Deliverable D2.2

Continuously certifiable technical and organizational measures and Catalogue of cloud security metrics-v2

Editor(s):	Iñaki Etxaniz, Juncal Alonso
Responsible Partner:	Fundación TECNALIA Research and innovation
Status-Version:	Final – v1.0
Date:	31.01.2023
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v2
Due Date of Delivery to the EC	31.01.2023

Workpackage responsible for the Deliverable:	WP2 - Certification Metrics and Specification Languages
Editor(s):	Iñaki Etxaniz, Juncal Alonso (TECNALIA)
Contributor(s):	TECNALIA, CNR, Bosch, FhG, Fabasoft, HPE, XLAB
Reviewer(s):	Christian Banse (FhG) Cristina Martínez (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	WP2, WP3, WP4, WP5

Abstract:	This is the second and last deliverable presenting the definition of the technical and organizational measures relevant for CSPs along with a set of security metrics (both quantitative and qualitative) for such security objectives. These measures will be expressed also in the form of a Catalogue of comprehensible cloud security metrics. This deliverable is the result of Task 2.1 and Task 2.2.
Keyword List:	Security metrics, Reference Technical and organizational measures, security requirements, draft candidate EU Cloud Services certification scheme (EUCS), security catalogue
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	15.11.2022	Table of Contents Chapter 5 (Catalogue)	Iñaki Etxaniz (TECNALIA)
v0.2	16.12.2022	Extended chapter 2. Mapping	Iñaki Etxaniz (TECNALIA)
v0.3	10.01.2023	Chapter 3. TOMs	Juncal Alonso (TECNALIA)
v0.4	15.01.2023	Completed chapter 4 (Metrics) Sent for internal review	TECNALIA, FhG, Fabasoft, XLAB
v0.5	25.01.2023	Addressed all comments received in the Internal QA review	Iñaki Etxaniz (TECNALIA)
v1.0	31.01.2023	Final QA review and changes. Ready for submission	Cristina Martínez (TECNALIA)

Table of contents

List of tables

List of figures

Terms and abbreviations

AICPA	Association of International Certified Professional Accountants
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AM	Asset Management
AMOE	Assessment and Management of Organisational Evidence
API	Application Programming Interface
AWS	Amazon Web Services
BC	Business Continuity
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Conformance Assessment Body
CCF	Cloud Controls Framework
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
CSA or EU CSA	EU Cybersecurity Act
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic application security testing
DEV	Development of Information Systems
DoA	Description of Action
DOC	User Documentation
EC	European Commission
ENISA	European Union Agency for Cybersecurity
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
IEC	International Electrotechnical Commission
IM	Incident Management
INQ	Dealing with Investigation requests from government agencies
IRAP	Information Security Registered Assessors Program
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ISP	Information Security Policies

JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KR	Key Result
IT	Information Technologies
KPI	Key Performance Indicator
MFA	Multi-factor Authentication
NDA	Non-Disclosure Agreement
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
RPO	Recovery Point Objective
RTO/RPO	Recovery Time Objective
RM	Risk Management
SaaS	Software as a Service
SIEM	Security Information and Event Management
SFC	Security Framework Control
SLA	Service Level Agreement
SOC	System and Organization Controls
SQL	Structured Query Language
TCDP	Trusted Cloud Data Protection Profile
TOM	Technical and Organizational Measure
TSC	Trust Services Principles
UI	User Interface
VAT	Vulnerability Assessment Tools
VM	Virtual Machine

Executive Summary

This deliverable presents the second and final version of the *Catalogue of Controls and Metrics*, defined as the KR1 in MEDINA project. The document is based on and shares the same structure than its predecessor D2.1 [1], although many parts have been updated or added. Due to this, with the goal to provide a self-contained deliverable that facilitates the reader´s understanding, part of the content of the original document has been included.

This document, delivered in M27, contains updated versions of the security controls mapping adapted to the evolution of the EUCS scheme since the first version was presented in D2.1, new and updated Technical and Organizational Measures (TOMs), as well as new and updated metrics. It also includes the final version of the *Catalogue of Controls and Metrics* software component.

The document starts with a comparative analysis of five security schemes: EUCS, ISO/IEC 27000 family (27002, 27017), BSI C5, SecNumCloud, and Cisco CCF. This comparison is based on different dimensions such as categories, structure, levels and conformity assessment method, as well as on the mapping of the controls. The aim of this mapping is to allow a smoother transition from one scheme to another and to facilitate the reuse of evidence whenever possible.

The second goal of this document is to present an updated set of Reference TOMs for the 34 requirements with the assurance level high (“the 34”) identified in the August 2022 version of the European candidate draft EUCS [2]. A Reference TOM is a sort of implementation guidance that is vendor and technology agnostic. They are aimed at small and medium CSPs aiming at the assurance level high, and are used as input by the MEDINA certification language for the creation of their corpus of data.

The third goal is the definition of the MEDINA catalogue of security metrics, which are the core of the project as other MEDINA tools rely on them. More than 150 metrics have been elicited at this stage, coming from literature and other European projects, but also from the MEDINA partners themselves. Among these metrics, 54 are defined for “the 34” high level EUCS requirements selected by MEDINA. All metrics have been described following the same structure, which includes the defined data type, data range, interval, and formula (for more details, check *Appendix 2: MEDINA Security metrics*). Although most metrics are directly linked to a “high” assurance level requirement, there are some that have a more general purpose or fulfil a lower assurance level requirement.

Finally, the document includes the functional and technical design of the second version of the software implementation of the *Catalogue of Controls and Metrics*. It details how it fits into the MEDINA framework, its architecture, data model, sequence diagrams and installation instructions. A complete user manual is also included.

The deliverable includes four appendices complementing the previous sections.

This document is tightly related with other activities that are currently on-going in MEDINA such as the certification language, including the metric recommender, the ontology and rules, the evidence management tools and the continuous evaluation tools.

1. Introduction

1.1. About this deliverable

This document is the second iteration of two and aims at presenting a Catalogue of controls and metrics, which is defined as the Key Result 1 (KR1) in MEDINA. This deliverable builds on the previous version, D2.1 [1], which was presented in M12, with the required updates following the work done so far in tasks T2.1 and T2.2 until now, M27.

1.2. Document structure

The document is structured as follows. Section 2 presents an overview of five schemes, namely the European candidate EU Cloud Services certification scheme (EUCS) in its draft version of August 2022[1], ISO/IEC 27000, BSI C5, SecNumCloud and the Cisco Cloud Common Framework (CCF). This is followed by a comparative analysis in terms of control categories, structure, and conformity assessment method of these schemes. Finally, a mapping between the security controls of the aforementioned schemes is provided.

Section 3 presents an updated version of the 34 high-level assurance requirements of the EUCS August-2022 version [2] that require "continuous (automated)" monitoring and provides Reference Technical and Organizational Measures (TOMs) for them. A Reference TOM can be considered as an explanation of how a specific EUCS security requirement can be implemented, in a vendor– and technology-agnostic way, to comply with the scheme. The details of these 34 requirements can be found in *Appendix 1: Security Requirements relevant for continuous assessment – Description.*

Section 4 presents the security metrics for the continuous cloud certification which are relevant for the automated monitoring tools of MEDINA. The section includes the motivation, the sources where MEDINA has collected the metrics and the structure of the metrics. Most of the metrics elicited correspond to the 34 high level EUCS requirements selected by MEDINA, but some additional metrics for other requirements deemed relevant for the continuous monitoring or operational effectiveness have been also defined. Finally, the coverage of the metrics by the MEDINA tools is also presented. The complete description of metrics can be found in *Appendix 2: MEDINA Security metrics*.

Section 5 describes the second version of a software tool named *Catalogue of Controls and Metrics*, which brings together the implementation of all the elements described in the previous sections. The section includes the functional and technical description, the architecture, the data model, and includes a detailed user manual. It extends the information provided in D5.2 [3].

Section 6 concludes this deliverable.

The Appendices present more detailed information of the main issues of the document, which for reasons of space are not included in the chapters. Namely, the details of "the 34" requirements, the list and details of the elicited metrics, the mapping of controls between schemes extended by Cisco CCF, and the MEDINA Glossary.

1.3. Updates from D2.1

This deliverable evolves from D2.1 [1], so it shares the same basic structure. With the ultimate goal of providing a self-contained deliverable that facilitates the reader´s understanding, part of its content is common to that included in the previous document. In order to facilitate the

[1] 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.

tracking of developments with respect to the previous version, Table 1 shows a brief summary of the changes and additions to each of the sections of the document.

Table 1. Overview of deliverable updates with respect to D2.1 [1]

Section	Change
Section 2	Cisco CCF has been added to the list of schemes and standards compared (cf. Section 2.1.5), and has been included in the mapping of the controls (cf. Section 2.2).
Section 3	The list of TOMs or requirements for continuous assessment (cf. Section 3.1) has been updated, adapting it to the most recent EUCS scheme of August 2022 [2]. Some high level requirements have been dropped and new ones have been added, resulting in a total of 34 requirements. The Reference TOM section has been also updated and completed (cf. Section 3.3).
Section 4	The list of security metrics has been revamped according to the reformulation of MEDINA KPIs in July 2022. In this version 54 metrics have been implemented for "the 34" requirements and are measurable. The section also includes a list of Techniques defined in WP3 to complete the metrics. A table that updates the coverage of the requirements by tool, previously elicited in D3.2 [4], is also included.
Section 5	The whole section has been updated with the description of the final version of the *Catalogue of Controls and Metrics* tool. The functional description (cf. Section 5.1) includes the new set of requirements. The technical description (cf. Section 5.2) includes the final version of the architecture and interactions of the Catalogue. The Delivery and usage chapter (cf. Section 5.3) includes installation instructions and a complete user manual.
Appendix 1	The details of the 34 high level assurance requirements of the EUCS August-2022 version [2] have been updated.
Appendix 2	The list of MEDINA security metrics has been updated.
Appendix 3	An extended mapping for "the 34" using the Cisco CCF has been included.
Appendix 4	The glossary of MEDINA terms has been updated.

2. Mapping of Security Controls

One of the objectives of MEDINA is to provide a comprehensive repository of technical and organisational measures (TOMs) to address controls referenced in major standard frameworks. To achieve this, we have conducted an analysis of the main security schemes that are active at the time of writing, namely the European draft candidate EU Cloud Services certification scheme (EUCS) in its August 2022 version[2], the ISO/IEC 27000 family, BSI C5:2020, SecNumCloud and finally Cisco CCF, which has been added in this second version of the deliverable.

For each scheme or standard, the following items are presented:

- Categories, i.e., the domains that the scheme covers
- Structure of the scheme
- Conformity assessment method

The section then includes a table that summarises and compares the previously analysed schemes in various dimensions, and ends with a mapping of the security controls of the schemes and standards previously analysed. The aim of this mapping is to provide a guidance in the transitioning to the EUCS standard.

2.1. Compared Schemes and Standards

2.1.1. EU Cloud Services Certification Scheme (EUCS)

The European draft candidate EU Cloud Services certification scheme (EUCS) looks into the certification of cloud services. The EUCS version on which D2.1 [1] was based dated from December 2020 [5] but, as the scheme has evolved since then, this document has taken a more recent version - the August 2022 draft [2] - as the reference EUCS for MEDINA. Please note that at the time of writing, the EUCS draft is still evolving.

EUCS is the second certification scheme that is being created under the scope of the Cybersecurity Act (EU CSA) [6][3]. Following the request of the European Commission on November 2020 and in accordance to Article 48.2 of the EU CSA [6], ENISA created an ad-hoc working group consisting of 20 members [7] representing different stakeholders (e.g. industry, auditors, academia) to support them in the development of the European candidate scheme for cloud services.

EUCS draws from various sources such as the recommendations report from the expert group CSPCERT [8], BSI C5 [9], SecNumCloud [10], ISO standards [11] [12] [13], and ISAE [12] [14], among others.

EUCS follows the three levels proposed in the Article 52(6) of the EU CSA, namely ‘basic’, ‘substantial’ and ‘high’. In this scheme, this is achieved through the security requirements on the cloud services and on their assessment as they increase with levels in several dimensions: scope, rigour and depth. The draft candidate [2] states that “*the requirements at level ‘high’ are demanding and close to the state-of-the-art, and may therefore serve to protect the most sensitive cases of cloud usage, including those closely associated to national security or very sensitive businesses where no real compromise to cybersecurity can be expected.* […] *On the other hand of the spectrum, the requirements at level ‘basic’ define a minimum acceptable baseline for cloud cybersecurity. That baseline is nevertheless comprehensive, as it covers all*

[2] 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.

[3] The first one is the EUCC or Common Criteria, derived from SOG-IS.

major aspects of cloud security. […] *The 'substantial' level, in between, will serve to protect most business cases, and may be the most appropriate level for many applicants and their customers*".

Table 2 shows the categories and objectives defined in the draft EUCS [2].

Table 2. Categories and objectives of the controls from the draft EUCS August 2022 version

EUCS Category [2]	**EUCS Objective** [2]
Organisation of Information Security	Plan, implement, maintain, and continuously improve the information security framework within the organisation
Information Security	Policies and Procedures: Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements
Risk Management	Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the CSP
Human Resources	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.
Asset Management	Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle
Physical Security	Prevent unauthorised physical access and protect against theft, damage, loss, and outage of operations
Operational security	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Identity, authentication and access control management	Limit access to information and information processing facilities
Cryptography and key management	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information
Communication security	Ensure the protection of information in networks and the corresponding information processing systems
Portability and interoperability	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider
Change and configuration management	Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service
Development of information systems	Ensure information security in the development cycle of information systems
Procurement management	Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements
Incident management	Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents
Business continuity	Plan, implement, maintain and test procedures and measures for business continuity and emergency management
Compliance	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements
User documentation	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers
Dealing with investigation requests from government agencies	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data
Product safety and security	Provide appropriate mechanisms for cloud customers

In the case of EUCS, the structure of the scheme is as follows:

- Category title
- Category objective: statement of that category
- Control id and name
- Control objective: goal of that control
- Requirement id, description, and assurance level
- Implementation guidance, for now, only considered in some controls

With respect to the conformity assessment methodologies:

- For basic level: is based on a self-assessment methodology performed by the CSP whose results are then audited by a conformity assessment body (CAB). CSPs are not allowed to issue statements of conformity.
- For substantial and high: EUCS has defined an assessment approach that is compatible with both ISO/IEC 27000 series of standards (based on ISO/IEC 17065) and also with International Auditing Standards (ISAE 3402), allowing CSPs to easily integrate EUCS into their assurance strategy.

2.1.2. ISO/IEC 27000 family

The ISO/IEC 27000 family of standards are security norms that contain information about security best practices to develop, implement and maintain information security management systems (ISMS).

The following standards of the ISO/IEC 27000 family are relevant for the scope of MEDINA:

- ISO/IEC 27001 [12]: specifies the requirements to set up, implement and maintain an ISMS of an organization. Annex A of the standard contains the controls.
- ISO/IEC 27002 [11]: provides the guidelines and best practices for the implementation of the ISMS. It actually presents the controls for implementing the ISMS of ISO/IEC 27001. The controls are the same as in Annex A of ISO/IEC 27001, but also includes some implementation guidance.
- ISO/IEC 27017 [13]: extends the controls of ISO/IEC 27002 with controls applicable to cloud services.

Table 3 shows the categories of controls defined in ISO/IEC 27002 [11].

Table 3. ISO/IEC 27002 control categories and objectives

ISO/IEC 27002 Category [11]	**ISO/IEC 27002 Objective** [11]
Information security policies	Aims at providing policies for the management and review of information security.
Organization of information security	Aims at setting up roles and responsibilities for the information security, aspects related to segregation of duties as well as contact with stakeholders (e.g., authorities and interest groups), and remote working.
Human resource security	Define all aspects related to the policies and procedures related to human resources prior, during and after employment.
Asset management	Identify and document organizational assets as well as define and document the way in which these shall have to be used and handled.
Access control	Manage the access, rights, controls and authentication of users.
Cryptography	Cryptographic controls and key management.

