07.1B	Does the CSP implement technical and organizational measures to monitor the execution of data backups?	- Documented technical and organizational measures report
				Q3-OPS-07.1B	Are the technical and organizational measures to monitor the execution of data backups in accordance with	- Documented conformity report

					the policies and procedures defined in OPS- 06?	
OPS-08	DATA BACKUP AND RECOVERY – REGULAR TESTING	OPS-08.1B	The CSP shall test the restore procedures at least annually.	Q1-OPS-08.1B	Does the CSP test the restore procedures at least annually?	- A filled form or screenshot identifying which information was requested to be restored, the requester, the date of request, the date when the restore was performed, and the result of the restore procedure (successful / fail)
		OPS-08.2B	The CSP shall not use CSC data, but only data in test accounts controlled by CSP staff for testing purposes.	Q1-OPS-08.1B	Does the CSP use CSC data, except for data in test accounts controlled by CSP staff for testing purposes? --> NO	- Contractual agreements
OPS-09	DATA BACKUP AND RECOVERY – STORAGE	OPS-09.1B	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location.	Q1-OPS-09.1B	Does the CSP transfer backup data to a remote location or transport them on backup media to a remote location?	- Data transport report
		OPS-09.2B	When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM-02).	Q1-OPS-09.2B	When the backup data is transmitted to a remote location via a network, do the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art (cf. CKM- 02)?	- Data transport report (encompasses an encrypted form that corresponds to the state-of-the-art (cf. CKM- 02))
OPS-10	LOGGING AND MONITORING – POLICIES	OPS-10.1B	The CSP shall define and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility.	Q1-OPS-10.1B	Does the CSP define policies and procedures according to ISP-02 that govern the logging of events on system components under its responsibility?	- Documented policies and procedures
				Q2-OPS-10.1B	Does the CSP implement policies and procedures according to ISP-02 that govern the logging of events on system components under its responsibility?	- Documented Reports - Logs

OPS-11	LOGGING AND MONITORING – DERIVED DATA MANAGEMENT	OPS-11.1B	The CSP shall define and implement policies and procedures according to ISP-02 that govern the secure handling of cloud service derived data.	Q1-OPS-11.1B	Does the CSP define policies and procedures according to ISP-02 that govern the secure handling of derived data?	- Documented policies and procedures
				Q2-OPS-11.1B	Does the CSP implement policies and procedures according to ISP-02 that govern the secure handling of derived data?	- Records derived from the implementation of the policies and procedures covering the governance of the secure handling of derived data - Logs
OPS-12	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	OPS-12.1B	The CSP shall monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements, and the identified events shall be reported to the appropriate departments for timely assessment and remediation.	Q1-OPS-12.1B	Does the CSP monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements?	- Documented monitoring of log data (Logs) - Documented security incidents
				Q2-OPS-12.1B	Are identified events reported to the appropriate departments for timely assessment and remediation?	- Security incidents notification event report
OPS-13	LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION	OPS-13.1B	The CSP shall store all log data in an integrity-protected and aggregated form that allow its evaluation.	Q1-OPS-13.1B	Does the CSP store all log data in an integrity-protected and aggregated form that allow its centralized evaluation?	- Log data Database
		OPS-13.2B	The communication between the assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality whenever possible.	Q1-OPS-13.2B	Is the communication between the assets to be logged and the logging servers authenticated in integrity?	- Logs
				Q2-OPS-13.2B	Is the communication between the assets to be logged and the logging servers authenticated in confidentiality?	- Logs

				Q3-OPS-13.2B	Is the communication between the assets to be logged and the logging servers protected in integrity?	- Logs
				Q4-OPS-13.2B	Is the communication between the assets to be logged and the logging servers protected in confidentiality?	- Logs
		OPS-13.3B	Log data shall be deleted when no longer required for the purpose for which it was collected.	Q1-OPS-13.3B	Are log data deleted when it is no longer required for the purpose for which they were collected?	- Log data deletion record
OPS-14	LOGGING AND MONITORING – ATTRIBUTION	OPS-14.1B	The log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis during and following a security incident.	Q1-OPS-14.1B	Does the log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis in the event of an incident?	- Logs
OPS-15	LOGGING AND MONITORING – CONFIGURATION	OPS-15.1B	The CSP shall restrict access to system components under its responsibility, that are used for logging and monitoring, with strong authentication (for example multi-factor authentication).	Q1-OPS-15.1B	Does the CSP restrict access to system components under its responsibility, that are used for logging and monitoring with strong authentication?	- Documented authorized access users list
		OPS-15.2B	Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01).	Q1-OPS-15.2B	Are changes to the logging and monitoring configuration made in accordance with applicable policies (cf. CCM-01)?	- Cross References between changes to the logging and monitoring configuration and policies for changes to information systems
OPS-16	LOGGING AND MONITORING – AVAILABILITY	OPS-16.1B	The CSP shall monitor the system components for logging and monitoring under its responsibility, and shall automatically report failures to the responsible departments for assessment and remediation.	Q1-OPS-16.1B	Does the CSP monitor the system components for logging and monitoring under its responsibility?	- Documented system components monitor report
				Q2-OPS-16.1B	Does the CSP automatically report failures to the responsible departments for assessment and remediation?	- Automatized failures report

OPS-17	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES	OPS-17.1B	The CSP shall define and implement, in accordance with ISP-02, policies and procedures, including technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service.	Q1-OPS-17.1B	Does the CSP define in accordance with ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service?	- Documented policies and procedures
				Q2-OPS-17.1B	Does the CSP implement in accordance with ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service?	- Documented list of vulnerabilities in the system components used to provide the cloud service - Vulnerabilities addressing report
		OPS-17.2B	The CSP shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities.	Q1-OPS-17.2B	Does the CSP use a scoring system for the assessment of vulnerabilities?	- Documented scoring system
				Q2-OPS-17.2B	Does the scoring system for the assessment of vulnerabilities include at least “critical” and “high” classes of vulnerabilities?	- Classes of vulnerabilities identified in the scoring system. ("critical" & "high" at least)
OPS-18	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	OPS-18.1B	The CSP shall publish and maintain a publicly and easily accessible online register of vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or operate under their own responsibility.	Q1-OPS-18.1B	Does the CSP publish a publicly and easily accessible online register of vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or operate under their own responsibility?	-WEB - email - etc.
				Q2-OPS-18.1B	Does the CSP maintain a publicly and easily accessible online register of vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or	- Register of vulnerabilities update date

					operate under their own responsibility?	
		OPS-18.2B	The online register shall indicate at least the following information for every vulnerability: (1) A presentation of the vulnerability following an industry-accepted scoring system; (2) A description of the remediation options for that vulnerability; (3) Information on the availability of updates or patches for that vulnerability; (4) Information about the remediation or deployment of patches or updates by the CSP or CSC, including detailed instructions for operations to be performed by the CSC.	Q1-OPS-18.2B	Does the online register indicate for every vulnerability a presentation of the vulnerability following an industry-accepted scoring system?	- Vulnerability online register
				Q2-OPS-18.2B	Does the online register indicate for every vulnerability a description of the remediation options for that vulnerability?	- Vulnerability online register
				Q3-OPS-18.2B	Does the online register indicate for every vulnerability information on the availability of updates or patches for that vulnerability?	- Vulnerability online register
				Q4-OPS-18.2B	Does the online register indicate for every vulnerability information about the remediation or deployment of patches or updates by the CSP or CSC, including detailed instructions for operations to be performed by the CSC?	- Vulnerability online register
		OPS-18.3B	The CSP shall publish and maintain a publicly and easily accessible online register of vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have	Q1-OPS-18.3B	Does the CSP publish a publicly and easily accessible online register of vulnerabilities that affect the cloud service and assets?	- Vulnerability online register

			to install, provide or operate under their own responsibility.			
		OPS-18.4B	The CSP shall consult regularly the online registers published by its subservice providers and suppliers, analyse the potential impact of the published vulnerabilities on the cloud service, and handle them according to the vulnerability handling process (cf. OPS-17).	Q1-OPS-18.4B	Does the CSP regularly consult the online registers of vulnerabilities published by its subservice providers and suppliers?	
				Q2-OPS-18.4B	Does the CSP shall analyse the potential impact of the published vulnerabilities on the cloud service?	- Documented analysis of the potential impact of the published vulnerabilities on the cloud service
				Q3-OPS-18.4B	Does the CSP handle the vulnerabilities according to the vulnerability handling process (cf. OPS-17)?	Audit records concerning to the handled vulnerabilities
OPS-19	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION	OPS-19.1B	The CSP shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the cloud service, in accordance with policies for handling vulnerabilities (cf. OPS-17).	Q1-OPS-19.1B	Does the CSP perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the cloud service?	- Test report
OPS-20	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS	OPS-20.1B	The CSP shall regularly measure, analyse and assess the procedures with which vulnerabilities and security incidents are handled to verify their continued suitability, appropriateness and effectiveness.	Q1-OPS-20.1B	Does the CSP regularly measure the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness?	- Documented procedures review - Procedures' review date

	OF PROCEDURES					
				Q2-OPS-20.1B	Does the CSP regularly analyse the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness?	- Documented procedures review - Procedures' review date
				Q3-OPS-20.1B	Does the CSP regularly assess the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness?	- Documented procedures review - Procedures' review date
OPS-21	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	OPS-21.1B	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards.	Q1-OPS-21.1B	Does the CSP harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards?	- Documented hardens to all the system components under its responsibility - Changes in the system components (encompasses the hardens)
OPS-21		OPS-21.2B	The hardening requirements for each system component shall be documented.	Q1-OPS-21.2B	Are the hardening requirements for each system component documented?	- Documented hardening requirements for each system component
OPS-22	SEPARATION OF DATASETS IN THE CLOUD INFRASTRUCTURE	OPS-22.1B	The CSP shall segregate from other CSCs the data stored and processed on shared virtual and physical resources on behalf of a CSC to ensure the confidentiality and integrity of this data.	Q1-OPS-22.1B	Does the CSP segregate the CSC data stored and processed on shared virtual and physical resources to ensure the confidentiality and integrity of this data?	- CSC data stored and processed on shared virtual and physical resources