ISO/IEC 27002 Category [11]	**ISO/IEC 27002 Objective** [11]
Physical and environmental security	Deal with the protection of secure areas and equipment.
Operations security	Related to the secure operations of operational procedures and responsibilities, malware and vulnerabilities, monitoring, and operational software.
Communications security	Aspects related to networks security management and information transfer.
System acquisition, development and maintenance	It entails the analysis, specification, and development and support of systems and application services. It includes also change and control management, testing, outsourcing and secure engineering principles.
Supplier relationship	Everything related to the protection of the organization's assets accessible by suppliers as well as the maintenance of an agreed level of information security and service delivery aligned with supplier agreements.
Information security incident management	Aims at defining an approach for an effective management of security incidents, events and weaknesses.
Business continuity	Plan, implement and review a business continuity policy and procedure.
Compliance	Identify any applicable legislation and contractual requirements that the organization must comply with.

The controls in ISO/IEC 27002 [11] are structured as follows:

- Control name
- Control objective: defines the statement that needs to be satisfied
- Implementation guidance: provides some support on how the control should be implemented to meet the control objective
- Other information: information that should be considered, such as legal aspects or reference to other sources such as other standards.

The conformity assessment method is based on ISO 17065 [15].

2.1.3. BSI C5

The German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik - BSI*) published in 2016 a Catalogue of controls[4] for cloud computing, often referred as C5 [16]. The goal of C5 is to be an "*aid for the customer providing a better overview for a higher level of security and avoiding redundant audits*".

C5 is based on known standards and schemes [17], such as ISO/IEC 27001:2017, ISO/IEC 27017:2015, ISO/IEC 27018:2014, CSA CCM v3.0.1, AICPA Trust services principles criteria 2017, TCDP - Version 1.0, and BSI IT-Grundschutz-Kompendium - Edition 2019. Moreover, C5 states [16] that for the definition of the requirements they used as baseline content coming from requirements from ANSSI Referentiel Secure Cloud 2.0, BSI IT Grundschutz Catalogueues 2014, BSI SaaS Sicherheitsprofile 2014, ISO/IEC 27001, CSA CCM v3.0.1, and TSP. C5 provides a mapping of their controls to international standards.

[4] While the original document from 2016 uses initially indistinctively the wording "controls or requirements" in p.5 to define the scope of the catalogue of C5, the remainder of the document uses "requirements".

BSI has aimed to document the requirements in a transparent manner so CSPs could perform a comparative analysis with their own security level. C5 is audited following the ISAE methodology [14] [18] by a public accountant where the result is a report.

C5 has released two versions of the catalogue of controls, one in 2016 and a second one in 2020, in preparation and response to the EU CSA. Table 4 presents the categories defined in C5:2020 [9], which is the version considered in MEDINA during the mapping process (cf. Section 2.2).

Table 4. C5:2020 control categories and objectives

C5:2020 Category [9]	**C5:2020 Objective** [9]
Organisation of Information Security	Plan, implement, maintain and continuously improve the information security framework within the organisation.
Security Policies and Instructions	Provide policies and instructions regarding security requirements and to support business requirements.
Personnel	Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organisation’s assets are protected in the event of changes in responsibilities or termination.
Asset Management	Identify the organisation’s own assets and ensure an appropriate level of protection throughout their lifecycle.
Physical Security	Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.
Operations	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.
Portability and Interoperability	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.
Identity and Access Management	Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access.
Cryptography and Key Management	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.
Communication Security	Ensure the protection of information in networks and the corresponding information processing systems.
Procurement, Development and Modification of Information Systems	Ensure information security in the development cycle of cloud service system components.
Control and Monitoring of Service Providers and Suppliers	Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.
Security Incident Management	Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.
Business Continuity Management	Plan, implement, maintain and test procedures and measures for business continuity and emergency management.
Compliance	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.
Dealing with investigation requests from government agencies	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.
Product Safety and Security	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers,

C5:2020 Category [9]	**C5:2020 Objective** [9]
	appropriate mechanisms for troubleshooting and logging, as well as authentication

The controls in C5:2020 are structured as follows:

- Basic Criteria: state the minimum scope for an audit. BSI leaves it up to the customer to decide and assess in their individual case if the basic criteria adequately reflect their protection needs.
- Additional Criteria: in the event a customer decides that a higher level of protection is needed, this additional criteria shall be included in the audit.
- Supplementary information:
  - Notes on Continuous Auditing: this part includes information related to how a CSP could implement automated monitoring mechanisms through the use of third-party tools.
  - Complementary Customer Criteria: since cloud services follow a shared responsibility model, several C5 controls already indicate this fact. The goal is twofold: 1) to support auditors when assessing the system description and the appropriateness of the information provided regarding the complementary controls, and 2) to support customers in setting up better such controls.

2.1.4. SecNumCloud

SecNumCloud [10] is a label created in 2016 by the French State as part of its Cloud Computing plan. It is designed for the certification of CSPs in order to assure their quality and their security levels.

SecNumCloud is based on ISO/IEC 27000 family and comprises a set of requirements that shall be fulfilled by IaaS, PaaS and SaaS.

Even if the domains or categories are not exactly the same, they are mostly structured around the same as in ISO/IEC 27002. Since they have the same scope as in ISO/IEC 27002 they are not further detailed to avoid duplication of content [10]:

- Risk management and information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communication security
- System acquisition, development and maintenance
- Supplier relationship
- Information security incident management
- Business continuity
- Compliance

In addition to these, SecNumCloud contains additional requirements which are summarised in Table 5.

Table 5. SecNumCloud additional requirements

SecNumCloud Additional requirements [10]	**SecNumCloud Additional requirements description** [10]
Service agreements	Agreements and conditions between the CSP and the customer, shared responsibilities between customer and CSP. Applicable law and regulations to the service, reversibility clause and technical means to apply this clause (e.g., APIs). Availability level. Data ownership, that is, the data belongs to the customer. Non-disclosure of the customer's data to a third-party, except with formal authorisation. Approval of the service, and complaint possibilities to ANSSI.
Location of data	The CSP shall document and inform the customer where the data is stored and processed, which shall be done within the EU. Support operations can be performed from outside the EU.
Regionalisation	Interfaces of the service shall be accessible at least in French as well as first level support.
End of contract	The CSP shall ensure a secure erase of all the customer data.

In SecNumCloud, the scheme is structured as follows:

- Category title
- Control title
- Requirements, usually defined in separate sentences.

2.1.5. Cisco CCF

The Cisco Cloud Controls Framework (CCF) v1.0 [19] is a comprehensive set of international and national security compliance and certification requirements, aggregated into a single framework. It provides a structured, “build-once-use-many” approach for achieving multiple regional and international certifications, enabling market access and scalability, as well as easing compliance strain.

In addition to the control mapping, Cisco CCF also contains ‘narratives’, guidelines for users to understand how to implement the necessary controls, and ‘audit artifacts’ that include examples of what auditors generally request when testing the operating effectiveness of controls. It should be noted that Cisco CCF is purely guidance, and each organization should review, evaluate, and tailor the control framework according to its needs and integrate it into its own compliance regime.

Cisco CCF will be updated as security compliance frameworks and regulations evolve. Currently, the following security compliance frameworks and certification standards are covered: AICPA SOC 2 Trust Services Criteria, ISO/IEC 27001:2013, ISO/IEC 27017:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC27701:2019, Esquema Nacional de Seguridad (ENS), Infosec Registered Assessors Program (IRAP December 2020), Payment Card Industry Data Security Standard (PCI-DSS v3.2.1), Information System Security Management and Assessment Program (ISMAP), Cloud Computing Compliance Controls Catalogue (C5), EU Cloud Code of Conduct (CoC), Third-Party Cybersecurity Compliance Certificate (CCC), and The Federal Risk and Authorization Management Program (FedRAMP Li-SAAS).

Cisco CCF is structured in 15 domains and contains a total of 661 controls, that are summarized in Table 6. Controls from CCF 285 onwards are unique to IRAP[5] and no other frameworks.

Table 6. Cisco CCF v1 domains and controls

Cisco CCF [19] Domain Title	Controls range	Unique to IRAP
Audit Assurance & Compliance	CCF 1 – CCF 3	
Application and Interface Security	CCF 4 – CCF 6	CCF 285
Business Continuity Management & Operational Resilience	CCF 7 – CCF 22	CCF 626 - CCF 630
Change Control & Configuration Management	CCF 23 – CCF 34	
Data Center Security	CCF 35 – CCF 50	CCF 444 - CCF 530
Data Security and Privacy Lifecycle Management	CCF 51 – CCF 70	CCF 440 - CCF 443
Cryptography, Enterprise and Key Management	CCF 71 – CCF 83	CCF 568 - CCF 625
Governance and Risk Management	CCF 84 – CCF 114	CCF 286 - CCF 289
Human Resources	CCF 115 – CCF 130	CCF 531 - CCF 534
Identity & Access Management	CCF 131 – CCF 169	CCF 535 - CCF 567
Infrastructure & Virtualization Security	CCF 170 – CCF 193	CCF 290 - CCF 421
Privacy Handling & Security	CCF 194 – CCF 235	CCF 289
Security Incident Management, E-Discovery & Cloud Forensics	CCF 236 – CCF 244	
Supply Chain Management, Transparency, and Accountability	CCF 245 – CCF 260	CCF 422 - CCF 439
Threat and Vulnerability Management	CCF 262 – CCF 284	CCF 631 - CCF 661

In Cisco CCF, the scheme is structured as follows:

- Domain Title (e.g., *Audit Assurance & Compliance*)
- Control Title (e.g., *Control Self-Assessments*)
- Control Reference (e.g., *CCF 1*)
- Control Wording (e.g., *Independent Control self-assessments are performed by control owners, at least annually, to gain reasonable assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution.*)
- Control Type [*People/Process/Technology*]
- Control Narrative (e.g., *1. Develop and document a procedure for performance of control self-assessments against the CCF controls that have been implemented. 2. The self-assessment procedure shall minimally include: Tracking of the self-assessment in a ticketing system.*)
- Control Supporting Audit Artifacts (e.g., *1. Provide org chart to showcase independence of the audit team members. 2. Provide the list of controls/scope that were audited (…)*
- Applicable Framework (e.g., *ISO 22301, BS1 C5, Fedramp Tailored, Saudi CCC*)

2.1.6. Summary – Comparative analysis of Security Schemes

Table 7 summarizes the information that has been presented in the previous sections.

[5] IRAP—the Information Security Registered Assessors Program—provides a framework for assessing the implementation and effectiveness of an organization's security controls against the Australian government's security requirements.

Table 7. Summary – comparative analysis (source: MEDINA's own contribution)

	EUCS [2]	**C5:2020** [9]	**SecNumCloud** 11]	**ISO/IEC 27002 – ISO/IEC 27017** [11]	**Cisco CCF** [19]
Scope / Areas / Domains	Organisation of Information Security Security Policies and Procedures Risk Management Human Resources Asset Management Physical Security Operational security Identity, authentication, and access control management Cryptography and key management Communication security Portability and interoperability Change and configuration management Development of information systems Procurement management Incident management Business continuity Compliance User documentation Dealing with investigation requests from government agencies	Organisation of Information Security (OIS) Security Policies and Instructions (SP) Personnel (HR) Asset Management (AM) Physical Security (PS) Operations (OPS) Identity and Access Management (IDM) Cryptography and Key Management (CRY) Communication Security (COS) Portability and Interoperability (PI) Procurement, Development and Modification of Information Systems (DEV) Control and Monitoring of Service Providers and Suppliers (SSO) Security Incident Management (SIM) Business Continuity Management (BCM) Compliance (COM)	Risk management and information security policies Organization of information security, Human resource security Asset management, Access control, Cryptography Physical and environmental security Operations security Communication security System acquisition, development, and maintenance Supplier relationship Information security incident management Business continuity Compliance Service agreements Location of data Regionalisation End of contract	Information security policies Organization of information security Human resource security Asset management Access control Cryptography, Physical and environmental security Operations security Communication security System acquisition, development, and maintenance Supplier relationship Information security incident management Business continuity Compliance.	Audit Assurance & Compliance Application and Interface Security Business Continuity Management & Operational Resilience Change Control & Configuration Management Data Center Security Data Security and Privacy Lifecycle Management Cryptography, Enterprise and Key Management Governance and Risk Management Human Resources Identity & Access Management Infrastructure & Virtualization Security Privacy Handling & Security Security Incident Management, E-Discovery & Cloud Forensics Supply Chain Management, Transparency, and Accountability

	EUCS [2]	**C5:2020** [9]	**SecNumCloud** 11]	**ISO/IEC 27002 – ISO/IEC 27017** [11]	**Cisco CCF** [19]
	Product safety and security	Dealing with investigation requests from government agencies (INQ) Product Safety and Security (PSS)			Threat and Vulnerability Management
Structure of the controls	Category title Category objective: statement of that category Control id and name Control objective: goal of that control Requirement id, description and assurance level Implementation guidance	Basic Criteria Additional Criteria: Supplementary information: Notes on Continuous Auditing Complementary Customer Criteria:	Category title Control title Requirements	Category title Control name Control objective Implementation guidance Other information	Domain title Control Title Control Reference Control Wording Control Type Applicable Criteria Applicable Framework
Levels	Basic Substantial High	-	-	-	-
Conformity Assessment Method	For basic: Based on a self-assessment audited by a conformity assessment body (CAB). CSPs are not allowed to issue statements of conformity. For substantial and high: EUCS has defined an assessment approach compatible ISO/IEC 17065 ISAE 3402	ISAE 3402	Qualification	ISO based (ISO 17065)	-
Scope	Service	Service	Provider (*Prestataire*)	ISMS	Service

2.2. Mapping of the controls of the schemes analysed above

The goal of the mapping process is to identify similar controls (regarding their scope) between EUCS and other schemes to facilitate, as much as possible, the transition from other schemes towards EUCS and vice versa, as well as the reuse of evidence, whenever possible.

The initial mapping was made in a manual and empirical way, by reading the controls one by one and matching them. The analysis showed the different granularity level of the different schemes structure. However, a minimum common level of comparability can be perceived at control level.

The mapping has been incorporated to the *Catalogue of Controls and Metrics* database, so that the user can check which controls in EUCS have some equivalent controls in the other schemes (further information can be found in user manual of the Catalogue, Section 5.3.3).

In this version, we have made the exercise to leverage the Cisco CCF framework to extent the mapping provided in the previous version of this deliverable (D2.1 [1]), that included the mapping between EUCS, C5:2020, SecNumCloud, ISO/IEC 27002 and ISO/IEC 27017.

This extension focuses on a subset of EUCS controls, in particular the controls (26 in total) related to the 34 high level EUCS requirements relevant for MEDINA (cf. Section 3.1). The idea of the mapping among EUCS and Cisco CCF is simple: we need to identify which CCF control (or controls) map to each of those selected EUCS 26 controls. To help with the task, we first identified which standards are common between the initial mapping and the CCF mapping, resulting in three standards: BSI C5, ISO 27002 and ISO 27017. We decided to use BSI C5, because it is the standard to which the EUCS requirements are most closely aligned. Then, based on the C5 controls, we looked for those identified in the initial mapping in the CCF map table. If one was found, we could identify which CCF control it was related to, and therefore use the initial mapping to identify the corresponding EUCS control. If more than one CCF control was identified, we empirically selected the more appropriate (s) match(es). Table 8 shows the result of this process.

The EUCS controls are considered the baseline controls. Whenever a control similar in scope or meaning was found in the other schemes or standards, it was noted, even if the match was not 1:1 or 100%, hence the multiple matches. This has been done on purpose so as not to leave out any requirements. The orange lines in Table 8 indicate the controls (26 in total), corresponding to the 34 high level EUCS requirements relevant for MEDINA (cf. Section 3.1), that have been mapped to the Cisco CCF.

Based on Table 8, and leveraging that Cisco CCF covers a wide range of standards, an extended map of the selected EUCS controls can be obtained, using the identified CCF controls to extend the current mapping to the 14 frameworks covered by CCF. The extended mapping of security controls is shown in *Appendix 3: Extended mapping of security controls.*

Table 8. Mapping of EUCS 2022 security controls with C5:2020, SecNumCloud, ISO/IEC 27002, ISO/IEC 27017 and Cisco CCF (source: MEDINA's own contribution)

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
OIS-01 - INFORMATION SECURITY MANAGEMENT SYSTEM	OIS-01		4.1 - 10.2		
OIS-02 - SEGREGATION OF DUTIES	OIS-04	6.1 6.2	6.1.2	CLD.6.3.1	CCF 91

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
OIS-03 - CONTACT WITH AUTHORITIES AND INTEREST GROUPS	OIS-05	6.3 6.4	4.3 6.1.3 6.1.4	CLD.6.3.1	
OIS-04 - INFORMATION SECURITY IN PROJECT MANAGEMENT	OIS-05	6.5	6.1.5	CLD.6.3.1	
ISP-01 - GLOBAL INFORMATION SECURITY POLICY	OIS-02	5.2 5.1	6.2 5.1.1 6.1.1		
ISP-02 - SECURITY POLICIES AND PROCEDURES	SP-01 SP-02	5.1 5.2	5.1.1 5.1.2		
ISP-03 - EXCEPTIONS	SP-03				CCF 108
RM-01 - RISK MANAGEMENT POLICY	OIS-06		6.1.1		
RM-02 - RISK ASSESSMENT IMPLEMENTATION	OIS-07	5.3	6.1.1		
RM-03 - RISK TREATMENT IMPLEMENTATION	OIS-07		6.1.1		
HR-01 - HUMAN RESOURCE POLICIES	HR-01	7.2	7.1.1 7.2.1		
HR-02 - VERIFICATION OF QUALIFICATION AND TRUSTWORTHINESS	HR-01	7.1	7.1.1		
HR-03 - EMPLOYEE TERMS AND CONDITIONS	HR-02	7.2	7.1.2		CCF 120
HR-04 - SECURITY AWARENESS AND TRAINING	HR-03		7.2.2		CCF 123
HR-05 - TERMINATION OR CHANGE IN EMPLOYMENT	HR-05	7.5	7.3.1		CCF 120 CCF 165
HR-06 - CONFIDENTIALITY AGREEMENTS	HR-06		7.1.2 13.2.4		CCF 118 CCF 119
AM-01 - ASSET INVENTORY	AM-01	8.1.1. 8.1.2	8.1.1		CCF 52
AM-02 - ACCEPTABLE USE AND SAFE HANDLING OF ASSETS POLICY	AM-02	8.5	8.1.3		
AM-03 - COMMISSIONING AND DECOMMISSIONING	AM-03 AM-04	8.1.4	8.3.1 8.3.2		CCF 48
AM-04 - ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS	AM-05		8.1.4 8.2.1	CLD 8.1.5	CCF 48
AM-05 - ASSET CLASSIFICATION AND LABELLING	AM-06	8.2 8.3	8.2.2 8.2.3		
PS-01 - PHYSICAL SECURITY PERIMETERS	PS-01	11			
PS-02 - PHYSICAL SITE ACCESS CONTROL	PS-03 PS-04	11.2	9.2.1 9.2.2 9.2.3 11.1.1 11.1.2 A 11.1.3 11.1.6		CCF 35
PS-03 - WORKING IN NON-PUBLIC AREAS		11.4			
PS-04 - EQUIPMENT PROTECTION		11.6 11.7			

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
		11.8 10.1			
PS-05 - PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS	PS-01 PS-02	11.3	17.2.1		
OPS-01 - CAPACITY MANAGEMENT – PLANNING	OPS-01	12.1	12.1.3		
OPS-02 - CAPACITY MANAGEMENT – MONITORING	OPS-02		12.1.3		CCF 254
OPS-03 - CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES	OPS-03			CLD.12.4.5	
OPS-04 - PROTECTION AGAINST MALWARE – POLICIES	OPS-04	12.4			
OPS-05 - PROTECTION AGAINST MALWARE – IMPLEMENTATION	OPS-05	12.4	12.2.1		CCF 262
OPS-06 - DATA BACKUP AND RECOVERY – POLICIES	OPS-06	12.4	12.3.1		
OPS-07 - DATA BACKUP AND RECOVERY – MONITORING	OPS-07	12.4			CCF 18
OPS-08 - DATA BACKUP AND RECOVERY – REGULAR TESTING	OPS-08	12.4	12.3.1		
OPS-09 - DATA BACKUP AND RECOVERY – STORAGE	OPS-03	12.4			CCF 19
OPS-10 - LOGGING AND MONITORING – POLICIES	OPS-10	12.1 12.6	12.4.1 12.4.2 12.4.3		
OPS-11 - LOGGING AND MONITORING – DERIVED DATA MANAGEMENT	OPS-11	12.1 12.6	12.4.1 12.4.2 12.4.3		
OPS-12 - LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	OPS-13	12.1 12.6			CCF 109
OPS-13 - LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION	OPS-12 OPS-14	12.1 12.6	12.4.1 12.4.2 12.4.3		CCF 239
OPS-14 - LOGGING AND MONITORING – ATTRIBUTION	OPS-15	12.1 12.6			
OPS-15 - LOGGING AND MONITORING – CONFIGURATION	OPS-16	12.1 12.6	9.4.4 12.4.2		
OPS-16 - LOGGING AND MONITORING – AVAILABILITY	OPS-17	12.1 12.6	17.2.1		
OPS-17 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES	OPS-18 OPS-22		12.1.2 A 12.6.1 14.2.2		
OPS-18 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	PSS-03				CCF 87
OPS-19 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION	OPS-19 OPS-22	12.9	12.1.2 A 12.6.1 13.1.1 14.2.2 18.2.3		
OPS-20 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS,	OPS-20	12.9	12.6.1		

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
ANALYSES AND ASSESSMENTS OF PROCEDURES					
OPS-21 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	OPS-23	12.9			CCF 272
OPS-22 - SEPARATION OF DATASETS IN THE CLOUD INFRASTRUCTURE	OPS-24		13.1.3		
IAM-01 - POLICIES FOR ACCESS CONTROL TO INFORMATION	IDM-01	9.1	9.1.1		
IAM-02 - MANAGEMENT OF USER ACCOUNTS	IDM-01	9.3 9.2	9.1.1 9.4.1 9.4.2		
IAM-03 - LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	IDM-03	9.3	9.2.2 9.2.6		CCF 148
IAM-04 - MANAGEMENT OF ACCESS RIGHTS	IDM-02 IDM-04	9.3	9.2.2 9.2.3 9.2.6		
IAM-05 - REGULAR REVIEW OF ACCESS RIGHTS	IDM-05	9.4	9.2.5		
IAM-06 - PRIVILEGED ACCESS RIGHTS	IDM-06	9.3 9.4 9.6	6.1.2 9.2.3 12.4.3		
IAM-07 - AUTHENTICATION MECHANISMS	IDM-09	9.5	9.4.3		
IAM-08 - PROTECTION AND STRENGTH OF CREDENTIALS	IDM-08		9.2.4 9.3.1		
IAM-09 - GENERAL ACCESS RESTRICTIONS	IDM-07	9.7			
CKM-01 - POLICIES FOR THE USE OF CRYPTOGRAPHY AND KEY MANAGEMENT	CRY-01		10.1.1 10.1.2 13.2.1 13.2.2 18.1.5		
CKM-02 - ENCRYPTION OF DATA IN MOTION	CRY-02	10.2	10.1.1 13.1.1 13.2.3 14.1.2 14.1.3 18.1.5		
CKM-03 - ENCRYPTION OF DATA AT REST	CRY-03	10.1	10.1.1 10.1.2 18.1.4		
CKM-04 - SECURE KEY MANAGEMENT	CRY-04	10.5	10.1.2		
CS-01 - TECHNICAL SAFEGUARDS	COS-01		13.1.1 13.1.2		
CS-02 - SECURITY REQUIREMENTS TO CONNECT WITHIN THE CSP'S NETWORK	COS-02		13.1.1 13.1.2 13.1.3 13.2.1		
CS-03 - MONITORING OF CONNECTIONS WITHIN THE CSP'S NETWORK	COS-03	13.3	13.1.1 13.1.2 13.2.1		

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
CS-04 - NETWORKS FOR ADMINISTRATION	COS-06	13.2	13.1.3		
CS-05 - TRAFFIC SEPARATION IN SHARED NETWORK ENVIRONMENTS	COS-06		13.1.3		
CS-06 - NETWORK TOPOLOGY DOCUMENTATION	COS-07	13.1		CLD.13.1.4	
CS-07 - SOFTWARE DEFINED NETWORKING	PSS-10		13.2.2 12.5.1 14.1.3		
CS-08 - DATA TRANSMISSION POLICIES	CSO-08		13.2.1 13.2.2 13.2.3 14.1.1		
PI-01 - DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES	PI-01				
PI-02 - CONTRACTUAL AGREEMENTS FOR THE PROVISION OF DATA	PI-02		11.2.5		
PI-03 - SECURE DELETION OF DATA	PI-03	19.4	11.2.7		
CCM-01 - POLICIES FOR CHANGES TO INFORMATION SYSTEMS	DEV-03	12.2 14.2	8.1 14.2.2 14.2.3 14.2.4		
CCM-02 - RISK ASSESSMENT, CATEGORISATION AND PRIORITISATION OF CHANGES	DEV-05		8.1 14.2.2		
CCM-03 - TESTING CHANGES	DEV-06	14.2 14.3 14.7	12.1.2 14.2.2 14.2.8 14.2.9		
CCM-04 - APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	DEV-09				CCF 30
CCM-05 - PERFORMING AND LOGGING CHANGES	DEV-07	12.2 14.2	9.4.5 12.1.2 14.2.2 14.2.8 14.2.9		CCF 25
CCM-06 - VERSION CONTROL	DEV-07 DEV-08	14.2	7.5.3 9.4.5 12.1.2 14.2.2 14.2.8 14.2.9		
DEV-01 - POLICIES FOR THE DEVELOPMENT AND PROCUREMENT OF INFORMATION SYSTEMS	DEV-01	14.1	14.1.1 14.1.2 14.2.1 14.2.5 12.1.4		
DEV-02 - DEVELOPMENT SUPPLY CHAIN SECURITY					
DEV-03 - SECURE DEVELOPMENT ENVIRONMENT		14.4	14.2.1		

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
DEV-04 - SEPARATION OF ENVIRONMENTS	DEV-10		12.1.4		
DEV-05 - DEVELOPMENT OF SECURITY FEATURES		14.3 12.10			
DEV-06 - IDENTIFICATION OF VULNERABILITIES OF THE CLOUD SERVICE	PSS-02	12.11	12.6.1		
DEV-07 - OUTSOURCING OF THE DEVELOPMENT	DEV-02	14.5	14.2.7 14.2.8 14.2.9		
DEV-08 - CONTROLLING EXCHANGES WITH SUPPLIERS OF FUNCTIONAL COMPONENTS					
PM-01 - POLICIES AND PROCEDURES FOR CONTROLLING AND MONITORING THIRD PARTIES	SSO-01	15	15.1.1 15.1.2 15.1.3 7.2.2		
PM-02 - RISK ASSESSMENT OF SUPPLIERS	SSO-02	15	15.1.1 15.1.2 15.1.3 15.2.2		
PM-03 - DIRECTORY OF SUPPLIERS	SSO-03	15.1	-		
PM-04 - MONITORING OF COMPLIANCE WITH REQUIREMENTS	SSO-04	15.5	15.2.1		CCF 247
PM-05 - EXIT STRATEGY	SSO-05		-		
IM-01 - POLICY FOR SECURITY INCIDENT MANAGEMENT	SIM-01 SSO-01	16.1	15.1.1 15.1.2 15.1.3 16.1.1 16.1.2 16.1.4 16.1.5 16.1.6		
IM-02 - PROCESSING OF SECURITY INCIDENTS	SIM-02	16.3 16.5			CCF 236
IM-03 - DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS	SIM-03	16.5	16.1.1 16.1.2 16.1.7		
IM-04 - USER'S DUTY TO REPORT SECURITY INCIDENTS	SIM-04	16.2	16.1.2 16.1.3		
IM-05 - INVOLVEMENT OF CLOUD CUSTOMERS IN THE EVENT OF INCIDENTS	OPS-21	16.2	12.6.1		
IM-06 - EVALUATION AND LEARNING PROCESS	SIM-05	16.5	16.1.3 16.1.4 16.1.5 16.1.6		
IM-07 - INCIDENT EVIDENCE PRESERVATION	SIM-05	16.5	16.1.3 16.1.4 16.1.5 16.1.6		

EUCS Control	C5.2020 GERMANY	SecNum Cloud	ISO/IEC 27002	ISO/IEC 27017	Cisco CCF
BC-01 - BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY	BCM-01	17.1	17.1.1		
BC-02 - BUSINESS IMPACT ANALYSIS PROCEDURES	BCM-02 BCM-04	17.2 17.4	17.1.1 17.1.3		
BC-03 - BUSINESS CONTINUITY AND CONTINGENCY PLANNING	BCM-02 BCM-04	17.2	17.1.1 17.1.3		
BC-04 - BUSINESS CONTINUITY TESTS AND EXERCISES	BCM-02 BCM-04	17.3	17.1.1 17.1.3		
CO-01 - IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS	COM-01	18.1	18.1.1		
CO-02 - POLICY FOR PLANNING AND CONDUCTING AUDITS	COM-02	18.2	9.2 12.7.1		
CO-03 - INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	COM-03		9.2 9.3 12.7.1 18.2.2		CCF 1
CO-04 - INFORMATION ON INTERNAL CONTROL SYSTEM ASSESSMENT	COM-04		9.3		
DOC-01 - GUIDELINES AND RECOMMENDATIONS FOR CLOUD CUSTOMERS	PSS-01				
DOC-02 - LOCATIONS OF DATA PROCESSING AND STORAGE	BC-01	19.2			
DOC-03 - JUSTIFICATION OF THE TARGETED EVALUATION LEVEL					
DOC-04 - GUIDELINES AND RECOMMENDATIONS FOR COMPOSITION					
DOC-05 - CONTRIBUTION TO THE FULFILMENT OF REQUIREMENTS FOR COMPOSITION					
INQ-01 - LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRIES	INQ-01				
INQ-02 - INFORMING CLOUD CUSTOMERS ABOUT INVESTIGATION REQUESTS	INQ-02				
INQ-03 - CONDITIONS FOR ACCESS TO OR DISCLOSURE OF DATA IN INVESTIGATION REQUESTS	INQ-03				CCF 279
PSS-01 - ERROR HANDLING AND LOGGING MECHANISMS	PSS-04				
PSS-02 - SESSION MANAGEMENT	PSS-06		10.1.1 18.1.5		
PSS-03 - SOFTWARE DEFINED NETWORKING	PSS-10		13.1.4		
PSS-04 - IMAGES FOR VIRTUAL MACHINES AND CONTAINERS	PSS-11				CCF 173
PSS-05 – CHOICE OF LOCATIONS FOR DATA PROCESSING AND STORAGE	PSS-12				

3. Technical and Organizational Measures (TOMs) for Continuous Assessment

This section starts by identifying the TOMs or high-level requirements of EUCS 2022 [2] that are relevant for MEDINA. The section then discusses the methodology and the definition of the Reference TOMs. A Reference TOM can be considered as an explanation of how a specific EUCS security requirement can be implemented, in a vendor- and technology-agnostic way, to be compliant. This is to serve as guidance for the user, but also as an input to the MEDINA certification language that leverages Natural Language Processing (NLP) techniques.

The reference TOMs are included in the catalogue along with the rest of elements of the EUCS framework.

3.1. Requirements relevant for continuous assessment in EU Cloud Services certification scheme (EUCS)

The Cybersecurity Act (EU CSA) [3] defines in its article 52(6) three levels of assurance, namely, basic, substantial, and high depending on the risk appetite that the service provider is ready to accept. The EU CSA describes the levels as follows and shall meet the following criteria respectively:

- Basic: "*shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents*" [3];
- Substantial "*shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity incidents*" [3];
- High "*shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity incidents*" [3].

The three levels are in principle valid for all ICT products, processes and services that are to fall under the EU CSA. Of course, the EU CSA also leaves room for not having a three levelled certification scheme, shall it not be applicable [Article 54 d)].