13.8 Identity, Authentication and Access Management

Table 22. Checklist for IAM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
IAM-01	POLICIES FOR ACCESS CONTROL TO INFORMATION	IAM-01.1B	The CSP shall define role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on the business and security requirements of the CSP, in which at least the following aspects are covered: (1) Parameters to be considered for making access control decisions; (2) Granting and modifying access rights based on the “least-privilege” principle and on the “need to-know” principle; (3) Segregation of duties between managing, approving and assigning access rights; (4) Dedicated rules for users with privileged access; (5) Requirements for the approval and documentation of the management of access rights.	Q1-IAM-01.1B	Have the CSP defined role and rights policies and procedures for controlling access to information resources?	- Documented role and rights policies and procedures for controlling access to information resources
				Q2-IAM-01.1B	Are the above defined policies and procedures aligned with the Global Information Security Policy defined in ISP-02?	- Cross references between role and rights policies and procedures for controlling access to information resources and Global Information Security Policy
				Q3-IAM-01.1B	Are the above defined policies and procedures based on the business and security requirements of the CSP?	- Policies and procedures review records (Approval signature)

				Q4-IAM-01.1B	Does the above defined policies and procedure contains at least: <ul style="list-style-type: none"> Parameters to be considered for making access control decisions Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle. Use of a role-based mechanism for the assignment of access rights Segregation of duties between managing, approving and assigning access rights Dedicated rules for users with privileged access Requirements for the approval and documentation of the management of access rights 	- Documented role and rights policies and procedures for controlling access to information resources (include these five topics) - Policies and procedures review records
		IAM-01.2B	The CSP shall link the access control policy defined in IAM-01.1 with the physical access control policy defined in PS-02.1, to guarantee that the access to the premises where information is located is also controlled.	Q1-IAM-01.2B	Does the IAM-01.1 documented policy and the PS-02.1 documented policy make cross reference between them?	- Cross references between IAM-01-1 policy and PS-02.1 policy
IAM-02	MANAGEMENT OF USER ACCOUNTS	IAM-02.1B	The CSP shall define policies for managing accounts, according to ISP-02, in which at least the following aspects are described: <ol style="list-style-type: none"> Parameters to be considered for making access control decisions; Assignment of unique usernames; Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type; Events and periods of inactivity leading to blocking and revoking accounts. 	Q1-IAM-02.1B	Are the policies for managing accounts defined?	- Documented policies for managing accounts

				Q2-IAM-02.1B	Are the policies for managing accounts aligned with ISP-02 policy?	- Policies review records
				Q3-IAM-02.1B	Does the documented policies for managing accounts contain at least: <ul style="list-style-type: none"> Parameters for making access control decisions Assignment of unique usernames Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type Events and periods of inactivity leading to blocking and revoking accounts. 	- Documented policies (encompass assignment of unique usernames, definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type & events leading to blocking and revoking accounts) - Policies review records
		IAM-02.2B	The CSP shall define and implement according to ISP-02 procedures for managing user accounts and access rights to employees that comply with the role and rights policies (cf. IAM-01) and with the policies for managing accounts.	Q1-IAM-02.2B	Are the procedures for managing personal user accounts and access rights to employees specified in IAM-01 defined?	- Documented procedures for managing personal user accounts and access rights to employees
				Q2-IAM-02.2B	Are the previous documented policies complying the role and rights concept and with the policies for managing accounts?	- Policy assessment result
				Q3-IAM-02.2B	Are these procedures implemented for internal employees?	- Personal user account and access rights for internal employees
				Q4-IAM-02.2B	Are these procedures implemented for external employees?	- Personal user account and access rights for external employees
		IAM-02.3B	The CSP shall define and implement according to ISP-02 procedures for managing shared accounts and associated access rights that comply with the role and rights policies (cf.	Q1-IAM-02.3B	Are the procedures for managing non-personal shared accounts and associated access rights specified in IAM-01 documented?	- Documented procedures for managing non-personal shared accounts and associated access rights

			IAM-01) and with the policies for managing accounts.			
				Q2-IAM-02.3B	Are the previous documented policies complying the role and rights concept and with the policies for managing accounts?	- Policy assessment result
				Q3-IAM-02.3B	Are these procedures implemented?	- Non-personal shared accounts and associated access rights
		IAM-02.4B	The CSP shall define and implement according to ISP-02 procedures for managing non-human accounts and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights policies (cf. IAM-01) and with the policies for managing accounts.	Q1-IAM-02.4B	Are the procedures for managing technical accounts and associated access rights to system components involved in the operation of the cloud service specified in ISP-02 defined?	- Documented procedures for managing technical accounts and associated access rights to system components involved in the operation of the cloud service
				Q2-IAM-02.4B	Are the previous documented policies complying the role and rights concept and with the policies for managing accounts?	- Policy assessment result
				Q3-IAM-02.4B	Are these procedures implemented?	- Technical accounts and associated access rights to system components involved in the operation of the cloud service
		IAM-02.5B	The CSP shall be able to provide, for a given user account, whether it falls under the responsibility of the CSP or of the CSC, as well as the list of the access rights currently granted to that account	Q1-IAM-02.5B	Can the CSP provide for a given user account, whether it falls under the responsibility of the CSP or of the CSC?	- Fault register associated to a user account in which it is specified if the faults responsibility is of CSP or CSC
				Q2-IAM-02.5B	Can the CSP provide for a given user account, the list of the access rights granted to that account?	- List of access right granted associated to a user account that has fault
IAM-03	LOCKING, UNLOCKING AND REVOCATION	IAM-03.1B	The CSP shall document and implement an automated mechanism to block user accounts after a certain period of inactivity.	Q1-IAM-03.1B	Does the CSP document a mechanism that automatically block user accounts after a certain period of inactivity?	- Documented description of the mechanism to block user accounts after a certain period of inactivity

	OF USER ACCOUNTS					
				Q2-IAM-03.1B	Is the "certain period of inactivity" quantified and documented somewhere?	- Document in which is specified the "certain period of time" after which the user account is automatically blocked
				Q3-IAM-03.1B	Does the automated mechanism in place executed when some user account overcome the specified period of time?	- Evidence of blocked user accounts that meet the defined requirements
		IAM-03.2B	The CSP shall document and implement an automated mechanism to block accounts after a certain number of failed authentication attempts.	Q1-IAM-03.2B	Does the CSP define a mechanism that automatically block user accounts after a certain number of failed authentication attempts?	- Documented description of the mechanism to block user accounts
				Q2-IAM-03.2B	Is the "certain number of failed authentication attempts" quantified and documented somewhere?	- Document in which is specified the "certain number of failed authentication attempts" after which the user account is automatically blocked
				Q3-IAM-03.2B	Does the automated mechanism in place executed after the specified certain number of failed authentication attempts?	- Evidence of blocked user accounts that meet the defined requirements
IAM-04	MANAGEMENT OF ACCESS RIGHTS	IAM-04.1B	The CSP shall document and implement procedures to grant, update, and revoke to an account under its responsibility access rights to resources of the information system of the cloud service, and these procedures shall be in conformity with the role and rights policies and with the policies for managing access rights.	Q1-IAM-04.1B	Has the CSP documented procedures to grant, update, and revoke to a user account under its responsibility access rights to resources of the information system of the cloud service?	- Documented procedures to grant, update, and revoke to a user account under its responsibility access rights to resources of the information system of the cloud service
				Q2-IAM-04.1B	Are these documented procedures compliant with the role and rights concept and with the policies for managing access rights?	- Procedure assessment results

				Q3-IAM-04.1B	Are these procedures implemented within the CSP?	- Examples of user accounts to which access rights to resources of the information system of the cloud service have been granted, updated, revoked
		IAM-04.2B	The CSP shall document and implement a procedure to timely update or revoke the access rights of an internal or external employee when the role and responsibilities of the employee change.	Q1-IAM-04.2B	Has the CSP documented procedures to timely update or revoke the access rights of an internal or external employee when the role and responsibilities of the employee change?	- Documented procedures o timely update or revoke the access rights of an internal or external employee when the role and responsibilities of the employee change
				Q2-IAM-04.2B	Are the previous documented procedures implemented for internal employees?	- Example of internal employees whose access rights have been updated/revoked when their role and responsibilities has changed
				Q3-IAM-04.2B	Are the previous documented procedures implemented for external employees?	- Example of external employees whose access rights have been updated/revoked when their role and responsibilities has changed
IAM-05	REGULAR REVIEW OF ACCESS RIGHTS	IAM-05.1B	The CSP shall review the access rights of all the accounts under its responsibility at least once a year to ensure that they still correspond to the current needs.	Q1-IAM-05.1B	Does the CSP periodically review the access rights of all user accounts under its responsibility?	- Access rights review results (execution date less than 12 months).
				Q2-IAM-05.1B	Is the previous review executed at least annually for all the user accounts under the CSP responsibility?	- Review execution dates of the last 2/3 years
IAM-06	PRIVILEGED ACCESS RIGHTS	IAM-06.1B	Shared accounts under the responsibility of the CSP shall be assigned only to employees.	Q1-IAM-06.1B	Are the shared accounts under the responsibility of the CSP assigned only to employees?	- Assignment of the shared accounts

IAM-07	AUTHENTICATI ON MECHANISMS	IAM-07.1B	The CSP shall define and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects: (1) The selection of mechanisms suitable for every type of account and each level of risk; (2) The protection of credentials used by the authentication mechanism; (3) The generation and distribution of credentials for new accounts; (4) Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and (5) Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules.	Q1-IAM-07.1B	Has the CSP defined policy and procedures about authentication mechanisms according to IPS-02?	- Documented policy and procedures
				Q2-IAM-07.1B	Does these policy and procedures cover at least the following aspects: • The selection of mechanisms suitable for every type of account and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new accounts; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules	- Documented policy and procedures (encompass the five topics) - Documented policy and procedures review records

				Q3-IAM-07.1B	Are these policy and procedures implemented within the CSP organization?	- Logs -Databases or any other software asset
		IAM-07.2B	The access to all environments of the CSP shall be authenticated, including non-production environments.	Q1-IAM-07.2B	Is the access to all the CSP environments authenticated?	- Access Logs to the -production environment, in order to see the authentication protocol applied to production environment
				Q2-IAM-07.2B	Are the non-production environment also included in the previous authentication?	- Access Logs to the non-production environments, in order to see the authentication protocol applied to non-production environment
		IAM-07.3B	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts.	Q1-IAM-07.3B	Does every authentication mechanism in place within CSP include a mechanism to block an account after a predefined number of unsuccessful attempts?	- If this is something "static": documents that for each authentication mechanism document the blocking mechanism - If this is something "dynamic": examples of blocked account due to unsuccessful attempts
IAM-08	PROTECTION AND STRENGTH OF CREDENTIALS	IAM-08.1B	The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: (1) Non-reuse of credentials; (2) Trade-offs between entropy and ability to memorize; (3) Recommendations for renewal of passwords; (4) Rules on storage of passwords.	Q1-IAM-08.1B	Have the CSP documented rules and recommendations for the management of credentials?	- Document with rules and recommendations for the management of credentials
				Q2-IAM-08.1B	Does the previous document contain at least:	- Document with rules and recommendations for the

					<ul style="list-style-type: none"> • Non-reuse of credentials • Trade-offs between entropy and ability to memorize • Recommendations for renewal of passwords • Rules on storage of passwords 	management of credentials (encompass the four topics) - Document with rules and recommendations for the management of credentials review records
				Q3-IAM-08.1B	Have the CSP communicated to all users under its responsibility the rules and recommendations for the management of credentials?	- Communication mechanism: - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q4-IAM-08.1B	Have the CSP made available to all users under its responsibility the rules and recommendations for the management of credentials?	- Examples of documents with rules and recommendations for the management of credentials provided by sampled users
		IAM-08.2B	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01)	Q1-IAM-08.2B	Are all the passwords stored using cryptographically strong hash functions according to the policy defined in CKM-01?	- Example of stored passwords randomly selected
		IAM-08.3B	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	Q1-IAM-08.3B	If cryptographic authentication mechanisms are used, do they follow the policies and procedures specified in CKM-01?	- Example of cryptographic authentication mechanisms randomly selected + Review results against CKM-01 policies
IAM-09	GENERAL ACCESS RESTRICTIONS	IAM-09.1B	The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems.	Q1-IAM-09.1B	Have the CSP implemented partitioning measures between the information system providing the cloud service and its other information systems?	- Example of partitioning measures randomly identified
				Q2-IAM-09.1B	Are the partitioning measures sufficient?	N.B. Not possible to demonstrate with the current level of objectiveness
		IAM-09.2B	The CSP shall implement suitable measures for partitioning between the CSCs.	Q1-IAM-09.2B	Did the CSP implement measures for partitioning between the CSCs?	- Example of partitioning measures between CSCs randomly identified

13.9 Cryptography & Key management

Table 23. Checklist for CKM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
CKM-01	POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT	CKM-01.1B	The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described: (1) Usage of strong cryptographic mechanisms and secure network protocols; (2) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; (3) Consideration of relevant legal and regulatory obligations and requirements.	Q1-CKM-01.1B	Does the CSP document policies with technical and organizational safeguards for encryption and key management, according to ISP-02?	- Documented policies with technical and organizational safeguards for encryption and key management (encompasses the three aspects)
				Q2-CKM-01.1B	Does the CSP implement policies with technical and organizational safeguards for encryption and key management, according to ISP-02?	- Audit records / Logs
				Q3-CKM-01.1B	Do policies describe usage of strong encryption procedures and secure network protocols?	- Policies (describe usage of strong encryption procedures and secure network protocols)
				Q4-CKM-01.1B	Do policies describe requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, and deletion of the keys?	- Policies (describe requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, and deletion of the keys)
				Q5-CKM-01.1B	Do policies describe consideration of relevant legal and regulatory obligations and requirements?	- Policies (describe consideration of relevant legal

						and regulatory obligations and requirements)
CKM-02	ENCRYPTION OF DATA IN TRANSIT	CKM-02.1B	The CSP shall define and implement strong cryptographic mechanisms for the transmission of CSC data over public networks, in order to protect the confidentiality, integrity and authenticity of data.	Q1-CKM-02.1B	Does the CSP define strong encryption mechanisms for the transmission of CSC data over public networks?	- Encryption mechanisms design
				Q2-CKM-02.1	Does the CSP implement strong encryption mechanisms for the transmission of cloud customer data over public networks?	- Audit records - Examples of encrypted data
CKM-03	ENCRYPTION OF DATA AT REST	CKM-03.1B	The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	Q1-CKM-03.1B	Does the CSP document procedures and technical safeguards to protect cloud customers' data during storage according to ISP-02?	- Documented procedures and technical safeguards to encrypt cloud customers' data during storage
				Q2-CKM-03.1B	Does the CSP implement technical safeguards to protect cloud customers' data during storage?	- Audit records - Examples of encrypted data
CKM-03		CKM-03.2B	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	Q1-CKM-03.2B	Does the CSP notify customers about any updates to technical safeguards and to the procedures that protect the confidentiality of customers' data during storage that may affect the confidentiality of the data?	- Documented notifications to customers (email, reports, web, etc.)
				Q2-CKM-03.2B	Does the CSP notify customers about any changes in the storage of customer data that may affect the confidentiality of the data?	- Documented notifications to customers (email, reports, web, etc.)

CKM-04	SECURE KEY MANAGEMENT	CKM-04.1B	Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects: (1) Generation of keys for different cryptographic systems and applications; (2) Issuing and obtaining public-key certificates; (3) Provisioning and activation of the keys; (4) Secure storage of keys including description of how authorised users get access; (5) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; (6) Handling of compromised keys; and (7) Withdrawal and deletion of keys;	Q1-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include a generation of keys for different cryptographic systems and applications?	- Documented procedures and technical safeguards for secure key management (include a generation of keys for different cryptographic systems and applications) - Documented procedures and technical safeguards for secure key management compliance review record
				Q2-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include issuing and obtaining public-key certificates?	- Documented procedures and technical safeguards for secure key management (include issuing and obtaining public-key certificates) - Documented procedures and technical safeguards for secure key management compliance review record
				Q3-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include provisioning and activation of the keys?	- Documented procedures and technical safeguards for secure key management (include provisioning and activation of the keys) - Documented procedures and technical safeguards for secure key management compliance review record

				Q4-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include secure storage of keys including description of how authorised users get access?	<ul style="list-style-type: none"> - Documented procedures and technical safeguards for secure key management (include secure storage of keys including description of how authorised users get access) - Documented procedures and technical safeguards for secure key management compliance review record
				Q5-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised?	<ul style="list-style-type: none"> - Documented procedures and technical safeguards for secure key management (include changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised) - Documented procedures and technical safeguards for secure key management compliance review record
				Q6-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include handling of compromised keys?	<ul style="list-style-type: none"> - Documented procedures and technical safeguards for secure key management (include handling of compromised keys) - Documented procedures and technical safeguards for secure key management compliance review record
				Q7-CKM-04.1B	Do procedures and technical safeguards for secure key management in the area of responsibility of the CSP include withdrawal and deletion of keys?	<ul style="list-style-type: none"> - Documented procedures and technical safeguards for secure key management (include withdrawal and deletion of keys)

						- Documented procedures and technical safeguards for secure key management compliance review record
--	--	--	--	--	--	---

13.10 Communications Security

Table 24. Checklist for CS basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
CS-01	TECHNICAL SAFEGUARDS	CS-01.1B	The CSP shall define and implement technical safeguards that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems, in accordance with ISP-02.	Q1-CS-01.1B	Does the CSP document technical safeguards to ensure the protection of information and information processing systems that are suitable to promptly detect and respond to network-based attacks?	- Documented technical safeguards
				Q2-CS-01.1B	Does the CSP communicate technical safeguards that are suitable to promptly detect and respond to network-based attacks?	- Intranet - email - Wallchart - Specific meetings minutes - etc.
				Q3-CS-01.1B	Does the CSP implement technical safeguards that are suitable to promptly detect and respond to network-based attacks?	- Event log and monitoring to allow the recording and detection of actions that could affect, or be relevant, for information security - Audit report
				Q4-CS-01.1B	Does the CSP document technical safeguards to ensure the protection of information and information processing systems?	- Documented technical safeguards

				Q5-CS-01.1B	Does the CSP communicate technical safeguards to ensure the protection of information and information processing systems?	<ul style="list-style-type: none"> - Intranet - email - Wallchart - Specific meetings minutes - etc.
				Q6-CS-01.1B	Does the CSP implement technical safeguards to ensure the protection of information and information processing systems?	<ul style="list-style-type: none"> - Event log and monitoring to allow the recording and detection of actions that could affect, or be relevant, for information security - Audit report
CS-02	SECURITY REQUIREMENTS TO CONNECT WITHIN THE CSP'S NETWORK	CS-02.1B	The CSP shall define and implement according to ISP-02 specific security requirements to connect within its network, including at least: (1) When the security zones are to be separated and when the CSCs are to be logically or physically segregated; (2) What communication relationships and what network and application protocols are permitted in each case; (3) How the data traffic for administration and monitoring are segregated from each other at the network level; (4) What internal, cross-location communication is permitted; and (5) what cross-network communication is allowed.	Q1-CS-02-1B	Do the CSP document specific security requirements to connect within its network?	- Documented specific security requirements to connect within its network
				Q2-CS-02-1B	Do the CSP communicate specific security requirements to connect within its network?	<ul style="list-style-type: none"> - Communication mechanism: <ul style="list-style-type: none"> -Intranet/WEB -email - Wallchart - Specific meetings minutes - etc.
				Q3-CS-02-1B	Do the CSP make available specific security requirements to connect within its network?	<ul style="list-style-type: none"> - Distribution mechanism: <ul style="list-style-type: none"> - Information management system