Article 52(7) requires that in the assurance level 'high' the security controls include a vulnerability assessment of known vulnerabilities, a review of functional tests as well as automated monitoring requirements, the use of state-of-the-art security functionalities and penetration testing, as also stated in the draft version of the candidate EUCS scheme [5].

EUCS distinguishes the different assurance levels by dimensions such as Intention, Suitability, Attacker profile, Scope of the Evaluation, Depth, and Rigour, using the criteria and definition coming from ISO/IEC 15408-3. The following dimensions include a reference to the wording "automatically monitor*", which is mainly the scope of MEDINA:

- Intention: "*[…] Security controls are monitored for continuous operation in accordance with their design; they are reviewed, and pen tested to validate their actual ability to prevent or detect security breaches*."
- Intention rationale: "[…] *Scope, depth and rigour of this assurance level extend the previous level for Substantial by additional procedures to be performed for automated controls. Automated monitoring is applied by the CSP to identify exceptions in the application of controls (e.g., changes to the configuration) and initiate corrective actions. […]*"
- Scope: "*[…] Operating effectiveness of the controls shall be demonstrated. (Including automated monitoring if required by the control definition).*"
- Scope rationale *"[…] Enhancements often included additional constraints, references to state-of-the-art requirements, and automated monitoring of some controls*."
- Depth rationale: *"[…] The main addition in depth come from additional requirements for level High […]"*

Coming down to the requirements that are within the scope of MEDINA for continuous assessment, the ones that are considered are those that comply with the following requisites:

- They are of assurance level high.
- They include the wording "automatically monitor" or variations thereof.

Based on these requisites, the scopes of the MEDINA KPI 1.1 and KPI 1.2 were reformulated in July 2022 as follows:

> *KPI 1.1: Provide realizable metrics for at least 70% of the technical measures referenced in EUCS-High assurance requiring 'continuous (automated)' monitoring.*
>
> *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.*

Table 9 shows the TOMs from the draft EUCS of August 2022 EUCS [2][6] that meet the above-mentioned requisites and are therefore considered for the assessment of KPI 1.1 and KPI 1.2 in MEDINA.

Table 9. "The 34": Requirements considered in MEDINA that are of assurance level high and require 'continuous (automated)' monitoring (source: EUCS [2])

Category	Security control	Req. ID	Requirement
Organization of information security	**OIS-02 Segregation of Duties**	**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."
Information security policies	**ISP-03 Exceptions**	**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."
Risk management	**N/A**		

[6] 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.

Category	Security control	Req. ID	Requirement
Human resources	**HR-03 Employee Terms and Conditions**	**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 Security Awareness and Training	**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 Termination or Change in Employment	**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 Confidentiality Agreements	**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."
Asset management	**AM-01 Asset Inventory**	**AM-01.4H**	"The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date."
	AM-03 Commissioning and Decommissioning	**AM-03.4H**	"The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored."
	AM-04 Acceptable Use, Safe Handling and Return of Assets	**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."
Physical security	**PS-02 Physical Site Access Control**	**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."
Operational security	**OPS-02 Capacity Management – Monitoring**	**OPS-02.2H**	"The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards."
	OPS-05 Protection	**OPS-05.3H**	"The CSP shall automatically monitor the systems covered by the malware protection and the

Category	Security control	Req. ID	Requirement
	Against Malware – Implementation		configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.”
	OPS-07 Data Backup and Recovery – Monitoring	**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 Data Backup and Recovery – Storage	**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 Logging and Monitoring – Identification of Events	**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 Logging and Monitoring – Access, Storage and Deletion	**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 Managing Vulnerabilities, Malfunctions and Errors – Online Registers	**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 Managing Vulnerabilities, Malfunctions and Errors – System Hardening	**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.”
Identity, authentication and access control management	**IAM-03 Locking, Unlocking and Revocation of User Accounts**	**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 IAM-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.”

Category	Security control	Req. ID	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 IAM-02, based on the risks of the accounts, associated access 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 IAM-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."
Cryptography and key management	**N/A**		
Communication security	**N/A**		
Portability and interoperability	**N/A**		
Change and configuration management	**CCM-04 Approvals for Provision in the Production Environment**	**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 Performing and Logging Changes	**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."
Development of information systems	**N/A**		
Procurement management	**PM-04 Monitoring of Compliance with Requirements**	**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."

Category	Security control	Req. ID	Requirement
Incident management	**IM-02 Processing of Security Incidents**	**IM-02.5H**	"The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures."
Business continuity	**N/A**		
Compliance	**CO-03 Internal Audits of the Internal Control System**	**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."
User documentation	**N/A**		
Dealing with investigation requests from government agencies	**INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests**	**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."
Product security	**PSS-04 Images for Virtual Machines and Containers**	**PSS-04.2H**	"An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails."

3.2. Methodology and motivation to extract reference implementations for technical and organizational measures

The aim of this section is to facilitate, especially for small and medium CSPs, with some technical and organizational reference implementations of high security level requirements. A Reference TOM can be considered an explanation of how a specific security requirement can be implemented, in a vendor – and technology-agnostic way, and can be enriched with examples from larger CSPs such as Amazon or Azure, which can serve as inspiration. These TOM reference implementations are used as input in the MEDINA certification language for associations between TOMs and metrics using Natural language processing (NLP). TOMs are used in this case as obligations (see D2.4 [20]).

Cloud Security Posture Management (CSPM) [15] is a class of tools that allows to identify misconfiguration issues and compliance matters on the cloud. Current solutions exist such as Fugue [16] or Prisma [17] but for the time being they do not cover EUCS requirements.

Large CSPs such as Amazon and Azure offer their own resources to their own customers to avoid misconfigurations on their services, e.g. RDS [18] and for different domains, e.g. Identity management [19] but smaller CSPs may have more challenges, especially when addressing composition.

For the extraction of the Reference TOMs, experts within the MEDINA consortium have revised different literature sources as well as current state-of-the-art practices coming from commercial vendors such as the ones listed above but also from those participating in the MEDINA project. These existing practices have been abstracted, both from the technology and the vendor perspective and reformulated in a way in which they can be used as guidance and reference.

The identifier of a Reference TOM consists of three elements: EUCS Category, EUCS Control name and EUCS Requirement ID, e.g., *Organisation of Information Security :: Segregation of Duties :: OIS-02.4H.*

The definition of a Reference TOM includes the description of the associated EUCS requirement, the identification of the EUCS security control and other related controls, some key concepts, and some guidelines for the implementation of the requirement.

3.3. Technical and organizational measures reference implementations per category and security requirement

The following section describes the second version of the elicited Reference TOMs, classified per category and security requirement, derived from the 34 high-level EUCS requirements listed in Table 9[7] . Depending on the complexity of the requirement, different levels of detail are provided in the definition of the Reference TOM.

3.3.1. Reference TOMs for Organization of Information Security

3.3.1.1. Organisation of Information Security :: Segregation of Duties :: OIS-02.4H

The EUCS requirement OIS-02.4H states [2]:

> "**The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced**".

and references as "measures" the following requirement also from OIS-02 Segregation of Duties:

OIS-02.1H	"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 cloud service, 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."

3.3.1.1.1. EUCS Security Control

Code	Name	Objective [2]
OIS-02	Segregation of Duties	"Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of CSC data processed, stored or transmitted in the cloud service."

Dependencies:

- RM-01: Risk Management Policy
- IAM-01: Policies for Access Control to Information
- DEV-01: Policies for the Development and Procurement of Information Systems
- CCM-01: Policies for Changes to Information Systems

[7] 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.

3.3.1.1.2. Key concepts

Term	Definition
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Cloud RBAC	Cloud role-based access control is an authorization system provided by the CSP that provides fine-grained access management of Cloud resources to ensure that measures related to segregation of duties are enforced.
Role assignment	It is the process (grant, change, revoke) of attaching a role definition to a security principal at a particular scope.

3.3.1.1.3. Guidelines

Typically, managing access to cloud resources is a critical function and is performed by the CSP by implementing a cloud RBAC (e.g., Azure RBAC, AWS RBAC) to manage who has access to specific cloud resources, what they can do with those resources, and what areas they have access to. The assignment of tasks to roles will allow a separation of duties as part of the role management process. The role assignment is monitored by the CSP.

Roles and responsibilities of the users are defined and agreed on in a risk assessment performed by the CSP. The risk assessment should cover administrative and user rights, and should include definitions related to data ownership, information security accountability, access provisioning and approval responsibilities, development, testing and release of changes, data backup and recovery responsibilities, and operation of the system components. Some mitigation measures should be introduced to monitor the activities in order to detect unauthorised or unintended changes as well as misuse.

A defined team shall be defined that is responsible for overseeing the security and control environments at the organization. It will verify the roles of each member and validate that security and control environments are being reviewed and followed up upon. Managers will check in with each member to review responsibilities and roles at least annually.

3.3.2. Reference TOMs for Information Security Policies

3.3.2.1. Information Security Policies :: Exceptions :: ISP-03.5H

The EUCS requirement ISP-03.5H states [2]:

> “***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***”.

and references as “measures” the following requirement also from ISP-03 Exceptions:

ISP-03.1H	"The CSP shall maintain a list of exceptions, limited in time, to the security policies and procedures, including associated controls."

3.3.2.1.1. EUCS Security Control

Code	Name	Objective [2]
ISP-03	Exceptions	“Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed”

Dependencies:

- RM-01: Risk Management Policy

3.3.2.1.2. Key concepts

Term	Definition
Exception	Exceptions to information security policies, standards, guidelines, and procedures
Risk Management	Risk management is the identification, evaluation, and prioritization of risks.

3.3.2.1.3. Guidelines

This security control ensures that exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.

Deviation from Information Security policy implemented by the CSP is discouraged. However, exception may be considered if a presentation of a reasonable and justifiable reason is provided. The expression, "there is an exception to every rule" is also true in information security policies context. There are often legitimate reasons why an exception to a policy is needed. In these cases, the policy should define how approval for the exception to the policy is obtained, and management should be aware of exceptions to security policies as the exception to the policy could introduce risks that need to be mitigated in another way.

In the context of EUCS requirements exceptions can have organizational or technical causes, such as:

- An organizational unit deviating from the intended processes and procedures in order to meet the requirements of a cloud customer.
- A system component lacking technical properties to be configured according to the applicable requirements.

Cloud customers can use appropriate controls to ensure that they obtain information from the Cloud Service Provider about deviations from information security policies and instructions in order to assess and appropriately manage the associated risks to their own information security.

While at basic assurance level, maintaining a list of exceptions is sufficient, at substantial level, those exceptions are required to be approved and taken into account by the risk management. Therefore, the exceptions need to be collected and approved, as part of the risk management process. A complete description of the exception shall be maintained including relevant information such as exception description, exception duration, compensating controls for managing the risk associated with the exception, proposed review date, or others. The approvals of exceptions may be documented, limited in time and reviewed for appropriateness at least annually by the risk owners.

At the high assurance level, the list of the exception must also be automatically monitored. The continuous monitoring of the exceptions list should be automated to ensure that they do not exceed their "lifespan" in the system and that exceptions do not remain active after approval has been revoked. Such a monitoring tool should be capable of issuing notifications and regular status updates when an exception expires, has been approved or has been revoked by the risk owner. This could be achieved through languages similar to the one defined in the OSCAL (Open Security Controls Assessment Language).

3.3.3. Reference TOMs for Human Resources

3.3.3.1. Human Resources :: Employee terms and conditions :: HR-03.4H

The EUCS requirement HR-03.4H states [2]:

> "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**".

3.3.3.1.1. EUCS Security Control

Code	Name	Objective [2]
HR-03	Employee terms and conditions	"The CSP's internal and external employees are required by the employment terms and conditions to comply with applicable policies and procedures relating to information security, and to the CSP's code of ethics, before being granted access to any CSC data or system components under the responsibility of the CSP used to provide the cloud service in the production environment"

3.3.3.1.2. Key concepts

Term	Definition
Information security policies	Information security policies refer to policies, processes, and tools designed and deployed to protect sensitive business information and data assets from unauthorised access.
Code of Ethics	A code of ethics sets out an organization's ethical guidelines and best practices to follow for honesty, integrity, and professionalism.

3.3.3.1.3. Guidelines

Typically, a CSP defines information security policies and procedures to determine the organisation's approach to manage its security objectives. These policies should be communicated to the internal and external employees in a relevant and understandable form [11].

In order to track who has been informed of these policies and procedures, the CSP should prepare a simple acknowledgement form for employees to sign, preferably digitally so it can be automatically monitored and tracked. Every time a change is introduced in the information security policies, procedures and practices, the same form should be digitally signed again to make sure that all employees are aware of the changes. The signed form serves as evidence that the employees who signed it have been informed about the recent approach of the organisation to manage cyber security.

A typical acknowledgement form includes the name of the party which should read the policy and procedure, states which document is to be acknowledged, describes what is expected from the party regarding the implementation of the policy, the date when the form is signed and the signature [26].

In addition to the digital signature, the process of collecting and accounting of acknowledgement forms must be automated to ensure a quick update and report of the status of informed employees about the information security policies, identification of those who have not yet signed it, and defining further steps for ensuring that all employees get up-to-date information about the policies.

3.3.3.2. Human Resources :: Security awareness and training :: HR-04.3H

The EUCS requirement HR-04.3H states [2]:

> "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**".

and references as “measures” the following requirement also from HR-04 Security awareness and training:

HR-04.1H	"The CSP shall define a security awareness and training program on a target group oriented manner, taking into consideration at least the position’s risk classification and technical duties, and 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."

3.3.3.2.1. EUCS Security Control

Code	Name	Objective [2]
HR-04	Security awareness and training	“The CSP operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the CSP on a regular basis”

3.3.3.2.2. Key concepts

Term	Definition
Security awareness	The capacity to be conscious and alert of the possible security threats.

3.3.3.2.3. Guidelines

Upstream of this requirement is the fact that the CSP employees must participate in training and refresher courses related to the functions to be performed in their employment. The CSP is required to ensure that the employees have taken these courses.

Thus, a possible way to implement this requirement could be as follows:

- the employee can attend a refresher course organized by the CSP online, and
- the employee can digitally sign an exam taken after the course.

The CSP training program shall include a security awareness sub-program and content specifications according to the different positions.

3.3.3.3. Human Resources :: Termination or change in employment :: HR-05.2H

The EUCS requirement HR-05.2H states [2]:

> “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**”.

3.3.3.3.1. EUCS Security Control

Code	Name	Objective [2]
HR-04	Termination or change in employment	“Internal and external employees have been informed about which responsibilities, arising from the policies and procedures relating to information security, will remain in place when their employment is terminated or changed and for how long.

		Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately”

3.3.3.3.2. Key concepts

Term	Definition
Access rights	The permissions that are granted to a user in this case to an employee to read, write, access or modify certain resources.
Account revocation	Account deletion.

3.3.3.3.3. Guidelines

The CSP should specify in advance a procedure for defining which access rights should remain and which should be revoked immediately once a contract of an internal or external employee is terminated. This procedure should define specific roles and responsibilities and will include a documented checklist of the steps to be performed.

The defined procedures should be based on information security requirements, legal responsibilities, responsibilities with respect to relevant confidential agreements, and the terms and conditions of employment [11]. In all cases, the employees should be communicated about the termination of their responsibilities. The accounts to be revoked shall be disabled in order to keep required audit trails [27].

For internal employees, the human resources department is typically responsible for the termination process together with the superior of the leaving employee. For external employees, the termination process is undertaken by the external party and should be executed in accordance with the contract between this party and the organisation.

This requirement could be implemented if the internal employee receives digital confirmation that s/he has been informed about the required topics, and this is requested again digitally at the termination process. By doing so, the auditor would be able to check each termination and identify any deviations [9].

3.3.3.4. Human Resources :: Confidentiality agreements :: HR-06.2H

The EUCS requirement HR-06.2H states [2]:

> “The agreements shall be accepted by external service providers and suppliers when the contract is agreed, **and this acceptation shall be automatically monitored**”.

and references as “measures” the following requirement also from HR-06 Confidentiality agreements:

HR-06.1H	"The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers, based on the requirements identified by the CSP for the protection of confidential information and operational details."