						- Intranet/WEB - email - etc.
				Q4-CS-02-1B	Do the CSP implement specific security requirements to connect within its network?	- Audit records
				Q5-CS-02-1B	Do specific security requirements to connect within its network address when the security zones are to be separated and when the cloud customers are to be logically or physically segregated?	- Documented specific security requirements to connect within its network review record
				Q6-CS-02-1B	Do specific security requirements to connect within its network address what communication relationships and what network and application protocols are permitted in each case?	- Documented specific security requirements to connect within its network review record
				Q7-CS-02-1B	Do specific security requirements to connect within its network address how the data traffic for administration and monitoring are segregated from each other at the network level?	- Documented specific security requirements to connect within its network review record
				Q8-CS-02-1B	Do specific security requirements to connect within its network address what internal, cross-location communication is permitted?	- Documented specific security requirements to connect within its network review record
				Q9-CS-02-1B	Do specific security requirements to connect within its network address what cross-network communication is allowed?	- Documented specific security requirements to connect within its network review record
CS-03	MONITORING OF CONNECTIONS WITHIN THE	CS-03.1B	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment.	Q1-CS-03.1B	Does the CSP distinguish between trusted and untrusted networks?	- Documented list of trusted and untrusted networks

	CSP'S NETWORK					
				Q2-CS-03.1B	Is that distinction based on a risk assessment?	- Documented risk assessment
		CS-03.2B	The CSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable).	Q1-CS-03.2B	Does the CSP separate trusted and untrusted networks into different security zones for internal network areas?	- Documented network topology
				Q2-CS-03.2B	Does the CSP separate trusted and untrusted networks into different security zones for external network areas?	- Documented network topology
				Q3-CS-03.2B	Does the CSP separate trusted and untrusted networks into different security zones for DMZ, if applicable?	- Documented network topology
		CS-03.3B	The CSP shall design and configure both physical and virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02).	Q1-CS-03.3B	Does the CSP shall design virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02)?	- Documented physical network environments design
				Q2-CS-03.3B	Does the CSP shall design virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02)?	- Documented virtualized network environments design
				Q3-CS-03.3B	Does the CSP configure physical network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02)?	- Documented physical network environments configuration

				Q4-CS-03.3B	Does the CSP configure virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02)	- Documented virtualized network environments configuration
		CS-03.4B	The CSP shall review at specified intervals the business justification for using all services, protocols, and ports. This review shall also include the compensatory measures used for protocols that are considered insecure.	Q1-CS-03.4B	Does the CSP review at specified intervals the business justification for using all services, protocols, and ports?	- Documented review records (last 2/3 years)
CS-04	NETWORKS FOR ADMINISTRATION	CS-04.1B	The CSP shall define and implement separate networks for the administrative management of the infrastructure and the operation of management consoles.	Q1-CS-04.1B	Does the CSP define separate networks for the administrative management of the infrastructure and the operation of management consoles?	- Documented network topology - Documented network design
				Q2-CS-04.1B	Does the CSP implement separate networks for the administrative management of the infrastructure and the operation of management consoles	- Audit records
		CS-04.2B	The CSP shall logically or physically separate the networks for administration from the CSCs' networks.	Q1-CS-04.2B	Does the CSP logically or physically separate the networks for administration from the CSCs' networks?	- Documented network topology - Documented network design
		CS-04.3B	The CSP shall segregate physically or logically the networks used to migrate or create virtual machines.	Q1-CS-04.3B	Does the CSP segregate physically or logically the networks used to migrate or create virtual machines?	- Documented network topology - Documented network design
CS-05	TRAFFIC SEGREGATION IN SHARED NETWORK ENVIRONMENTS	CS-05.1B	The CSP shall document and implement separation mechanisms at network level the data traffic of different CSCs.	Q1-CS-05.1B	Does the CSP define separation mechanisms at network level the data traffic of different CSCs?	- List of separation mechanisms at network level

				Q2-CS-05.1B	Does the CSP document separation mechanisms at network level the data traffic of different cloud customers?	- Documented separation mechanisms design at network level
				Q3-CS-05.1B	Does the CSP implement separation mechanisms at network level the data traffic of different cloud customers?	- Audit records
CS-06	NETWORK TOPOLOGY DOCUMENTATION	CS-06.1B	The CSP shall maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service.	Q1-CS-06.1B	Does the CSP maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service?	- Document version control box up-to-date - Configuration management audit record
		CS-06.2B	The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with third-party and public networks, and the geographical locations in which the CSC data is stored.	Q1-CS-06.2B	Does the documentation cover how the subnets are allocated?	- Documentation of the logical structure of the network used to provision or operate the cloud service review record
				Q2-CS-06.2B	Does the documentation cover how the network is zoned and segmented?	- Documentation of the logical structure of the network used to provision or operate the cloud service review record
				Q3-CS-06.2B	Does the documentation cover how it connects with third-party and public networks?	- Documentation of the logical structure of the network used to provision or operate the cloud service review record
				Q4-CS-06.2B	Does the documentation cover the geographical locations in which the CSC data is stored?	- Documentation of the logical structure of the network used to provision or operate the cloud service review record

CS-07	SOFTWARE DEFINED NETWORKING	CS-07.1B	The CSP shall ensure the confidentiality of CSC data by suitable procedures when offering functions to CSCs for software-defined networking (SDN).	Q1-CS-07.1B	Does the CSP ensure the confidentiality of the cloud user data by suitable procedures when offering functions to CSCs for software-defined networking (SDN)?	- Documented suitable procedures to ensure the confidentiality of the cloud user data
		CS-07.2B	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features.	Q1-CS-07.2B	Does the CSP validate the functionality of the SDN functions before providing new SDN features to CSCs?	- SDN functions validation record
CS-08	DATA TRANSMISSIO N POLICIES	CS-08.1B	The CSP shall define and implement policies and procedures with technical and organisational safeguards to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, according to ISP-02.	Q1-CS-08.1B	Does the CSP define policies and procedures with technical and organisational safeguards to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, according to ISP-02?	- Documented policies and procedures with technical and organisational safeguards
				Q2-CS-08.1B	Does the CSP implement policies and procedures with technical and organisational safeguards to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, according to ISP-02?	- Audit records

13.11 Portability and Interoperability

Table 25. Checklist for PI basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
PI-01	DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES	PI-01.1B	Inbound and outbound interfaces that are made accessible for use by cloud services from other CSPs or CSCs' IT systems shall be documented.	Q1-PI-01.1B	Is the cloud service accessible by cloud services from other CSPs or cloud customers IT systems?	- Accessible APIs - Public URLs
				Q2-PI-01.1B	Are the inbound interfaces documented?	- Documented inbound interfaces (internal domain names)
				Q3-PI-01.1B	Are the outbound interfaces documented?	- Documented outbound interfaces
		PI-01.2B	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.	Q1-PI-01.2B	Are the interfaces clearly documented for subject matter experts to understand how they can be used to retrieve the data?	- Documented inbound and outbound interfaces (internal domain names and ports, mechanisms, username/pwd, etc.) - Peer review of the documented interfaces
		PI-01.3B	Communication on these interfaces shall use documented communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements, and the adequate authentication of the user.	Q1-PI-01.3B	Does communication on these interfaces use standardized communication protocols?	- Documented list of supported communication protocols
				Q2-PI-01.3B	Do protocols ensure the confidentiality and integrity of the transmitted information according to its protection requirements and the adequate authentication of the user?	- Documented list of supported communication protocols

		PI-01.4B	Communication over untrusted networks shall be protected in confidentiality, integrity and authenticity according to CKM-02.	Q1-PI-01.4B	Is the communication over untrusted networks protected in confidentiality, integrity and authenticity according to CKM-02?	- Authentication and Protection Settings
PI-02	CONTRACTUAL AGREEMENTS FOR THE PROVISION OF DATA	PI-02.1B	The CSP shall include in cloud service contractual agreements, at least, the following aspects concerning the termination of the contractual relationship: (1) Type, scope and format of the data the CSP provides to the CSC; (2) Delivery methods of the data to the CSC; (3) Definition of the timeframe, within which the CSP makes the data available to the CSC; (4) Definition of the point in time as of which the CSP makes the data inaccessible to the CSC and deletes these; and (5) The CSC's responsibilities and obligations to cooperate for the provision of the data.	Q1-PI-02.1B	Does the CSP in cloud service contractual agreements concerning the termination of the contractual relationship include type, scope and format of the data the CSP provides to the CSC?	- Contractual agreements concerning the termination of the contractual relationship (include type, scope and format of the data the CSP provides to the CSC)
				Q2-PI-02.1B	Does the CSP in cloud service contractual agreements concerning the termination of the contractual relationship include delivery methods of the data to the cloud customer?	- Contractual agreements concerning the termination of the contractual relationship (include delivery methods of the data to the cloud customer)
				Q3-PI-02.1B	Does the CSP in cloud service contractual agreements concerning the termination of the contractual relationship include definition of the timeframe, within which the CSP makes the data available to the CSC?	- Contractual agreements concerning the termination of the contractual relationship (include definition of the timeframe, within which the CSP makes the data available to the CSC)
				Q4-PI-02.1B	Does the CSP in cloud service contractual agreements concerning the termination of the contractual relationship include definition of the point in time as of which the CSP	- Contractual agreements concerning the termination of the contractual relationship (include definition of the point in time as of which the CSP

					makes the data inaccessible to the CSC and deletes these?	makes the data inaccessible to the CSC and deletes these)
				Q5-PI-02.1B	Does the CSP in cloud service contractual agreements concerning the termination of the contractual relationship include the CSC's responsibilities and obligations to cooperate for the provision of the data?	- Contractual agreements concerning the termination of the contractual relationship (include the CSC's responsibilities and obligations to cooperate for the provision of the data)
PI-03	SECURE DELETION OF DATA	PI-03.1B	The CSP shall implement procedures for deleting its customers' data upon termination of their contract in compliance with the contractual agreements between them.	Q1-PI-03.1B	Does the CSP implement procedures for deleting its customers' data upon termination of their contract in compliance with the contractual agreements between them?	- Procedures for deleting customer's data - Data destruction tools - Data destruction records (a filled form or screenshot identifying the data deletion (successful / fail))
		PI-03.2B	The CSC's data deletion shall include all CSC data, as well as related metadata and cloud service derived data, such as data stored in data backups.	Q1-PI-03.2B	Does the CSC's data deletion include all CSC data, as well as related metadata and cloud service derived data?	- Procedures for deleting customer's data - Data destruction tools - Data destruction records (a filled form or screenshot identifying the data deletion (successful / fail))
				Q2-PI-03.2B	Does the CSC's data deletion include data stored in the data backups?	- Procedures for detecting customer's data - Data destruction tools - Data destruction records (a filled form or screenshot identifying the data deletion (successful / fail))
		PI-03.3B	At the end of the contract, the CSP shall delete the technical data concerning the CSC.	Q1-PI-03.3B	At the end of a contract, does the CSP delete the technical data concerning the CSC?	- Technical data erasure records

13.12 Change and configuration management

Table 26. Checklist for CCM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
CCM-01	POLICIES FOR CHANGES TO INFORMATION SYSTEMS	CCM-01.1B	The CSP shall define and implement policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02.	Q1-CCM-01.1B	Is there a document describing the policy for change management of the IT systems supporting the cloud service?	- Change management policy document
				Q2-CCM-01.1B	Are there documented procedures for change management of the IT systems supporting the cloud service?	- Documented procedures for change management
				Q3-CCM-01.1B	Does the CSP communicate the defined policies and procedures for change management of the IT systems supporting the cloud service?	-Intranet/WEB -email - Wallchart - Specific meetings minutes - etc.
				Q4-CCM-01.1B	Does the CSP implement the defined policies and procedures for change management of the IT systems supporting the cloud service?	- Change managements record & evidence - Audit records
CCM-02	RISK ASSESSMENT, CATEGORISATION AND PRIORITISATION OF CHANGES	CCM-02.1B	The CS shall categorise and prioritise changes considering the potential security effects on the system components concerned.	Q1-CCM-02.1B	Does the CSP categorize changes considering the potential security effects on the system components concerned?	-List of categorised changes
				Q2-CCM-02.1B	Does the CSP prioritise changes considering the potential security effects on the system components concerned?	-List of how changes are prioritized

CCM-03	TESTING CHANGES	CCM-03.1B	The CSP shall test proposed changes before deployment to the production environment.	Q1-CCM-03.1B	Does the CSP test proposed changes before deployment to the production environment?	<ul style="list-style-type: none"> - Test plan - Tests (unit tests / continuous integration tests) - Documented test execution results
		CCM-03.2B	Before using CSC data for tests, the CSP shall first obtain approval from CSC and anonymise CSC data, and the CSP shall guarantee the confidentiality of the data during the whole process.	Q1-CCM-03.2B	Before using CSC data for tests, does the CSP first obtain approval from CSC?	<ul style="list-style-type: none"> - Documented approval from CSC
				Q2-CCM-03.2B	Before using customer data for tests, does the CSP anonymise customer data?	<ul style="list-style-type: none"> - Documented compliance review of anonymized customer data
				Q3-CCM-03.2B	Before using customer data for tests, does the CSP guarantee the confidentiality of the data during the whole process?	<ul style="list-style-type: none"> - Confidentiality agreement
CCM-04	APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	CCM-04.1B	The CSP shall approve any change to the cloud service, based on defined criteria, before they are made available to CSCs in the production environment.	Q1-CCM-04.1B	Are there defined criteria to approve any change to the cloud service before they are made available to CSCs in the production environment?	<ul style="list-style-type: none"> - Documented list of defined criteria to approve any change to the cloud service before they are made available to CSCs in the production environment
				Q2-CCM-04.1B	Does the CSP use the defined criteria to approve any change to the cloud service before they are made available to CSCs in the production environment?	<ul style="list-style-type: none"> - Evidence of use the defined criteria to approve any change to the cloud service before they are made available to CSCs in the production environment - Audit records
CCM-05	PERFORMING AND LOGGING CHANGES	CCM-05.1B	The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment.	Q1-CCM-05.1B	Does the CSP define roles for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment?	<ul style="list-style-type: none"> - Documented list of roles and the changes they are allowed to make and to which components

				Q2-CCM-05.1B	Does the CSP shall define rights for the defined roles according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment?	- Documented list of rights for each role
		CCM-05.2B	All changes to the cloud service in the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change.	Q1-CCM-05.2B	Are all changes to the cloud service in the production environment logged to the individual or system component that initiated the change?	- Log record of the session of the individual or system component that initiated the change
				Q2-CCM-05.2B	Are all changes to the cloud service in the production environment traceable back to the individual or system component that initiated the change?	- Log record of the session of the individual or system component that initiated the change
CCM-06	VERSION CONTROL	CCM-06.1B	The CSP shall implement version control procedures to track the dependencies of individual changes and to be able to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.	Q1-CCM-06.1B	Does the CSP document version control procedures to track the dependencies of individual changes?	- Documented version control procedures
				Q2-CCM-06.1B	Does the CSP implement version control procedures to track the dependencies of individual changes?	- Documented list of dependencies of individual changes - Version control management tool - Tool for the management of binaries
				Q3-CCM-06.1B	Are the CSP document version control procedures able to restore affected system components back to their previous state as a result of errors or identified vulnerabilities?	- Documented version control procedures

				Q4-CCM-06.1B	Does the CSP implement version control procedures that are able to restore affected system components back to their previous state as a result of errors or identified vulnerabilities?	<ul style="list-style-type: none"> - System tags - Version control tool
--	--	--	--	---------------------	---	---

13.13 Development of Information Systems

Table 27. Checklist for DEV basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
DEV-01	POLICIES FOR THE DEVELOPMENT AND PROCUREMENT OF INFORMATION SYSTEMS	DEV-01.1B	The CSP shall define and implement policies and procedures according to ISP-02 with technical and organisational measures for the secure development of the cloud service.	Q1-DEV-01.1B	Does the CSP document policies and procedures according to security policies and procedures (ISP-02) with technical and organisational measures for the secure development of the cloud service?	<ul style="list-style-type: none"> - Documented policies and procedures
				Q2-DEV-01.1B	Does the CSP communicate policies and procedures according to security policies and procedures (ISP-02) with technical and organisational measures for the secure development of the cloud service?	<ul style="list-style-type: none"> - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q3-DEV-01.1B	Does the CSP implement policies and procedures according to security policies and procedures (ISP-02) with technical and organisational measures for the secure development of the cloud service?	<ul style="list-style-type: none"> - Safe development guides for each programming language used - Safety requirements in the design phase - Security checkpoints incorporated into project

						milestones - Secure repositories - Security by design practices
		DEV-01.2B	The policies and procedures for secure development shall consider information security from the earliest phases of design.	Q1-DEV-01.2B	Do the policies for secure development consider information security from the earliest phases of design?	- Documented policies (encompasses information security from the earliest phases of design)
				Q2-DEV-01.2B	Do the procedures for secure development consider information security from the earliest phases of design?	- Documented procedures (encompass information security from the earliest phases of design)
DEV-02	DEVELOPMENT SUPPLY CHAIN SECURITY	DEV-02.1B	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its cloud service.	Q1-DEV-02.1B	Does the CSP maintain a list of dependencies to hardware products used in the development of its cloud service?	- Documented list of dependencies to hardware products used in the development of its cloud service
				Q2-DEV-02.1B	Does the CSP maintain a list of dependencies to software products used in the development of its cloud service?	- Documented list of dependencies to software products used in the development of its cloud service
DEV-03	SECURE DEVELOPMENT ENVIRONMENT	DEV-03.1B	The CSP shall ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.	Q1-DEV-03.1B	Does the CSP ensure that the confidentiality of the source code is adequately protected at all stages of development?	- Source code protection policy (e.g., NDA, IPR, License)
				Q2-DEV-03.1B	Does the CSP ensure that the integrity of the source code is adequately protected at all stages of development?	- SAST and DAST results - security code checks
		DEV-03.2B	The CSP shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers.	Q1-DEV-03.2B	Does the CSP use version control to keep a history of the changes in source code?	- Version control tool in use
				Q2-DEV-03.2B	Is it maintained an attribution of changes to individual developers?	- Version control tool - Change log records

DEV-04	SEPARATION OF ENVIRONMENTS	DEV-04.1B	The CSP shall ensure that production environments are physically or logically separated from development, test or pre-production environments.	Q1-DEV-04.1B	Does the CSP ensure that production environments are physically or logically separated from development environments?	- Documented environments description
				Q2-DEV-04.1B	Does the CSP ensure that production environments are physically or logically separated from test environments?	- Documented environments description
				Q3-DEV-04.1B	Does the CSP ensure that production environments are physically or logically separated from pre-production environments?	- Documented environments description
		DEV-04.2B	CSC data contained in the production environments shall not be used in development, test or pre-production environments in order not to compromise their confidentiality.	Q1-DEV-04.2B	Is CSC data contained in the production environments being prevented to be used in development, test or pre-production environments?	- Data set used in test and pre-production environments
DEV-05	DEVELOPMENT OF SECURITY FEATURES	DEV-05.1B	The CSP shall define and implement according to ISP-02 specific procedures for the development of security features that implement technical mechanisms or safeguards required by the EUCS, with increased testing requirements.	Q1-DEV-05.1B	Does the CSP define specific procedures for the development of functions that implement technical mechanisms or safeguards required by the EUCS scheme, with increased testing requirements?	- Documented specific procedures for the development of functions
				Q2-DEV-05.1	Does the CSP implement specific procedures for the development of functions that implement technical mechanisms or safeguards required by the EUCS scheme, with increased testing requirements?	- Technical mechanisms or safeguards required by the EUCS scheme, with increased testing requirements
DEV-06	IDENTIFICATION OF VULNERABILITIES OF THE CLOUD SERVICE	DEV-06.1B	The CSP shall apply appropriate measures to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process.	Q1-DEV-06.1B	Does the CSP apply appropriate measures to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process?	-Vulnerability assessments results (manual)