3.3.3.4.1. EUCS Security Control

Code	Name	Objective [2]
HR-06	Confidentiality agreements	“Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them”

3.3.3.4.2. Key concepts

Term	Definition
NDA	A non-disclosure agreement (NDA), also called a confidentiality agreement, is a legally binding contract which obliges one party to not disclose secret information without permission from another party.

3.3.3.4.3. Guidelines

An NDA is required to ensure that external service providers and suppliers will not reveal CSP's secrets or any confidential information they are working with. An NDA must be signed before the relationship with the external service providers or suppliers starts.

An NDA can be digitally signed, so that the signing of NDA can be easily monitored in an automatic way by the CSP. The digital signature process also allows the CSP to easily obtain up-to-date status of how many NDAs have been signed, identify those external service providers or suppliers who have not yet signed the document, and to ensure that those who did not sign have no access to secrete or confidential information. Such automatization requires tool support for the monitoring, e.g., Adaptive Non-Disclosure Agreement (NDA) Manager [28].

3.3.3.5. Human Resources :: Confidentiality agreements :: HR-06.3H

The EUCS requirement HR-06.3H states [2]:

> "The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, **and this acceptation shall be automatically monitored**".

and references as "measures" the following requirement also from HR-06 Confidentiality agreements:

HR-06.1H	"The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers, based on the requirements identified by the CSP for the protection of confidential information and operational details."

3.3.3.5.1. EUCS Security Control

Code	Name	Objective [2]
HR-06	Confidentiality agreements	"Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them"

3.3.3.5.2. Key concepts

Term	Definition
NDA	A non-disclosure agreement (NDA), also called a confidentiality agreement, is a legally binding contract which obliges one party to not disclose secret information without permission from another party.

3.3.3.5.3. Guidelines

An NDA is required to ensure that internal employees will not reveal CSP's secretes or any confidential information they are working with. An NDA must be signed before an employee is granted access to any confidential information [11]. This is typically done before employment [29].

An NDA can be digitally signed, so that the signing of NDA can be easily monitored in an automatic way by the CSP. The digital signature process also allows the CSP to easily obtain up-to-date status of how many NDAs have been signed, identify those internal employees who have not yet signed the document, and to ensure that those who did not sign have no access to secrete or confidential information. Such automatization requires tool support for the monitoring, e.g., Adaptive Non-Disclosure Agreement (NDA) Manager [28].

3.3.3.6. Human Resources :: Confidentiality Agreements :: HR-06.5H

The EUCS requirement HR-06.5H states [2]:

> "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 acceptation shall be automatically monitored**".

and references as "measures" the following requirement also from HR-06 Confidentiality Agreements:

HR-06.4H	"The requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be modified, then the non-disclosure or confidentiality agreements shall be modified accordingly."

3.3.3.6.1. EUCS Security Control

Code	Name	Objective [2]
HR-06	Confidentiality agreements	"Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them"

3.3.3.6.2. Key concepts

Term	Definition
NDA	A non-disclosure agreement (NDA), also called a confidentiality agreement, is a legally binding contract which obliges one party to not disclose secret information without permission from another party.

3.3.3.6.3. Guidelines

An NDA is required to ensure that internal employees, external service providers and suppliers will not reveal CSP's secrets or any confidential information they are working with. An NDA must be signed before an internal employee, external service provider or supplier is granted access to any confidential information [11].

The NDAs should be reviewed at regular intervals, at least annually. If the review shows that the requirements need to be modified, then the NDA shall be modified accordingly, and the internal employees, external service providers and suppliers must accept it, i.e., the updated NDA must be signed [2].

An NDA can be digitally signed, so that the signing of NDA can be easily monitored in an automatic way by the CSP. The digital signature process also allows the CSP to easily obtain up-to-date status of how many NDAs have been signed and whether the NDAs are up-to-date; identify those internal employees, external service providers and suppliers who have not yet signed the document; and to ensure that those who did not sign have no access to secret or confidential information. Such automatization requires tool support for the monitoring, e.g., Adaptive Non-Disclosure Agreement (NDA) Manager [28].

3.3.4. Reference TOMs for Operational Security

3.3.4.1. Operational Security :: Capacity Management – Monitoring :: OPS-02.2H

The EUCS requirement OPS-02.2H states [2]:

> "**The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards**".

and references as "measures" the following requirement also from OPS-02 Capacity Management – Monitoring:

OPS-02.1H	"The CSP shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement."

3.3.4.1.1. EUCS Security Control

Code	Name	Objective [2]
OPS-02	Capacity management – monitoring	"The capacities of critical resources such as personnel and IT resources are monitored"

3.3.4.1.2. Key concepts

Term	Definition
SLA	Service Level Agreement
Provisioning	Cloud Services provisioning is the allocation of CSP's resources to a CSC.
De-provisioning	Cloud Services de-provisioning is the process of removing CSC's access to the CSP's resources.

3.3.4.1.3. Guidelines

Technical and organizational safeguards related to monitoring the provisioning and de-provisioning of cloud services may cover topics such as the [2]:

- definition and implementation of detective controls (mechanisms used to detect problems in due time)
- system monitoring and tuning: number of transactions, number of users, number of new customers, availability of RAM (Random Access Memory) and disk in peak times, response times for some big queries, etc.)
- identification and analysis of trends of usage.

The CSP may use tools such as load balancers in order to automatically handle the provisioning and de-provisioning of cloud services. These tools may be provided to CSCs to receive relevant information related to capacity and availability that will allow them handling themselves the resources. Usually, the CSP provides a Cloud Resource Manager which enables the Cloud Service Customer to view the deployment history of all cloud services for which the CSP is responsible. The Cloud Service Customer can examine specific operations in past deployments and see which resources were provisioned and un-provisioned.

This information will be useful to react to unexpected events such as unprecedented traffic or to detect any unused resources that may sometimes be redirected or be ridden of, conducting to the provisioning or de-provisioning of cloud services when necessary, in order to maintain good resources levels without major losses of services' quality. [2]

3.3.4.2. Operational Security :: Protection Against Malware – Implementation :: OPS-05.3H

The EUCS requirement states [2]:

> "**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**".

and references as "measures" the following requirements also from OPS-05 Protection Against Malware – Implementation:

OPS-05.1H	"The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures"
OPS-05.2H	"Signature-based and behaviour-based malware protection tools shall be updated at least daily."

3.3.4.2.1. EUCS Security Control

Code	Name	Objective [2]
OPS-05	Protection against malware – implementation	"Malware protection is deployed and maintained on systems that provide the cloud service"

3.3.4.2.2. Key concepts

Term	Definition
Malware	Malicious software such as viruses, spyware, etc.
Antimalware	Solutions, typically in the form of software, to identify and remove malicious software.

3.3.4.2.3. Guidelines

Typically, the CSP shall provide an antimalware solution to identify and remove viruses, spyware, and other malicious software. It shall periodically scan and monitor the activity in Cloud Services such as Virtual Machines to detect and block any malware execution. It shall automatically act on detected malware, such as deleting or quarantining malicious files and generating alerts. This enables the Cloud Service Customer to refine the service and enable troubleshooting.

Core features of the provided antimalware solution shall be, but are not limited to:

- Real-time protection
- Scheduled scanning
- Malware remediation
- Signature updates
- Active protection
- Antimalware event collection

According to ISO/IEC 27002 [11], protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered to ensure a better security [30]:

- Implementing controls that prevent or detect the use of unauthorized software .

- Implementing controls that prevent or detect the use of known or suspected malicious websites.
- Conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated.
- Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis the scan carried should include: any files received over networks or via any form of storage medium, electronic mail attachments and downloads, and web pages.
- Isolating environments where catastrophic impacts may result.

3.3.4.3. *Operational Security :: Data Backup and Recovery – Monitoring :: OPS-07.2H*

The EUCS requirement OPS-7.2H states [2]:

> "**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**".

and references as "measures" the following requirements also from OPS-Operational Security:

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-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-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-08.2H	"The CSP shall not use CSC data, but only data in test accounts controlled by CSP staff for testing purposes."
OPS-08.3H	"The CSP shall thoroughly document restore tests, including the safe disposal of restored data."
OPS-08.4H	"Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation."
OPS-08.5H	"The CSP shall inform CSCs, at their request, of the results of the recovery tests."

3.3.4.3.1. EUCS Security Control

Code	Name	Objective [2]
OPS-07	Data backup and recovery – monitoring	"The proper execution of data backups is monitored"

Dependencies:

- OPS-06: Data Backup and Recovery – Policies
- OPS-08: Data Backup and Recovery – Regular Testing

3.3.4.3.2. Key concepts

Term	Definition
RTO	Recovery Time Objective, the maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or comparable event takes place.
RPO	Recovery Point Objective, the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed as an amount of time.

3.3.4.3.3. Guidelines

CSPs should be capable of providing accesses for their CSCs to allow them to monitor their own backed-up data automatically. This could be done through usual interfaces used internally for monitoring or specific interfaces put in place specifically for customers. These provided accesses should be implemented in compliance with the IAM-09 requirements [30].

Native cloud backup services offered by most CSPs (e.g., Azure backup[8] or AWS backup[9] will offer out of the box the "portal" or API functionalities which implement data backup and recovery services (with exception of the organizational parts from these requirements). Continuous monitoring in this case implies assessing if those services are being deployed by the cloud customer, although the obvious limitation of this approach is that it does not guarantee that the actual configuration has been performed (e.g., data retention times).

Continuous monitoring of the data backup service offered by the CSP will assess the existence of technical configuration properties like those mentioned on OPS-06.1H, which have to do with retention time, backup frequency, RTO/RPO, encryption, and role management. It can be expected that these technical configuration properties can be assessed directly from the data backup service's configuration offered by the CSP[10]. However, it must be noticed that automated assessment can be limited (out of the box) to the data backup services native to the CSP, but not to 3rd party services which are deployed by the cloud customer.

Also, to be noticed is the referenced OPS-08 (recovery procedures), which mostly consists in organizational requirements (e.g., OPS-08.3H), which cannot be expected to be automatically monitored at the state of practice.

3.3.4.4. Operational Security :: Data Backup and Recovery – Storage :: OPS-09.2H

The EUCS requirement OPS-09.2H states [2]:

> "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**".

and references as "measures" the following requirements:

[8] https://docs.microsoft.com/en-us/azure/backup/backup-center-overview

[9] https://docs.aws.amazon.com/aws-backup/?id=docs_gateway

[10] As an example, Azure Policies in the case of Azure backup (https://docs.microsoft.com/en-us/azure/backup/backup-center-overview), or ConfigRules for AWS backup (https://docs.aws.amazon.com/aws-backup/?id=docs_gateway)

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-09.3H	“The data classification of the original data is applied automatically to backups.”
OPS-09.4H	“The security measures at the remote site shall have the same level as at the main site”
CKM-02.1H	“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-02.2H	“The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including employee authentication.”
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.”

3.3.4.4.1. EUCS Security Control

Code	Name	Objective [2]
OPS-09	Data backup and recovery – storage	Backup data is stored at an appropriate remote location

Dependencies:

- CKM-02: Encryption of Data in Transit
- OPS-08: Data Backup and Recovery – Regular Testing

3.3.4.4.2. Key concepts

Term	Definition
RTO	Recovery Time Objective, the maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or comparable event takes place.
RPO	Recovery Point Objective, the maximum acceptable amount of data loss after an unplanned data-loss incident, expressed as an amount of time.

3.3.4.4.3. Guidelines

Requirement OPS-09.2H targets the automatic monitoring of the backup transmission to remote locations. While the automatic monitoring of transporting backups via backup media, like physical disks, is usually not possible, backups to remote locations can be monitored automatically.

For example, cloud providers like Azure and AWS provide redundancy options which also include automatic backups to remote locations, e.g., different regions for Azure Storage Accounts. Depending on the cloud provider and the chosen tier, options include automatic redundancy within a certain region or zone, or replication across zones.

The monitoring of this requirement therefore may be conducted by checking if the configuration of geo-redundant backups in the respective storage services is active. If no such managed backup option is available, the monitoring may be performed by verifying the existence of the respective backup at the remote location.

3.3.4.5. Operational Security :: Logging and monitoring – Identification of events :: OPS-12.1H

The EUCS requirement OPS-12.1H states [2]:

> "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".

3.3.4.5.1. EUCS Security Control

Code	Name	Objective [2]
OPS-12	Logging and monitoring – identification of events	"Logs are monitored to identify security events that may lead to security incidents"

3.3.4.5.2. Key concepts

Term	Definition
Logging data	It is the process of collecting and storing data over a period of time specific to the events that occur in a controlling application (or program) in different systems or environments.

3.3.4.5.3. Guidelines

The CSP may produce a list of potential security incidents and identify the events that trigger those incidents. A risk analysis helps in the identification of critical assets and the results may be used as input for the monitoring of event detection. These events (or combination of events) should then be supervised in higher priority during monitoring of log data. The CSP should use tools that automate log monitoring and are able to trigger alerts to the persons responsible to take appropriate actions. These tools should help the CSP to track the effectiveness of event detection by recording the number of false positives and false negatives, thus improving the calibration of what constitutes suspicious events. [30]

3.3.4.6. Operational Security :: Logging and monitoring – Identification of events :: OPS-12.2H

The EUCS requirement OPS-12.2H states [2]:

> "**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)**".

and references as "measures" the following requirements:

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."
AM-05.1H	"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, and provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives."
AM-05.2H	"When applicable, the CSP shall label all assets according to their classification in the asset classification schema."

3.3.4.6.1. EUCS Security Control

Code	Name	Objective [2]
OPS-12	Logging and monitoring – identification of events	"Logs are monitored to identify security events that may lead to security incidents"

Dependencies:

- AM-05: Asset Classification and Labelling

3.3.4.6.2. Key concepts

Term	Definition
Logging data	It is the process of collecting and storing data over a period of time specific to the events that occur in a controlling application (or program) in different systems or environments.

3.3.4.6.3. Guidelines

To identify events that can lead to security incidents, the CSP may use different means: one possibility is to install agents on computing resources, which can analyse log data on the resource, for instance on a virtual machine. The logs can then be centrally collected and analysed.

Also, the log data created by the cloud system on the management plane of a cloud system may be used to identify security-relevant events, like the creation or modification of certain resources. This is possible to enable in cloud systems, like Azure and AWS, where such events can be stored and analysed in dedicated analytics services.

To automatically ensure that this monitoring is effective, the CSP therefore needs to ensure that the resource-level monitoring is enabled (e.g., installed agents), and/or that management-level monitoring is enabled (e.g., Azure activity logs).

Note also that the retention time for such logs needs to be configured appropriately.

3.3.4.7. Operational Security :: Logging and monitoring – Access, Storage and Deletion :: OPS-13.1H

The EUCS requirement OPS-13.1H states [2]:

> "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**".

and references as "measures" the following requirements:

OPS-13.3H	"Log data shall be deleted when it is no longer required for the purpose for which they were collected."
OPS-13.4H	"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."
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-15.2H	"Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01)"

3.3.4.7.1. EUCS Security Control

Code	Name	Objective [2]
OPS-13	Logging and Monitoring – Access, Storage and Deletion	"The confidentiality, integrity and availability of logging and monitoring data are protected with measures adapted to their specific use"

Dependencies:

- OPS-10: Logging and Monitoring – Policies
- OPS-15: Logging and Monitoring – Configuration

3.3.4.7.2. Key concepts

Term	Definition
Logging data	It is the process of collecting and storing data over a period of time specific to the events that occur in a controlling application (or program) in different systems or environments.

3.3.4.7.3. Guidelines

To fulfil this requirement, the CSP should automatically monitor the effectiveness of the respective logging and monitoring mechanisms as well as incorporate changes in the monitoring configuration based on applicable policies. The CSP should put in place mechanisms to monitor the consolidation process resulting from the aggregation of logging data from various origins, and to keep track of deletion of the logs.

The data produced by the logging and monitoring processes must be stored in order to facilitate access and analysis for monitoring or other purposes. The data is usually stored in a way that allows centralized evaluation, and can contain sensitive private information or information about the system and cloud service functioning such that a breach or unauthorized access is highly undesirable. In addition, storage space is finite, and the longer logs are stored, the greater the security risk to the environment. Thus, once logs have been used for their intended purpose or their legally required storage duration is passed, they should be immediately and safely deleted from the system [30].