DEV-06		DEV-06.2B	The CSP shall apply appropriate measures to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process.	Q1-DEV-06.2B	Are the procedures for identifying vulnerabilities integrated in the development process?	<ul style="list-style-type: none"> - Documented procedures for identifying vulnerabilities - Documented development process - Development process audit records
DEV-07	OUTSOURCING OF THE DEVELOPMENT	DEV-07.1B	<p>When outsourcing development of the cloud service or components thereof to a contractor, the CSP and the contractor shall contractually agree on specifications regarding at least the following aspects:</p> <p>(1) Security in software development (requirements, design, implementation, tests and verifications) in accordance with published standards and established methods;</p> <p>(2) Acceptance testing of the quality of the services provided in accordance with the agreed functional and nonfunctional requirements; and</p> <p>(3) Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.</p>	Q1-DEV-07.1B	When outsourcing development of the cloud service or components thereof to a contractor, do the CSP and the contractor contractually agree on specifications regarding at security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods?	- Contract signed by both parts
				Q2-DEV-07.1B	When outsourcing development of the cloud service or components thereof to a contractor, do the CSP and the contractor contractually agree on specifications regarding at acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements?	- Contract signed by both parts
				Q3-DEV-07.1B	When outsourcing development of the cloud service or components thereof to a contractor, do the CSP and the contractor contractually agree on specifications regarding	- Contract reviewed and signed by both parts

					providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities?	
--	--	--	--	--	--	--

13.14 Procurement Management

Table 28. Checklist for PM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
PM-01	POLICIES AND PROCEDURES FOR CONTROLLING AND MONITORING THIRD PARTIES	PM-01.1B	The CSP shall define and implement policies and procedures according to ISP-02 for controlling and monitoring third-parties whose products or services contribute to the provision of the cloud service.	Q1-PM-01.1B	Is there a document describing the policy for controlling and monitoring third parties whose products or services contribute to the provision of the cloud service?	-Controlling and monitoring third parties whose products or services contribute to the provision of the cloud service policy document
PM-02	RISK ASSESSMENT OF SUPPLIERS	PM-02.1B	The CSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties before they start contributing to the provision of the cloud service.	Q1-PM-02.1B	Does the CSP perform a risk assessment of its suppliers or the control and monitoring of third parties before they start contributing to the provision of the cloud service?	- Documented risk assessment
		PM-02.2B	Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of Complementary Subservice Organization Controls (CSOC) to be implemented by the subservice provider.	Q1-PM-02.2B	Following the risk assessment of a subservice provider, does the CSP define a list of Complementary Subservice Organization Controls (CSOC) to be implemented by the subservice provider?	- Documented list of Complementary Subservice Organization Controls
		PM-02.3B	The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available to the CSP assurance information supporting the assessment of their suitability for the targeted evaluation level.	Q1-PM-02.3B	Does the CSP ensure that the subservice provider has implemented the CSOCs?	- Subservice provider CSOC documented implementation results review - Audit report to the Subservice provider

		PM-02.4B	The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.	Q1-PM-02.4B	Is the adequacy of the risk assessment reviewed regularly?	- Documented risk assessment review records (2/3 years)
PM-03	DIRECTORY OF SUPPLIERS	PM-03.1B	The CSP shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the cloud service.	Q1-PM-03.1B	Does the CSP maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the cloud service?	- Centralised directory of suppliers
		PM-03.2B	The CSP shall verify the directory for completeness, accuracy and validity at least annually.	Q1-PM-03.2B	Do the CSP shall verify the directory for completeness, accuracy and validity?	- Directory audit report
PM-04	MONITORING OF COMPLIANCE WITH REQUIREMENTS	PM-04.1B	The CSP shall monitor the compliance of its suppliers with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties.	Q1-PM-04.1B	Does the CSP monitor the compliance of its suppliers with information security requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties?	- Documented compliance report of the monitoring
				Q2-PM-04.1B	Does the CSP monitor the compliance of its suppliers with applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties?	- Documented compliance report of the monitoring
		PM-04.2B	The CSP shall monitor the compliance of its subservice providers with the CSOCs applicable to them following the risk assessment (cf. PM-02).	Q1-PM-04.2B	Does the CSP monitor the compliance of its subservice providers with the CSOCs applicable to them following the risk assessment?	- Documented compliance report of the monitoring
		PM-04.3B	The frequency of the monitoring shall correspond to the classification of the third party based on the risk assessment conducted by the CSP (cf. PM-02), and the results of the monitoring shall be considered in the review of the third party's risk assessment.	Q1-PM-04.3B	Does the frequency of the monitoring correspond to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider?	- Documented compliance report of the monitoring version control and change history

				Q2-PM-04.2b	Are the results of the monitoring included in the review of the third party's risk assessment?	- Documented review of the third party's risk assessment
		PM-04.4B	Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf. RM-01).	Q1-PM-04.4B	Are Identified violations and deviations analysed, in accordance with the risk management procedure?	- Documented review of the Identified violations and deviations management
				Q2-PM-04.4B	Are Identified violations and deviations evaluated in accordance with the risk management procedure?	- Documented review of the Identified violations and deviations management
				Q3-PM-04.4B	Are Identified violations and deviations treated in accordance with the risk management procedure?	- Documented review of the Identified violations and deviations management
		PM-04.5B	When a change in a third-party contributing to the provision of the cloud service affects its level of security, the CSP shall inform all of its CSCs without undue delay.	Q1-PM-04.5B	Does the CSP shall inform all of its CSCs without undue delay when a change in a third-party contributes to the delivery of the cloud service affects its level of security?	- Intranet/WEB - email - etc.
PM-05	EXIT STRATEGY	PM-05.1B	The CSP shall define exit strategies for the purchase of products or services where the risk assessment of the suppliers identified a very high dependency.	Q1-PM-05.1B	Does the CSP define exit strategies for the purchase of services where the risk assessment of the suppliers identified a very high dependency?	- Documented exit strategies for the purchase of services

13.15 Incident Management

Table 29. Checklist for IM basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
IM-01	POLICY FOR SECURITY	IM-01.1B	The CSP shall define and implement policies and procedures according to ISP-02 containing technical and organisational safeguards to	Q1-IM-01.1B	Are all known security incidents documented?	- Documented security incidents - Guidelines for the

	INCIDENT MANAGEMENT		ensure a fast, effective and proper response to all known security incidents, including: (1) Guidelines for the classification, prioritization, and escalation of security incidents; (2) Description of interfaces for incident management and business continuity management.			classification, prioritization, and escalation of security incidents; - Description of interfaces for incident management and business continuity management. - Security incidents communicated (a sample)
				Q2-IM-01.1B	Does the CSP document policies and procedures containing technical and organisational safeguards to ensure a response to all known security incidents?	- Documented policies and procedures about security incidents management
				Q3-IM-01.1B	Does the documented technical and organisational safeguards ensure a fast, effective and proper response to all known security incidents?	- Technical and organisational safeguards assessment result
				Q4-IM-01.1B	Are the previous policies and procedures aligned with the ISP-02 policy (Global Security Policy) and do they include: • Guidelines for the classification, prioritization, and escalation of security incidents; • Description of interfaces for incident management and business continuity management?	- Cross References between Global Security Policy and Security Incident management Policy
				Q5-IM-01.1B	Are the previous policies and procedures implemented?	- Example of policy/procedures implementation randomly sampled
		IM-01.2B	The CSP shall establish a point of contact, which contributes to the coordinated resolution of security incidents.	Q1-IM-01.1B	Has the CSP established a point of contact, for a coordinated resolution of security incidents?	- Contact point's name
IM-02	PROCESSING OF SECURITY INCIDENTS	IM-02.1B	The CSP shall classify and prioritize security events that could constitute a security incident, and perform root-cause analyses for these	Q1-IM-02.1B	For the events that could constitute a security incident, does the CSP perform root-cause analysis?	- Security Incidents database - Root-Cause Analysis result

			events, using their subject matter experts and external security providers where appropriate.			document -Root-cause analysis
IM-03	DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS	IM-03.1B	The CSP shall document the implemented measures after a security incident has been processed and, in accordance with contractual agreements between CSC and CSP, information shall be made available to the affected CSCs for final acknowledgment or, if applicable, as confirmation.	Q1-IM-03.1B	Does the CSP document the implemented measures after a security incident has been processed and, in accordance with contractual agreements between CSC and CSP?	- Documented measures derived from the root-cause analysis
				Q2-IM-03.1B	Is the information made available to the affected CSCs for final acknowledgment or, if applicable, as confirmation?	- Security Incident newsletter/document for the customers
		IM-03.2B	The CSP shall make information on security incidents or confirmed security breaches available to all affected CSCs.	Q1-IM-03.2B	Does the CSP make information on security incidents or confirmed security breaches available to all affected customers?	Information mechanism used - WEB - email - Specific meetings minutes - etc.
				Q2-IM-03.2B	Does the CSP send information of security incidents to all the documented affected customers?	- Security Incident Newsletter for each affected customer
IM-04	USER'S DUTY TO REPORT SECURITY INCIDENTS	IM-04.1B	The CSP shall inform employees and external business partners of their contractual obligations to report all security events that become known to them and are directly related to the cloud service.	Q1-IM-04.1B	Does the CSP inform employees of their contractual obligations to report all security events that become known to them and are directly related to the cloud service?	Information mechanism used -Intranet/WEB -email - Wallchart - Specific meetings minutes - etc.
				Q2-IM-04.1B	Does the CSP inform external business partners of their contractual obligations to report all security events that become known to them and are directly related to the cloud service?	Information mechanism used -Intranet/WEB -email - Wallchart - Specific meetings minutes - etc.