Cloud providers like Azure offer managed logging services. In such services, e.g., Azure activity logs, a CSP can simply configure the retention time and monitor its correct settings to fulfil the requirement. For self-created logs, the agents or framework need to provide a way of checking the retention time. Alternatively, the storage that holds the logs needs to be monitored regarding its retention time / deletion mechanisms.

3.3.4.8. Operational Security :: Managing vulnerabilities, malfunctions and errors – online registers :: OPS-18.6H

The EUCS requirement OPS-18.6H states [2]:

> "**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**".

and references as "measures" the following requirements:

OPS-18.2H	"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".
OPS-18.3H	"The CSP shall publish and maintain a publicly and easily accessible online register of known vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or operate under their own responsibility."
OPS-18.4H	"The information contained in the online register shall include sufficient information to form a suitable basis for risk assessment and possible follow-up measures on the part of CSCs."
OPS-18.5H	"The CSP shall consult at least daily 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)."

3.3.4.8.1. EUCS Security Control

Code	Name	Objective [2]
OPS-18	Managing Vulnerabilities, Malfunctions and Errors – Online Registers	"Online registers are used to identify and publish known vulnerabilities"

Dependencies:

- OPS-17: Managing Vulnerabilities, Malfunctions and Errors – Policies

3.3.4.8.2. Key concepts

Term	Definition
Rollout	Launch of new patches or updates when necessary.
Vulnerabilities	The quality of being exposed to attacks.

3.3.4.8.3. Guidelines

The CSP shall maintain an up-to-date online register of vulnerabilities that affect services and assets under its responsibility and also under CSCs' responsibility. Whenever a vulnerability is identified, the CSP should address the vulnerability in parallel, retrieving related information and publishing it on its own online register in order to allow its CSCs understanding the vulnerability and its criticality and acknowledging the way how to handle it. [30]

Unpatched assets are a major security issue in many cloud systems. OPS-18.6H moves the responsibility of providing a mechanism to automate patching by the CSP. It should be possible to distribute software updates to the affected users automatically (without human interaction) and to perform the updates only after explicit approval from the user, the approval should be recorded.

Cloud providers usually offer the possibility of enabling automatic patching for managed resources, like virtual machines. For example, Azure VMs can be patched automatically (or on demand)[11]. In this case, a monitoring can simply check whether the respective configuration is enabled.

[11] https://docs.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching

It depends, however, on the resource type if such a mechanism is available, or if more effort by the CSP is needed. For example, language runtimes in Azure Web Apps may be updated automatically or have to be switched by the user[12].

Note, however, that this requirement concerns assets provided to the CSCs.

3.3.4.9. *Operational Security :: Managing vulnerabilities, malfunctions and errors – system hardening :: OPS-21.1H*

The EUCS requirement OPS-21.1H states [2]:

> "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**".

And references as "measures" the following requirements:

OPS-21.2H	"The hardening requirements for each system component shall be documented."

3.3.4.9.1. EUCS Security Control

Code	Name	Objective [2]
OPS-21	Managing Vulnerabilities, Malfunctions and Errors – System Hardening	"System components are hardened to reduce their attack surface and eliminate potential attack vectors"

3.3.4.9.2. Key concepts

Term	Definition
Hardening	The capacity to reinforce or strengthen a system.

3.3.4.9.3. Guidelines

The goal of hardening a system is to remove any unnecessary functionality to reduce their attack surfaces and to eliminate potential attack vectors. Part of the system hardening elimination process involves deleting or disabling needless system applications, permissions, ports, user accounts, and other features. This will allow to reduce attackers' opportunities to gain access to a mission-critical or critical-infrastructure system's sensitive information. The hardening process should then be updated to include new patches or software versions in the baseline configuration, so that the next time similar systems are deployed, old vulnerabilities are not re-introduced into environments. [30]

To fulfil OPS-21.1H, first, a set of hardening specifications (and assets that should be hardened) needs to be defined and documented. The CSP then needs to monitor the fulfilment according to these specifications. The verification of compliance with the specifications for the hardening of system components can be automatically tested and subsequently documented (logs). For instance, a set of hardened virtual machine images may be defined, and then it can be monitored if the deployed images comply with this set. Further hardening specifications may target the existence of components with known Common Vulnerabilities and Exposures (CVEs) and open ports. If the CSP is using non-modifiable images, the hardening process should be done during the creation of those images. Configuration and log files regarding the continuous availability of the images should be retained.

[12] https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime

Service components can be monitored as part of their secure development lifecycle. Regular checks should run on source repositories of service components. Scans should check for old and vulnerable software dependencies. In addition, regularly executed validation can ensure that newly identified vulnerabilities are discovered quickly.

3.3.5. Reference TOMs for Asset Management

3.3.5.1. Asset Management :: Asset Inventory :: AM-01.4H

The EUCS requirement AM-01.4H states [2]:

> "***The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date***".

and references as "measures" the following requirement also from AM-01 Asset Inventory:

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."

3.3.5.1.1. EUCS Security Control

Code	Name	Objective [2]
AM-01	Asset Inventory	"The CSP has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle"

Dependencies:

- RM-01: Risk Management Policy

3.3.5.1.2. Key concepts

Term	Definition
Asset	Item, thing or entity that has potential or actual value to an organization. The value can be tangible or intangible, financial or non-financial, and include consideration of risks and liabilities.

3.3.5.1.3. Guidelines

Typically, the CSP sets a suitable framework for identifying, classifying and implementing an inventory of IT-processes, systems and components (assets). These assets include the physical and virtual objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of the information in the CSP's area of responsibility, e.g., firewalls, load balancers, web servers, application servers and database servers.

Asset management shall support the rollout of updates and patches. It also shall monitor that only authorized resources are provided access, and that unauthorized and unmanaged resources are identified and removed and where appropriate, determining which components are affected by new security issues.

An inventory of these Software and Hardware assets shall be maintained through automatic means to guarantee that all are up to date. Automation is preferable over a manual process due to efficiency and cost reasons.

Monitoring the process performing the inventory of Software assets means that [20]:

- Assets are tagged.
- All software on the network is actively managed, which means, all software is inventoried, tracked, and corrected, so that only authorized software is installed and executed. Unauthorized and unmanaged software shall be therefore 'found' and prevented from being installed or executed.
- Software inventory tools are used throughout the whole organization and more specifically for the service under certification. These tools allow to keep a catalogue of all software, applications, patches, and versions functioning in the service or resource, as well as to keep track of the changes in the software, resource, or the network. It also allows to manage the licenses of the software assets installed on the service. Furthermore, they also aid in the documentation management.
- Application whitelisting technology is used to ensure that only authorized software is executed, and that all unauthorized software is blocked from being executed on the service's assets.

Monitoring the process performing the inventory of Hardware assets means [20]:

- To manage actively all hardware devices. This means to inventory, track and correct them so that only authorized devices are provided access, while unauthorized and unmanaged devices are found and prevented from gaining access.
- To use an active discovery tool in order to identify devices that are connected and update the hardware asset inventory accordingly.
- To maintain an up-to-date and accurate inventory of assets that have the potential to store or process information.

In order to perform automated monitoring of the process performing the inventory of assets the following practices are often considered:

- Make an inventory of all the assets within the cloud service, such as the software, the network interfaces, etc. Large CSPs allow the retrieval of the Cloud inventory with services such as the Azure Resource Graph[13] or AWS Config.
- Ensure that all the appropriate permissions in the tenant are granted. Role-based Access control is an appropriate method for this as it allows segregation of duties.
- Tag the assets and organize them so they can be accessible by different groups of users, also, if applicable, with different policies. For each asset, record its identification data, function, model and version and location.
- Review the inventory on a regular basis to ensure that unauthorized resources are deleted.
- Log at least all changes to the information related to risk management
- Also, query regularly the assets and resources to make sure that they are present in the approved service.
- Ensure appropriate (read) permissions in the tenant.
- Automate the collection of information about all software on resources. Examples: software name, version, publisher, refresh time, install date and other information.

3.3.5.2. Asset Management :: Commissioning and Decommissioning :: AM-03.4H

The EUCS requirement AM-03.4H states [2]:

[13] https://docs.microsoft.com/en-us/azure/governance/resource-graph/first-query-portal

> “**The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored**”.

and references as “measures” the following requirements also from AM-03 Commissioning and Decommissioning:

AM-03.1H	"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, including those defined in RM-01, to ensure that the risks arising from the commissioning are identified, analysed and mitigated."
AM-03.2H	“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.”

3.3.5.2.1. EUCS Security Control

Code	Name	Objective [2]
AM-03	Commissioning and decommissioning	“Procedures for the commissioning and decommissioning of hardware assets used in the provision of the cloud service are documented, communicated and implemented, ensuring the proper configuration before commissioning and the proper deletion of data during decommissioning”

Dependencies:

- RM-01: Risk Management Policy

3.3.5.2.2. Key concepts

Term	Definition
Commissioning	The process of ensuring that all the hardware components are designed, installed, tested, operated, and maintained according to the operational requirements of the owner and tenants.
Decommissioning	The process of removing hardware components from the active status ensuring that appropriate security measures are taken prior to reuse/disposal, including hard drive reformatting.
Asset	Item, thing or entity that has potential or actual value to an organization. The value can be tangible or intangible, financial or non-financial, and include consideration of risks and liabilities.

3.3.5.2.3. Guidelines

A commissioning and decommissioning process shall be documented so that it can be properly apply and monitored. Whenever a server is removed from service or placed into service, the process shall be documented with decommissioning and commissioning documents. There shall also exist a digital log of the commissioning and decommissioning requests.

The commissioning hardware process should include the automatic monitoring and verification of the existence of a documented procedure accessible to all internal and external employees for the commissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures. The identification and management of the risks arising from the commissioning are included in that process. The commissioning procedure shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication, and authorisation according to the intended use and based on the applicable policies before authorization to commission the asset can be granted.

The decommission of hardware process should include the automatic monitoring and verification of the existence of a documented procedure accessible to all internal and external employees for the decommissioning of hardware that is used to provide the cloud service in the production environment, requiring approval based on applicable policies. The decommissioning procedure shall include the complete and permanent deletion of the data or the proper destruction of the media, The process may differ from every hardware type or technology, but some basics steps include: identify and record the hardware assets that need to be decommissioned, create a log of all actions performed during the server decommissioning including the certificate of erasure/destruction, terminate the contracts, create backups, wipe data, unplug, cut power and remove, and destroy server. [32]

3.3.5.3. Asset Management :: Acceptable use, safe handling and return of assets :: AM-04.1H

The EUCS requirement AM-04.1H states [2]:

> "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**".

and references as "measures" the following requirement from AM-02 Acceptable Use and Safe Handling of Assets Policy:

AM-02.1H	"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."

3.3.5.3.1. EUCS Security Control

Code	Name	Objective [2]
AM-04	Acceptable use, safe handling and return of assets	"The CSP's internal and external employees are probably committed to the policies and procedures for acceptable use and safe handling of assets before they can be used if the CSP has determined in a risk assessment that loss or unauthorised access could compromise the information security of the cloud service"

Dependencies:

- AM-02: Acceptable Use and Safe Handling of Assets Policy

3.3.5.3.2. Key concepts

Term	Definition
Removable media	Any type of data storage device that can be removed from a computer while the system is running. They are usually portable devices.

3.3.5.3.3. Guidelines

The CSP needs to monitor the assurance that internal and external employees are committed to the policies and procedures for acceptable use and safe handling of assets, by automatically monitoring and verifying the following policies and procedures related to the asset lifecycle: [30]

- Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components
- Inventory
- Classification and labelling based on the need for protection of the information and measures for the level of protection identified

- Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation
- Requirements for versions of software and images as well as application of patches
- Handling software that is no longer supported and no longer has security patches
- Restriction of software installations or use of services
- Protection against malware
- Remote deactivation, deletion or blocking
- Physical delivery and transport
- Dealing with incidents and vulnerabilities
- Complete and irrevocable deletion of the data upon decommissioning.

3.3.6. Reference TOMs for Physical Security

3.3.6.1. Physical Security :: Physical Site Access Control :: PS-02.8H

The EUCS requirement PS-02.8H states [2]:

> "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**".

and references as "measures" the following requirements also from PS-02 Physical Site Access Control:

PS-02.1H	"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, including requirements on the physical access control measures to be implemented."
PS-02.7H	"The access control policy shall include measures to identify individual visitors and third-party personnel, incorporating them into the access policy system, thereby monitoring and escorting the building access during their stay."

3.3.6.1.1. EUCS Security Control

Code	Name	Objective [2]
PS-02	Physical site access control	"Physical access through the security perimeters are subject to access control measures that match each security area's requirements and that are supported by an access control system"

3.3.6.1.2. Key concepts

Term	Definition
Physical access control	These are types of physical security measures designed to restrict or allow access to a certain area or building.

3.3.6.1.3. Guidelines

Physical security measures should be in place to restrict and monitor for unauthorized access to the buildings which contain sensitive or critical information, information systems, or other network infrastructure. A mix of prevention and detection measures must be defined for each level and confirmed incidents must be documented and tracked to resolution.

The maintenance of data centres must be performed by authorized personnel at designated intervals and targets recommended by the suppliers. Maintenance records are stored for the agreed upon time intervals and then properly and permanently destroyed thereafter. Physical access to data centres requires management approval and documented specification of but not limited to: [30]

- account type (e.g., standard, visitor, or supplier)
- access privileges granted
- intended business purpose
- visitor identification method, if applicable
- temporary badge issued, if applicable
- access start date
- access duration (with end date)

In order to perform the automated monitoring of access to non-public areas by unauthorized personnel a “loggable” access control must be implemented that allows to consider the following practices : [33]

- Detect unauthorized access attempts by monitoring the use of deactivated entitlements (e.g., expired/revoked badges or permits, etc.) to access restricted non-public areas.
- Detect suspicious accesses by inspecting any irregular/anomalous behaviours, such as a guard in day shifts that accesses at night-time, for instance.

3.3.7. Reference TOMs for Identity, Authentication and Access Control Management

3.3.7.1. Identity, Authentication and Access Control Management :: Locking, unlocking and revocation of user accounts :: IAM-03.1H

The EUCS requirement IAM-03.1H states [2]:

> “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 IAM-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”.

and references as “measures” the following requirements:

IAM-02.1H	“The CSP shall define policies for managing accounts, according to ISP-02, in which at least the following aspects are described: (1) Parameters to be considered for making access control decisions; (2) Assignment of unique usernames; (3) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type; (4) Events and periods of inactivity leading to blocking and revoking accounts."
IAM-02.2H	“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.”
IAM-02.3H	“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. IAM-01) and with the policies for managing accounts.”
IAM-02.4H	“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.”

3.3.7.1.1. EUCS Security Control

Code	Name	Objective [2]
IAM-03	Locking, Unlocking and revocation of User Accounts	"Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse"

Dependencies:

- IAM-02: Management of User Accounts

3.3.7.1.2. Key concepts

Term	Definition
Revocation of user accounts	This action implies the permanent disablement of the user account and prevents any user with the same name from being create.
Locking user accounts	The user account cannot be used during a specific period of time.
Unlocking user accounts	The user account can be used again after a period of inactivity.

3.3.7.1.3. Guidelines

To ensure the security of the cloud service, identity, authentication, and access control management is needed. Specifically, accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse[14].

Locking an account implies that the user is denied access temporarily from the account, the privileges and access rights associated to the account are not modified, the user needs to follow a procedure involving an administrator or system component in order to get the account unlocked. Revoking an account is a stronger measure, which implies that the user is denied access from the account, the privileges and access rights associated to the account are revoked, and it may be possible to re-create an account with the same identifier, but the access rights then must be provisioned again to the account, following the normal procedure. [30]

Hence, to be compliant with IAM-03 first it is important to set up a period of time in which it is allowed for an account to be inactive. Passed that time, the account shall be disabled, or an alert shall be sent to the user for an action to be taken in compliance with the policy and procedures defined under the ISP category. Secondly, the automated monitoring tool to be set up must verify that this alert was sent or that the disabling occurred on the interval of time specified. For this, the logs of the events produced by the automated mechanisms could be monitored.

All accounts should be automatically monitored to ensure that any account that has been inactive for more than the maximum period of inactivity associated to that account is indeed locked, and that the maximum period of inactivity associated to the account does not exceed two months. After this maximum period of inactivity is reached, the user account should be locked, so the user should be denied any attempt to authenticate. Typically, if a user attempts to connect to a locked account, they should be warned of the status of the account. Deviations should be detected and signalled to authorized personnel (e.g., administrator). [30]

[14] https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-identity-management#im-2-manage-application-identities-securely-and-automatically

3.3.7.2. Identity, Authentication and Access Control Management :: Locking, unlocking and revocation of user accounts :: IAM-03.2H

The EUCS requirement IAM-03.2H states [2]:

> "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 IAM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, **and automatically monitor its application**".

and references as "measures" the following requirements:

IAM-02.1H	"The CSP shall define policies for managing accounts, according to ISP-02, in which at least the following aspects are described: (1) Parameters to be considered for making access control decisions; (2) Assignment of unique usernames; (3) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type; (4) Events and periods of inactivity leading to blocking and revoking accounts."
IAM-02.2H	"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."
IAM-02.3H	"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. IAM-01) and with the policies for managing accounts."
IAM-02.4H	"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."

3.3.7.2.1. EUCS Security Control

Code	Name	Objective [2]
IAM-03	Locking, Unlocking and revocation of User Accounts	"Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse"

Dependencies:

- IAM-02: Management of User Accounts

3.3.7.2.2. Key concepts

Term	Definition
Revocation of user accounts	This action implies the permanent disablement of the user account and prevents any user with the same name from being create.
Locking user accounts	The user account cannot be used during a specific period of time.
Unlocking user accounts	The user account can be used again after a period of inactivity.

3.3.7.2.3. Guidelines

When a user fails to login after a specified number of tries, the user account should be "blocked". The maximum number of tries should be defined and built into the service by default. To provide flexibility, configuration options should also include the possibility to further reduce this number of authentication attempts according to the threat environment, type of user's account privilege and authentication type used. For example, an account with 2FA or a hardware MFA token may be allowed to attempt authentication a few more times than an account that authenticates using only a password.

All accounts should be automatically monitored to ensure that the number of failed authentication attempts has not been exceeded without incurring the blocking of an account. Deviations should be detected and signalled to authorized personnel (e.g., administrator). [30]

3.3.7.3. Identity, Authentication and Access Control Management :: Locking, unlocking and revocation of user accounts :: IAM-03.5H

The EUCS requirement IAM-03.5H states [2]:

> "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 IAM-02 for user accounts, **and automatically monitor its application".**

and references as "measures" the following requirements:

IAM-02.1H	"The CSP shall define policies for managing accounts, according to ISP-02, in which at least the following aspects are described: (1) Parameters to be considered for making access control decisions; (2) Assignment of unique usernames; (3) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type; (4) Events and periods of inactivity leading to blocking and revoking accounts."
IAM-02.2H	"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."
IAM-02.3H	"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. IAM-01) and with the policies for managing accounts."
IAM-02.4H	"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."

3.3.7.3.1. EUCS Security Control

Code	Name	Objective [2]
IAM-03	Locking, Unlocking and revocation of User Accounts	"Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse"

Dependencies:

- IAM-02: Management of User Accounts

3.3.7.3.2. Key concepts

Term	Definition
Revocation of user accounts	This action implies the permanent disablement of the user account and prevents any user with the same name from being create.
Locking user accounts	The user account cannot be used during a specific period of time.
Unlocking user accounts	The user account can be used again after a period of inactivity.

3.3.7.3.3. Guidelines

If an account remains continuously blocked for a period of time, then the account should be automatically revoked. A revoked account is for all intents and purposes, the same as a "deleted" account. Its information should only serve as record for historical purposes.

A default duration should be defined by the CSP. For the accounts associated to users under the responsibility of the CSP (e.g., employees, contractors), this duration should not be set to more than 6 months. To provide flexibility, clients' configuration may also include the option to modify this duration of maximum blocked status according to their threat environment.

All accounts should be automatically monitored to ensure that any account that has been blocked for more than the maximum period of continuously blocked state associated to that account is indeed revoked. Deviations should be detected and signalled to authorized personnel (e.g., administrator). The CSP should use applications that automate detection of deviations to the defined user account revocation. [30]

3.3.7.4. Identity, Authentication and Access Control Management :: Locking, unlocking and revocation of user accounts :: IAM-03.6H

The EUCS requirement IAM-03.6H states [2]:

> "**The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant**".

3.3.7.4.1. EUCS Security Control

Code	Name	Objective [2]
IAM-03	Locking, Unlocking and revocation of User Accounts	"Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse"

3.3.7.4.2. Key concepts

Term	Definition
Revocation of user accounts	This action implies the permanent disablement of the user account and prevents any user with the same name from being create.
Locking user accounts	The user account cannot be used during a specific period of time.
Unlocking user accounts	The user account can be used again after a period of inactivity.

3.3.7.4.3. Guidelines

The CSP should use automated context-based security techniques during user authentication to flag events that are suspicious and notify the user or administrators. An example of such is "geolocation" where a user whose IP at last login shows s/he is logging in from Europe should not have an IP from East Asia when s/he attempts to login again two hours later.

In this requirement, the strength of the authentication mechanisms is very important as it builds on top of the authentication mechanisms strength of the previous IAM-03 control requirements. This includes among other aspects the protection level of the passwords, the use of a centrally managed authentication method, and so on.

Having strong authentication methods can reduce significantly suspicious events. However, other practices should be put in practice such as single sign on, multi-factor authentication, multi-factor authentication with conditional access policy, role-based access control (RBAC), to name a few.

The automated monitoring of authentication attempts should consider at least the following aspects:

- Number of authentication attempts, which can be seen in the logs.
- Sign-ins of users, that is, who has logged in into the service and how the service and resources have been used. This can be seen by monitoring the logs.
- Suspicious sign-in such as brute-force attacks, leaked credentials, unfamiliar locations, time schedule or devices. This can be seen by analysing the logs.
- Enable alerts for these suspicious activities so that the customer is informed.

3.3.8. Reference TOMs for Change and Configuration Management

3.3.8.1. Change and Configuration Management :: Approvals for provision in the production environment :: CCM-04.1H

The EUCS requirement CCM-04.1H states [2]:

> “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**”.

3.3.8.1.1. EUCS Security Control

Code	Name	Objective [2]
CCM-04	Approvals for Provision in the Production Environment	“Changes to the cloud services are approved before being deployed in the production environment”

3.3.8.1.2. Key concepts

Term	Definition
Production environment[15]	Set of computing resources where finished, user-ready software is deployed and executed.

3.3.8.1.3. Guidelines

Typically, the CSP sets a secure baseline configuration to ensure the security of the delivered cloud service, described in the CSP’s Configuration Management Plan [34]. Although the configuration of the service is in constant change, it cannot be deployed without being approved in order the minimize the risks of failure upon implementation. These modifications to the architecture configuration are often are very frequent, so it is advisable to automatically monitor the approvals of these changes deployed in the production environment to ensure they are done before they are made available to CSCs in the production environment.

When changes impact CSC’s services, the CSP should make sure to involve the CSCs in the approval processes in accordance with the contractual agreements and before changes are made available in the production environment. In these situations, the cloud customers can ensure through suitable controls that authorized and qualified personnel receive the information made available, assesses the impact on the ISMS framework and decides on the approval in accordance with the conditions specified by the Cloud Service Provider. [30]

[15] https://www.suse.com/suse-defines/definition/production-environment/

Tools can be used to provide the administrator with an overview of all the approvals[16]. A checking process could carry out to check actual results against estimates. If this process is successfully passed, an approval could be maintained. The results of the tests performed can be documented by means of logs, which can then be automatically and continuously evaluated by the auditor.

3.3.8.2. Change and Configuration Management :: Performing and logging changes :: CCM-05.1H

The EUCS requirement CCM-05.1H states [2]:

> “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**”.

and references as “measures” the following requirement:

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."

3.3.8.2.1. EUCS Security Control

Code	Name	Objective [2]
CCM-05	Performing and Logging Changes	“Changes to the cloud service are performed through authorized accounts and traceable to the person or system component who initiated them”

Dependencies:

- IAM-01: Policies for Access Control to Information

3.3.8.2.2. Key concepts

Term	Definition
Production environment[17]	Set of computing resources where finished, user-ready software is deployed and executed.

3.3.8.2.3. Guidelines

Usually, the CSP sets a secure baseline configuration to ensure the security of the delivered cloud service, described in the CSP’s Configuration Management Plan [34]. Although the configuration of the service is in constant change, the modifications in the configuration of the architecture needs to be authorised and traceable.

[16] https://docs.microsoft.com/en-us/azure/devops/pipelines/process/approvals?view=azure-devops&tabs=check-pass

[17] https://www.suse.com/suse-defines/definition/production-environment/

Once a change has been made in the production environment , its identifier must be stored and matched with the person responsible for the change for a late consultation if necessary (in particular to check permissions, authorisations, later on). These data could be stored in a stack[18], in a queue, or by other means.

The changes to the role and rights concept can be documented in logs by the CSP. Thus, an automatic and continuous evaluation of these logs can be carried out, where irregularities could be detected and logged. Subsequently, the auditor can perform a continuous audit by automatically evaluating the logs and logged irregularities. [30]

3.3.9. Reference TOMs for Procurement Management

3.3.9.1. Procurement Management :: Monitoring of compliance with requirements :: PM-04.7H

The EUCS requirement PM-04.7H states [2]:

> “**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)**”.

3.3.9.1.1. EUCS Security Control

Code	Name	Objective [2]
PM-04	Monitoring of Compliance with Requirements	“Monitoring mechanisms are in place to ensure that third-parties comply with their regulatory and contractual obligations”

3.3.9.1.2. Key concepts

Term	Definition
CSPM	Cloud Security Posture Management service automates the identification and remediation of risks across cloud infrastructures.

3.3.9.1.3. Guidelines

At the state of practice, this requirement can be implemented by documenting the processes adopted by the CSP to leverage its Cloud Security Posture Management service (CSPM). Most commercial (and CSP-native) CSPMs will implement at least the automated monitoring aspects mentioned in the requirement, although some degree of customization might be needed to guarantee that new standard controls frameworks (e.g., EUCS) are integrated into the CSPM. Furthermore, the CSP should consider that integration with 3rd party tools (e.g., ITS) might be required to guarantee that aspects like response/recovery times are also properly monitored.

It has been observed that Gartner’s “magic quadrant” of CSPMs [35] are still on its early days related to multi-cloud support, so it is still a common practice to rely on more than one CSPM tool (despite the evident cost of ownership issues).

[18] https://www.elastic.co/guide/en/kibana/master/production.html

Also, current CSPMs are limited in the sense that only in-cloud compliance can be monitored i.e., it is usually not possible to monitor compliance of non-cloud services like HR Training databases. In these cases, another sort of automated monitoring system/organizational process should be implemented by the CSP.

Finally, notwithstanding the underlying technology being leveraged by the CSP, it must be guaranteed that the corresponding procedures are documented and integrated into the operational processes of the CSP.

3.3.9.2. Procurement Management :: Monitoring of compliance with requirements :: PM-04.8H

The EUCS requirement PM-04.8H states [2]:

> “**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**”.

3.3.9.2.1. EUCS Security Control

Code	Name	Objective [2]
PM-04	Monitoring of Compliance with Requirements	“Monitoring mechanisms are in place to ensure that third-parties comply with their regulatory and contractual obligations”

3.3.9.2.2. Key concepts

Term	Definition
Monitoring	To keep track of the system state and behaviour with the aim to detect and notify nonconformities.

3.3.9.2.3. Guidelines

As in the case of PM-04.7H, the deployment of a CSPM service can implement (at least partially) this PM-04.8H requirement. The vast majority of CSPMs implement some sort of notification mechanism to make responsible stakeholders aware of detected violations and discrepancies. CSPs should also look for CSPM features allowing ITS integration, which can greatly expand the notification/reporting capabilities of out-of-the-box CSPMs. This (automated) monitoring may also lead to the identification of nonconformities, which may need to be reported to the CAB as part of the CSP’s continuous monitoring obligations.

Challenges related to the implementation of PM-04.8H can be expected due to the heterogeneity of CSP’s implementations/platforms, where no single CSPM/ITS might be able to integrate all expected notifications/interoperability features. In analogy to PM-04.7H, CSPs are expected to rely on multiple technologies/products to integrate in their own IT systems for guaranteeing that related notifications are managed in accordance with EUCS.

3.3.10. Reference TOMs for Incident Management

3.3.10.1. Incident Management :: Processing of security incidents :: IM-02.5H

The EUCS requirement IM-02.5H states [2]:

> “**The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures**”.

3.3.10.1.1. EUCS Security Control

Code	Name	Objective [2]
IM-02	Processing of Security Incidents	"A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner"

3.3.10.1.2. Key concepts

Term	Definition
Security incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.[19]

3.3.10.1.3. Guidelines

Typical monitoring could occur through analysis a ticket management or other business process management system. This monitoring shall ensure that all the activities of the methodology for the processing of security incidents are performed and fulfilled. i.e., incident detections, categorization, resolution, etc. [30]

3.3.11. Reference TOMs for Compliance

3.3.11.1. Compliance :: Internal audits of the internal control system :: CO-03.5H

The EUCS requirement CO-03.5H states [2]:

> "**Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions**".

3.3.11.1.1. EUCS Security Control

Code	Name	Objective [2]
CO-03	Internal Audits of the Internal Control System	"Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements"

3.3.11.1.2. Key concepts

Term	Definition
ISMS	Information Security Management System

3.3.11.1.3. Guidelines

This requirement is in the heart of continuous monitoring, as it is a requirement utilizing all the other requirements involving automatic monitoring. In practice, this requirement aims to ensure that the policy statements and requirements from policies and instructions are automatically monitored. What this means, is that the automated monitoring associated with internal audit for that specified scope shall cover all the requirements set in the organization's ISMS. Therefore, this TOM must be adjusted for the internal audit scope. If the scope of the internal audit is the whole ISMS, the automated monitoring shall cover all the requirements set by policies and instructions in the ISMS scope.

The automatic evaluation of this requirement is twofold: firstly, the overall compliance is evaluated as a percentage of the automatically monitored requirements, where the target value

[19] https://csrc.nist.gov/glossary/term/security_incident

is 100 %. Secondly, fulfilment of this requirement needs an evaluation of whether the assessed component is compliant or not.

The assessment can be made by comparing the requirements in scope to automated monitoring processes. Each requirement in scope shall have a functioning automated monitoring process. Each monitoring process shall be linked to monitored assets which define the scope for the specified requirement. If there are existing monitoring processes but they are not implemented to all assets in scope, it lowers the percentage of automated monitoring coverage. With this information, an example table can be created to illustrate the evaluation process for this requirement. In Table 10 imaginary assets and requirements are used for illustration purposes.

Table 10. Example of an evaluation process (source: MEDINA's own contribution)

Requirement	Percentage of target assets monitored	Monitoring process(es)	Compliance status in specified timeframe	Nonconforming measurements
OIS-02.4H	100 % (1/1)	<link to measurement>	OK	N/A
HR-04.3H	0% (0/0)	<asset_X_measurement not defined>	N/A	N/A
OPS-07.2H	66 % (2/3)	<link to measurement_1> <link to measurement_2> <asset_Y_measurement not defined >	NOT OK	<nonconformity in measurement 1>

When calculating the results of the measurement, they can ultimately be presented in a more compact view with the following information:

Percentage of compliance monitors in place for the scope	< calculated percentage of assets monitored for all requirements in scope>
Compliance status (number of nonconformities)	<sum of all nonconformities>

3.3.11.2. Compliance :: Internal audits of the internal control system :: CO-03.6H

The EUCS requirement CO-03.6H states [2]:

> "**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**".

3.3.11.2.1. EUCS Security Control

Code	Name	Objective [2]
CO-03	Internal Audits of the Internal Control System	"Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements"

3.3.11.2.2. Key concepts

Term	Definition
ISMS	Information Security Management System

3.3.11.2.3. Guidelines

The conformity to this requirement consists of two sub-requirements which are applied to each monitored asset. First, it is monitored whether the asset in scope is identified to be vulnerable and secondly, it is monitored if the asset is deviating. Deviation could be challenging to define, but in this context, it is defined as a nonconformity to any measurement applied to that asset since the measurement requirements set a baseline for conformity.