		IM-04.2B	The CSP shall not take any negative action against those who report in good faith events that do not subsequently turn out to be incidents and shall make that policy known as part of its communication to employees and external business partners.	Q1-IM-04.2B	Does the security incident management policy contain an explicit mention that the CSP not take any negative action against those who communicate "false reports" of events that do not subsequently turn out to be incidents?	- Security incident management policy
				Q2-IM-04.2B	Is the previous policy communicated to employees?	Information mechanism used - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q3-IM-04.2B	Is the previous policy communicated to external business partners?	Information mechanism used - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
		IM-04.3B	The CSP shall define, publish and implement a single point of contact to report security events and vulnerabilities.	Q1-IM-04.3B	Has the CSP established a single point of contact to report security events?	Documented Role and Responsibilities related to the Security Incidents Manager/Collector
				Q2-IM-04.3B	Is the single point of contact made public?	Information mechanism used - Intranet/WEB - email - Wallchart - Specific meetings minutes - etc.
				Q3-IM-04.3B	Is the single point of contact operative?	- List of security incident received and managed by the single point of contact
IM-05	INVOLVEMENT OF CLOUD CUSTOMERS IN	IM-05.1B	The CSP shall periodically inform its CSCs on the status of the security incidents affecting the CSC, or, where appropriate and necessary,	Q1-IM-05.1B	Does the CSP periodically inform its CSCs on the status of the incidents affecting the CSC?	- Security Incident Newsletter / periodic communication to customers

	THE EVENT OF INCIDENTS		involve them in the resolution, according to the contractual agreements			
				Q2-IM-05.1B	Where appropriate and necessary, does the CSP involve customers in the incidents' resolution according to the contractual agreements?	- Requests of participations in incidents analysis - Contractual Agreements
		IM-05.2B	As soon as a security incident has been closed, the CSP shall inform the affected CSCs about the actions taken, according to the contractual agreements.	Q1-IM-05.2B	As soon as an incident has been closed, does the CSP inform the customers about the actions taken, according to the contractual agreements?	- Security Incident Newsletter - Contractual Agreements
IM-06	EVALUATION AND LEARNING PROCESS	IM-06.1B	The CSP shall perform an analysis of security incidents to identify recurrent or significant security events or incidents and to identify the need for further protection, if needed with the support of external bodies.	Q1-IM-06.1B	Does the CSP perform a security incidents analysis to identify recurrent and/or significant incidents?	- Security Incident Data Base with the classification of recurrent and significant incidents
				Q2-IM-06.1B	In case of recurrent or significant incidents detected, does the CSP identify need for further protection?	- Documented further protection associated to recurrent and significant incidents
				Q3-IM-06.1B	Does the CSP involve external bodies if necessary?	- Contracts with external bodies
		IM-06.2B	If the CSP determines the need for external assistance, it shall select a competent and trustworthy incident response service provider or one that is recommended by its NCCA.	Q1-IM-06.2B	If the CSP determines the need for external assistance, is selected a competent and trustworthy incident response service provider or one that is recommended by its NCCA?	- Qualifications of the contracted external bodies
IM-07	INCIDENT EVIDENCE PRESERVATION	IM-07.1B	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents.	Q1-IM-07.1B	Does the CSP document a procedure to archive all documents and evidence that provide details on security incidents?	- Documented procedure to archive security incidents
				Q2-IM-07.1B	Is the previous documented procedure implemented?	- Example of security incidents documentation randomly selected

		IM-07.2B	The CSP shall implement security mechanisms and processes for protecting all the information related to security incidents in accordance with criticality levels and legal requirements in effect.	Q1-IM-07.2B	Does the CSP implement security mechanisms and processes for protecting all the information related to security incidents?	- Example of security mechanisms and processes for protecting all the information related to security incidents randomly sampled
				Q2-IM-07.2B	Are the implemented security mechanism and processes in accordance with criticality levels and legal requirements in effect	- Audit records

13.16 Business Continuity

Table 30. Checklist for BC basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
BC-01	BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY	BC-01.1B	The CSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure business continuity and contingency management.	Q1-BC-01.1B	Has the CSP documented policies and procedures to ensure business continuity and contingency according to ISP-02?	- Documented policies and procedures related to business continuity and contingency
				Q2-BC-01.1B	Does the documented policies and procedures establish the strategy and guidelines to ensure business continuity and contingency?	- Documented policies and procedures related to business continuity and contingency (encompass the strategy and guidelines to ensure business continuity and contingency)
BC-02	BUSINESS IMPACT ANALYSIS PROCEDURES	BC-02.1B	The policies and procedures for business continuity and contingency management shall include the need to perform a business impact analysis to determine the impact of any malfunction to the cloud service or enterprise.	Q1-BC-02.1B	Does the CSP document all the possible malfunction to the cloud service or enterprise?	- Documented list of all the possible malfunction to the cloud service or enterprise

				Q2-BC-02.1B	Does the business continuity and contingency management policies and procedure contain the need to perform a business impact analysis related to all the documented malfunctions?	- Business continuity and contingency management policies and procedures (encompass the need to perform a business impact analysis related to all the documented malfunctions)
BC-03	BUSINESS CONTINUITY AND CONTINGENCY PLANNING	BC-03.1B	The CSP shall document and implement a business continuity plan and contingency plans to ensure continuity of the services, taking into account information security constraints and the results of the business impact analysis.	Q1-BC-03.1B	Does the CSP document a business continuity plan?	- Business Continuity Plan
				Q2-BC-03.1B	Does the CSP document a contingency plan to ensure continuity of the services?	- Contingency Plan
				Q3-BC-03.1B	Does the documented business continuity plan consider information security constraints and the results of the business impact analysis?	- Business Continuity Plan (encompasses information security constraints and the results of the business impact analysis) - Business Continuity Plan review
				Q4-BC-03.1B	Does the documented contingency plan consider information security constraints and the results of the business impact analysis?	- Contingency Plan (encompasses information security constraints and the results of the business impact analysis) - Contingency Plan Review
				Q5-BC-03.1B	Does the CSP implement the business continuity plan?	- According with the business continuity plan requirements, execution evidence randomly selected
				Q6-BC-03.1B	Does the CSP implement the contingency plan?	- According with the contingency plan requirements, execution evidence randomly selected

13.17 Compliance

Table 31. Checklist for CO basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
CO-01	IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS	CO-01.1B	The CSP shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service.	Q1-CO-01.1B	Does the CSP document the legal requirements relevant to the information security of the cloud service?	- Documented list of requirements (encompasses the legal requirements relevant to the information security of the cloud service) - Documented review of the list of requirements
				Q2-CO-01.1B	Does the CSP document the regulatory requirements relevant to the information security of the cloud service?	- Documented list of requirements (the regulatory requirements relevant to the information security of the cloud service) - Documented review of the list of requirements
				Q3-CO-01.1B	Does the CSP document the self-imposed requirements relevant to the information security of the cloud service?	- Documented list of requirements (encompasses the self-imposed requirements relevant to the information security of the cloud service) - Documented review of the list of requirements
				Q4-CO-01.1B	Does the CSP shall document the contractual requirements relevant to the information security of the cloud service?	- Documented list of requirements (encompasses the contractual requirements relevant to the information security of the cloud service) - Documented review of the list of requirements

CO-02	POLICY FOR PLANNING AND CONDUCTING AUDITS	CO-02.1B	The CSP shall define and implement policies and procedures for planning and conducting audits, made in accordance with ISP-02 and that would not interfere with the operation of the cloud service.	Q1-CO-02.1B	Does the CSP define policies and procedures for planning and conducting audits?	- Audit policy document - Audit planning and conducting procedures
				Q2-CO-02.1B	Does the CSP implement policies and procedures for planning and conducting audits?	- Audit plan - Audit report - Documented list of nonconformities
CO-03	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	CO-03.1B	The CSP shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control system to the requirements defined in CO-01, and to the requirements of the EUCS scheme at the targeted evaluation level.	Q1-CO-03.1B	Does the CSP perform audits to check the compliance of their internal security control system to the requirements defined?	- Audit plan - Audit report - Documented list of nonconformities
				Q2-CO-03.1B	Are the internal audits performed by subject matter experts?	- Internal auditor's training records
				Q3-CO-03.1B	Are the internal audits performed at least annually?	- Documented audit plan
				Q4-CO-03.1B	Does the internal audit check the compliance to the requirements defined in CO1 and to the requirements of the EUCS scheme at the targeted evaluation level?	- Internal audit reports and/or checklist aligned with EUCS scheme at the targeted evaluation level
		CO-03.2B	The CSP shall document specifically deviations that are nonconformities from the EUCS requirements, including an assessment of their severity, and keep track of their remediation.	Q1-CO-03.2B	Does the CSP document specifically deviations that are nonconformities from the EUCS requirements?	- Audit report - Documented list of deviations that are nonconformities from the EUCS requirements
				Q2-CO-03.2B	Do the documented deviations include an assessment of their severity?	- Documented list of deviations including an assessment of their severity
				Q3-CO-03.2B	Does the CSP keep track of their remediation?	- Monitoring report of the non-conformities from the EUCS requirements remediation

CO-04	INFORMATION ON INTERNAL CONTROL SYSTEM ASSESSMENT	CO-04.1B	The CSP shall regular inform its top management about the information security performance within the scope of the internal control system.	Q1-CO-04.1B	Does the CSP regular inform its top management about the information security performance within the scope of the internal control system?	<ul style="list-style-type: none"> - Information security performance report to top management - email - Another specific document
--------------	--	-----------------	---	--------------------	--	---

13.18 User documentation

Table 32. Checklist for DOC basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
DOC-01	GUIDELINES AND RECOMMENDATIONS FOR CLOUD CUSTOMERS	DOC-01.1B	The CSP shall make publicly available guidelines and recommendations to assist the cloud service users with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided.	Q1-DOC-01.1B	Does the CSP make publicly available guidelines and recommendations to assist the Cloud Service Users?	<ul style="list-style-type: none"> - Guidelines - Distribution mechanism: - Information management system - Intranet/WEB - etc.
		DOC-01.2B	The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use.	Q1-DOC-01.2B	Does the CSP maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use?	<ul style="list-style-type: none"> - Guidelines and recommendations version control and change history
DOC-02	ONLINE REGISTER OF KNOWN VULNERABILITIES	DOC-02.1B	The CSP shall provide comprehensible and transparent information on: (1) Its jurisdiction; and (2) System component locations, including its subservice providers, where CSC data is processed, stored and backed up.	Q1-DOC-02.1B	Does the CSP operate or refer to a publicly available online register of known vulnerabilities that affect the provided cloud service?	<ul style="list-style-type: none"> - Online register of known vulnerabilities (Web, e-mail)
				Q2-DOC-02.1B	Is the online register of known vulnerabilities daily updated?	<ul style="list-style-type: none"> - Web page updated date - e-mail sent date

		DOC-02.2B	The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective.	Q1-DOC-02.2B	Does the CSP provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective?	- Contractual agreement
DOC-03	LOCATIONS OF DATA PROCESSING AND STORAGE	DOC-03.1B	The CSP shall provide a justification for the evaluation level targeted for certification, based on the risks associated to the cloud service's targeted customers and use cases.	Q1-DOC-03.1B	Does the CSP provide comprehensible and transparent information on its jurisdiction?	-Contractual agreement: it indicates the location and the jurisdiction, explicitly - Web - Service catalogue - e-mail
				Q2-DOC-03.1B	Does the CSP provide comprehensible and transparent information on system component locations?	- Web - Service catalogue - e-mail -Contractual agreement: it indicates the location and the jurisdiction, explicitly
				Q3-DOC-03.1B	Does the CSP provide comprehensible and transparent information on its subcontractors?	-Web - Service catalogue - e-mail -Contractual agreement: it indicates the location and the jurisdiction, explicitly
				Q4-DOC-03.1B	Does the CSP provide comprehensible and transparent information on where the cloud customer's data is processed, stored and backed up?	-Web - Service catalogue - e-mail -Contractual agreement: it indicates the location and the jurisdiction, explicitly

				Q5-DOC-03.1B	Does the CSP provide comprehensible and transparent information about the on where the cloud customer's data is processed, stored and backed up?	Service Catalogue Other internal Documentation -Contractual agreement: it shall indicate where the data is processed, stored and backed up
		DOC-03.2B	If the CSP claims compliance to extension profiles for its cloud service, the justification shall cover these extension profiles.	Q1-DOC-03.2B	Does the CSP provide sufficient information for subject matter experts of the CSC to determine to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective?	Service Catalogue Other internal Documentation -Contractual agreement: it shall indicate where the data is processed, stored and backed up
		DOC-03.3B	A summary of the justification shall be made publicly available as part of the certification package, which shall allow CSCs to perform a high-level analysis about their own use cases.	Q1-DOC-03.3B	Is there a summary of the justification made publicly available as part of the certification package?	- Public repository with the summary of the justification
DOC-04	JUSTIFICATION OF THE TARGETED ASSURANCE LEVEL	DOC-04.1B	If a CSP wants to allow CSCs to certify with EUCS their own cloud services based on the CSP's cloud service using composition, the CSP shall develop specific documentation and make it available to CSCs upon request, based on the complementary user entity controls (CUECs) that they have defined.	Q1-DOC-04.1B	If a CSP wants to allow CSCs to certify with EUCS their own services based on the CSP's cloud service using composition, does the CSP develop specific documentation based on the Complementary User Customer Controls (CUECs) that they have defined?	- Documented specific documentation
				Q2-DOC-04.1B	Does the CSP make documentation available to CSCs upon request?	- Requests for specific documentation by the CSC - Records showing that the documentation has been sent to the CSC.
		DOC-04.2B	The CSP shall include in the description provided for each CUEC a list of actionable requirements for the CSC, and it shall associate each CUEC to an EUCS requirement.	Q1-DOC-04.2B	Does the CSP include in the description provided for each CUEC a list of actionable requirements for the CSC?	- Documented list of actionable requirements

				Q2-DOC-04.2B	- Each CCC is associated with an EUCS requirement.	- Traceability between each CCC to an EUCS requirement
DOC-05	GUIDELINES AND RECOMMENDATIONS FOR COMPOSITION	DOC-05.1B	If a CSP wants to allow CSCs to certify with EUCS their own services based on the CSP's cloud service using composition, it shall document for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of this requirement by the cloud service developed by the CSC using the CSP as subservice provider.	Q1-DOC-05.1B	If a CSP wants to allow CSCs to certify with EUCS their own services based on the CSP's cloud service using composition, it documents for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of the requirement by the cloud service developed by the CSC using the CSP as subservice provider.	- Documentation for each EUCS requirement on how its cloud service (if any) will contribute to the fulfilment of the requirement through the cloud service developed by the CSC using the CSP as a subservice organization.
		DOC-05.2B	The CSP shall make this documentation available to CSCs upon request.	Q1-DOC-05.2B	Does the CSP make this documentation available to CSCs upon request?	- CSS documentation request - Record of submission of the required documentation - e-mail - other

13.19 Dealing with Investigation Requests from Government Agencies

Table 33. Checklist for INQ basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
INQ-01	LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRIES	INQ-01.1B	The CSP shall subject investigation requests from government agencies to a legal assessment by subject matter experts.	Q1-INQ-01.1B	Does the CSP execute a legal assessment of every investigation request received from government agencies?	- Legal assessment results
				Q2-INQ-01.1B	Is the assessor and expert of the subject matter?	- Assessor documented qualifications
		INQ-01.2B	The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken.	Q1-INQ-01.2B	Does the government agency that sent the request has an applicable and legally valid basis?	- Foundations of the government agency

				Q2-INQ-01.2B	Does the legal assessment results contain the further steps need to be taken in response of the investigation request received?	- Legal assessment results (contain the further steps need to be taken in response of the investigation request received)
INQ-02	INFORMING CLOUD CUSTOMERS ABOUT INVESTIGATION REQUESTS	INQ-02.1B	The CSP shall inform the affected CSC(s) about investigation requests without undue delay unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	Q1-INQ-02.1B	Does the CSP inform without undue delay the affected CSC(s) about the received investigation requests?	- Documented notice sent to every CSC affected by the investigation request. This document must include the delivery date
				Q2-INQ-02.1B	In case CSP did not inform the affected CSC(s) was because the applicable legal basis on which the government agency is based prohibits this or because there are clear indications of illegal actions in connection with the use of the cloud service?	- Investigation Request + Legal Assessment Results
INQ-03	CONDITIONS FOR ACCESS TO OR DISCLOSURE OF DATA IN INVESTIGATION REQUESTS	INQ-03.1B	The CSP shall only provide access to or disclose CSC data in the context of government investigation requests after the CSP's legal assessment (cf. INQ-01) has shown that an applicable and valid legal basis exists, and that the investigation request must be granted on that basis.	Q1-INQ-03.1B	Has the CSP provided access to or disclose CSC data to government agency only after the legal assessment has shown that an applicable and valid legal basis exists?	- Record of the data in which CSP has provided access to customer data to the government agency - Assessment Results
		INQ-03.2B	The CSP shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate.	Q1-INQ-03.2B	Does the CSP document procedures to ensure that government agencies only have access to the data they need to investigate?	- Documented procedure that describe the mechanism to provide access to customer data to government agency by limiting the scope to only that data they need to investigate according to the investigation request
				Q2-INQ-03.2B	Does the CSP implement the documented procedures to ensure that government agencies only have	- Examples of Investigation Requests+Data needed for the investigation+evidence that the

					access to the data they need to investigate?	access has been authorized ONLY to that data
--	--	--	--	--	--	--

13.20 Product Safety and security

Table 34. Checklist for PSS basic assurance requirements (source: MEDINA's own contribution)

Control ID	Control	ReqID	Requirement	Question ID	Statement/Questions	Evidence
PSS-01	ERROR HANDLING AND LOGGING MECHANISMS	PSS-01.1B	The CSP shall offer to their CSCs error handling and logging mechanisms that allow them to obtain security-related information about the status of the cloud service as well as the data, services or functions it provides.	Q1-PSS-01.1B	Does the CSP offer to their CSCs error handling mechanisms?	- Error handling mechanism instantiated to every customer
				Q2-PSS-01.1B	Does error handling mechanisms allow customers to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides?	- Operation manual of the error handling mechanism
				Q3-PSS-01.1B	Does the CSP offer to their CSCs logging mechanisms?	- Logging mechanism instantiated to every customer
				Q4-PSS-01.1B	Does logging mechanisms allow customers to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides?	- Operation manual of the logging mechanism
PSS-02	SESSION MANAGEMENT	PSS-02.1B	A state-of-the-art session management system shall be used that is suitably protected against known attacks.	Q1-PSS-02.1B	Is a state-of-the-art session management system used? Is it protected against known attacks?	- Session management system description (functional)
PSS-03	SOFTWARE DEFINED NETWORKING	PSS-03.1B	The CSP shall document and implement procedures to ensure the confidentiality of CSC data when offering functions for software-defined networking (SDN).	Q1-PSS-03.1B	Does the CSP document procedures to ensure the confidentiality of CSC data when offering functions for	- Documented procedures

					software-defined networking (SDN).?	
				Q2-PSS-03.1B	Does the CSP implement the procedures to ensure the confidentiality of CSC data when offering functions for software-defined networking (SDN).?	- Audit
		PSS-03.2B	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features.	Q1-PSS-03.2B	Does the CSP validate the functionality of the SDN functions before providing new SDN features to CSCs?	- Validation Report
PSS-04	IMAGES FOR VIRTUAL MACHINES AND CONTAINERS	PSS-04.1B	The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: The CSC can restrict the selection of images of virtual machines or containers, so that users of this CSC can only launch the images or containers released according to these restrictions. Images made available by the CSP to the CSC are labelled with information about their origin (CSP or third-party) and about their security, and those provided by the CSP are hardened according to generally accepted industry standards.	Q1-PSS-04.1B	When the CSC operates virtual machine, does the CSP ensure that the CSC can restrict the selection of images of virtual machines according to its specifications?	-Authorization authentication procedures to access containers and the registry where they are stored
				Q2-PSS-04.1B	When the CSC operates container, does the CSP ensure that the CSC can restrict the selection of images of containers according to its specifications?	-Authorization authentication procedures to access containers and the registry where they are stored
				Q3-PSS-04.1B	Are the mages made available by the CSP to the CSC labelled with information about their origin (CSP or third-party)?	- Images origin information

				Q-PSS-04.1B	Are the images provided by the CSP hardened according to generally accepted industry standards?	- Use of generally accepted industry standards for securing images (e.g. CIS Hardened images, DISA STIG, NIST SP 800-190, ...)
--	--	--	--	--------------------	---	--