The first part of this requirement is measured by checking whether the asset is vulnerable. There could be industrial tools for doing this, but the simple way of doing this is to compare if the target asset version is known to be vulnerable. For example, for software components it is relatively easy to see if the software is updated to the latest version. Alternatively, the measurement can be made against a list of known vulnerable versions since the latest software version can be vulnerable. The measurement can be supplemented with other information which is not mandatory but could be beneficial. Table 11 shows an example of vulnerable assets identifying version number and identified vulnerability. The provided information may vary depending on the measurement tool’s capabilities.

Table 11. Example of vulnerable assets (source: MEDINA’s own contribution)

Target asset	Is vulnerable (TRUE/FALSE)	Version	Vulnerability
Asset_1	TRUE	1.1.2	CVE-2021-XXXX
Asset_2	FALSE	2.3.4	N/A

The second part of this TOM is to measure whether the asset is deviating. This is measured by assessing if the target asset is nonconforming to any of the requirements applied to it. This can be done with a simple Boolean operation, where conformity is 0 and nonconformity is 1. By applying a simple logical OR-operation the overall status can be calculated: If there is a single nonconformity, the result for the assessment is 1, indicating a nonconformity, or deviation in this context. Table 12 presents the simplified output with two measurements.

Table 12. Example of a deviating asset (source: MEDINA’s own contribution)

Asset	Measurement result 1	Measurement result 2	Is deviating? (TRUE / FALSE)
A	0	1	TRUE
B	0	0	FALSE

The final part of the requirement is to automatically report the findings to the CSP’s subject matter experts. The reporting functionality should be built into the system itself. Of course, there can be a metric to measure whether the automatic reporting is working or not, but it is not in the focus of this TOM as the reporting of nonconformities is built into the MEDINA framework itself.

3.3.12. Reference TOMs for Dealing with Investigation Requests from Government Agencies

3.3.12.1. Investigation Requests from Government Agencies :: Conditions for access to or disclosure of data in investigation requests :: INQ-03.4H

The EUCS requirement INQ-03.4H states [2]:

> “**The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01**”.

and references as “measures” the following requirement:

INQ-01.1H	“The CSP shall subject investigation requests from government agencies to a legal assessment by subject matter experts.”
INQ-01.2H	“The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken.”

3.3.12.1.1. EUCS Security Control

Code	Name	Objective [2]
INQ-03	Conditions for Access to or Disclosure of Data in Investigation Requests	“Investigators only have access to the data required for their investigation after validation of the legality of their request”

Dependencies:

- INQ-01: Legal Assessment of Investigative Inquiries

3.3.12.1.2. Key concepts

Term	Definition
Disclosure of data	The process of granting the right to examine data and the right to create or retain a copy.

3.3.12.1.3. Guidelines

Government agencies can request access to CSP’s systems to perform investigations. These requests need to be legally assessed by the legal department (or company) of the CSP in order to accept or reject them and to determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken.

3.3.13. Reference TOMs for Product Security

3.3.13.1. Product Security :: PSS-04 IMAGES FOR VIRTUAL MACHINES AND CONTAINERS :: PSS-04.2H

The EUCS requirement PSS-04.2H states [2]:

> “**An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails**”.

and references as “measures” the following requirement:

PSS-04.1H	"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."

3.3.13.1.1. EUCS Security Control

Code	Name	Objective [2]
PSS-04	Images for Virtual Machines and Containers	“Services for providing and managing virtual machines and containers to customers include appropriate protection measures”

3.3.13.1.2. Key concepts

Term	Definition
Integrity check	The process to confirm that all the necessary measures to prevent any unauthorized access to the related systems and files have been taken.
Images of virtual machines	A virtual machine image is a file which contains a virtual disk that has a bootable operating system installed on it. It is a compute resource that uses software instead of a physical computer to run programs and deploy applications.

3.3.13.1.3. Guidelines

If the CSP provides a service to manage virtual machines or containers to its customers, integrity checks of these virtual machines' or containers' images shall be performed automatically at start-up.

Data integrity checks are normally performed using a hash value calculation. The verified hash values for the images of virtual machines or containers shall be compared to a reference which is confirmed to be correct in order to ensure the images have not been tampered with. When a deviation is detected indicating a manipulation of the virtual machine or container image in question, the CSC shall be automatically notified. Starting the virtual machines or containers based on images with unconfirmed or deviated integrity values could also be automatically prevented.

Apart from notifying the CSC, the deviations detected shall also be reported to the responsive experts appointed by the CSP to analyse the deviation and its cause and prevent further damage. Security incident procedures shall be followed.

4. Security Metrics for the Continuous Cloud Certification

4.1. Motivation

Merriam-Webster defines a metric as a standard of measurement [36]. NIST 800-55 [37] standardizes the term measures for metrics to “*mean the collection, analysis, and reporting*”.

Metrics shall measure the efficiency and effectiveness of the technical and organizational measures put in place, in order to evaluate their accomplishment, so that corrective or improvement actions can be taken in case the goals are not reached.

Metrics can be obtained at different levels: organizational level, service level, system level, resource level or software level. These metrics can be later on aggregated, depending on the complexity of the asset or - in the case of the EUCS -, the complexity of the cloud service. Metrics are an indicator of the accomplishment of goals which should be consistently implemented through security requirements across the organization.

Metrics must yield quantifiable information for comparison purposes and allow to be collected on a regular basis so that these can also be compared to a baseline value or the “operational effectiveness” within a given period of time - such as six months or a year- can be evaluated. To achieve that, metrics often have formulas, and are represented as percentages or numbers (integers, real, Booleans) or reference values within interval (scales). For continuous monitoring approaches, such as the one in MEDINA, it is also important to provide the frequency in which a metric shall be gathered.

For measurements to be relevant they must be easily obtainable, and the process shall be consistent, reproducible, and repeatable. The effort of setting up a process or a tool to automate the collection and assessment of metrics is rather a complex one, so when applying an approach similar to the one like MEDINA, a trade-off cost-benefit must be sought.

The major benefits of applying a metrics-oriented approach are to [37]:

- **Increase Accountability,** as it helps to identify security controls that are implemented incorrectly, are not implemented, or are ineffective.
- **Improve Information Security Effectiveness,** as it allows organizations to quantify improvements and demonstrate progress in quantifiable way. It also allows to determine the effectiveness of the processes, procedures, and security controls put in place by the organization.
- **Demonstrate Compliance** with laws, rules and regulations, thanks to the regular and continuous collection of data (evidence).
- **Provide Quantifiable Inputs for Resource Allocation Decisions**, as it can support risk-based decision-making by providing quantifiable information to the risk management process measuring successes or failures, justifying investments, and so on.

The definition of good metrics is fundamental in MEDINA because several tools depend heavily on them, such as:

- **The Metric recommender** (see D2.4 [20]: this tool recommends a metric or set of metrics using pre-trained networks. It takes the definition of the metric as well as the security requirement text and puts it into an embedded feature space selecting the metric or metrics nearest to a requirement.
- **The MEDINA ontology and rules** (see D2.4 [20]): the metrics can be mapped to the MEDINA ontology, that offers a vendor-independent way to describe technical evidence.

- **Evidence Management Tools** (e.g., Clouditor, Wazuh, VAT, Codyze, NLP and AMOE. See D3.2 [4] and D3.5 [38]) which take this information as input.

4.2. Security metrics in MEDINA

At the time of writing, MEDINA partners have defined and implemented **54 metrics** to cover the 34 requirements (of high assurance level and continuous assessment) from the EUCS 2022 version scheme (cf. Section 3.1). These metrics are listed in Table 14.

However, the number of metrics defined in MEDINA is higher, **152 in total**. The reason of this is twofold: firstly, because some of the metrics elicited are not associated with any of those requirements but are of more generic purpose (see Section 4.3 dedicated to Techniques), and secondly, because other metrics are associated with EUCS requirements of different levels out of "the 34", that can be measured with the tools. These additional metrics can be used to demonstrate the effectiveness of the MEDINA project for different assurance levels.

Metrics have been created and elicited by the MEDINA partners for the purpose of the MEDINA project, to be measured by the MEDINA tools, and being compliant with the EUCS scheme. For the elicitation of the security metrics, MEDINA consortium partners have also consulted several sources as:

- NIST 800-55 r1 [37]
- EU funded projects such as EU FP7 CUMULUS [39], A4Cloud [40], SPECS [41]
- Literature [42], [43], [44], [45], [46]

Note that the number of metrics is considerably lower than what was reported in the first version of this deliverable (D2.1 [1]). This is because, in the first iteration, we focused on creating a large number of metrics without aligning them with the available tools and how they could actually measure them. In this second iteration we have completely refactored the metric list, focusing on high-quality metrics that are actionable and can be implemented in the MEDINA tools.

The metrics have been defined according to a structure shown in Table 13.

Table 13. Structure of the definition of the MEDINA metrics (source: MEDINA's own contribution)

Field	Explanation
MetricID	Unique identified of the metric
ReqID	Identifier of the EUCS security requirement
Control	EUCS control name
Metric Name	Name given to the (MEDINA) metric
Source	Source where the metric comes from, that is, if it comes from the literature, or if it comes from the project itself. If this is the case, the value is "EUCS"
Description	Explanation of the objective of the metric. It also often includes the formula needed to measure it
Scale	The valid values of the metric. Examples: >=0, [1;100], [true; false]
Operator	Valid logical operator to compare the metric value with a target value. This can be: =, >, >=, …
Target Value	The expected value that the metric should have. This is the value to which the different MEDINA tools (e.g., Clouditor, VAT, Wazuh, Codyze, AMOE) will compare the results against in order to assess the compliance.
Target Value Datatype	This indicates whether the data is of type integer, Boolean, real or any other type.

Interval (hours)	Indicates the frequency, i.e., how often a metric shall be collected. It can be daily, annual or event driven
Target/Asset	States which asset of the cloud service is affected by the metric. It can be a software, a person, a resource, or the organization itself.

Table 14 shows the metrics that have been defined and implemented at the time of writing by MEDINA partners to cover the 34 high level EUCS requirements identified in Table 9. A more complete list, with the definition and details of the metrics following the structure presented in Table 13 can be found in *Appendix 2: MEDINA Security metrics*.

The "Type" column identifies the type of the requirement: technical (tech) or organizational (org). Please note that the requirement is considered organizational if it implies the monitoring of a static policy document.

Table 14. Metrics implemented in MEDINA to cover the 34 high level EUCS requirements in M27 (source: MEDINA's own contribution)

EUCS Category	EUCS Req. ID	Type	Metric ID	# Metrics
Organization of Information Security	OIS-02.4H	Tech	MixedDuties	1
Information Security Policies	ISP-03.5H	Tech		0
Human Resources	HR-03.4H	Tech & Org	InformationSecurityPolicyAcknowledgementQ1	1
	HR-04.3H	Tech		0
	HR-05.2H	Tech	AccessRightManagementQ1	1
	HR-06.2H	Tech		0
	HR-06.3H	Tech		0
	HR-06.5H	Tech & Org	NDAQ1	1
Asset Management	AM-01.4H	Tech	AssetMonitoringQ1	1
	AM-03.4H	Tech		0
	AM-04.1H	Tech & Org		0
Physical Security	PS-02.8H	Tech & Org	AccessControlQ1	1
Operational Security	OPS-02.2H	Tech	ProvisioningPolicyCheckQ1, ProvisioningPolicyCheckQ2	2
	OPS-05.3H	Tech	MalwareProtectionEnabled, NumberOfThreatsFound, MalwareProtectionOutput, MalwareProtectionCheckQ3, AntimalwareScanFrequencyQ1	5
	OPS-07.2H	Tech	BackupEnabled, BackupRetentionSet, BackupMonitoringPolicyCheckQ1	3
	OPS-09.2H	Tech	BackupMonitoringPolicyCheckQ2, BackupMonitoringPolicyCheckQ3, BackupMonitoringPolicyCheckQ4, BackupMonitoringPolicyCheckQ5, SystemBackUpStorage03	5
	OPS-12.1H	Tech	EventMonitoringPolicyCheckQ1, EventMonitoringPolicyCheckQ2, EventMonitoringPolicyCheckQ3	3
	OPS-12.2H	Tech		0
	OPS-13.1H	Tech	AnomalyDetectionEnabled, ActivityLoggingEnabled, ApplicationLoggingEnabled,	8

EUCS Category	EUCS Req. ID	Type	Metric ID	# Metrics
			BootLoggingEnabled, OSLoggingEnabled, BootLoggingRetention, OSLoggingRetention BootLoggingImmutability	
	OPS-18.6H	Tech	AutomaticUpdatesEnabled, AutomaticUpdatesInterval, PatchManagementPolicyCheckQ1, PatchManagementPolicyCheckQ2, UpdatePolicyCheckQ1, UpdatePolicyCheckQ2	6
	OPS-21.1H	Tech	TLSVersion, WebApplicationFirewallEnabled, L3FirewallEnabled, JavaVersion, PHPVersion, PythonVersion, AtRestEncryptionEnabled, BackupEncryptionEnabled TlsCipherSuites, TlsDHGroups, TlsSignatureAlgorithms SystemHardeningPolicyQ1 SystemHardeningPolicyQ2 SystemHardeningPolicyQ3	14
Identity, Authentication and Access Control Management	IAM-03.1H	Tech	DeactivateInactiveUsers	1
	IAM-03.2H	Tech & Org	SignedCommits PasswordLoginAttemptsQ1	2
	IAM-03.5H	Tech & Org	PasswordLoginBlockDurationQ1	1
	IAM-03.6H	Tech	UnsuccesfulLoginAttemptLogged	1
Change and Conf. Management	CCM-04.1H	Tech & Org	CodeSignoff,	1
	CCM-05.1H	Tech & Org		0
Procurement Management	PM-04.7H	Tech	ProcurementManagementQ1	1
	PM-04.8H	Tech		0
Incident Management	IM-02.5H	Tech		0
Compliance	CO-03.5H	Tech & Org	ComplianceQ2	1
	CO-03.6H	Tech	SecureCryptographicPrimitives ComplianceQ1	2
Investigation Requests from Gov. Agencies	INQ-03.4H	Tech		0
Product Safety and Security	PSS-04.2H	Tech		0

4.3. List of Techniques

Gathering evidence of the EUCS certification scheme requirements [2], that cover various categories (such as human resources, physical security, or procurement management), requires a diverse set of tools and techniques.

Some requirements can be addressed by checking the configuration in the cloud provider, e.g., the use of a secure protocol for transport encryption. For others, however, there are several ways in which a CSP can fulfil the requirement. For example, the HR-03.4H requirement which says that *"All employees shall acknowledge in a documented form the information security policies and procedures presented to them […]"* can be implemented by using signed text documents, by using a SaaS solution, etc.

The *Generic Evidence Collector (GEC)* - introduced first in D3.2 [4] - is provided by MEDINA as an extra evidence gathering tool that implements a generic collector, i.e., a template which can easily be adapted to any CSP-specific system. Along with this tool, descriptions of some techniques are provided in text and as pseudo-code. These techniques act as a detailed guide for a CSP to successfully implement the evidence collection.

The *Generic Evidence Collector* is based on the *Cloud Evidence Collector*. It is compliant with the MEDINA data model and APIs, so it can be deployed as a Docker container, can establish a connection to the *Security Assessment,* and implements the MEDINA data model for evidence. A CSP that wants to integrate the *GEC* only needs to complete the API calls to the CSP-specific system and translate the responses to the MEDINA evidence model.

In addition to the techniques described in D3.2, we provide here a list of possible metrics that can be used to assess the evidence generated with the implemented techniques to cover the 34 high level EUCS requirements identified in Table 9.

Table 15. Metrics associated to the GEC Techniques to cover the 34 high level EUCS requirements (source: MEDINA's own contribution).

EUCS Req. ID	Metric ID	Scale	Operator	Target Value	Value Type	Resource Type
OIS-02.4H	MixedDuties	[0…1]	<=	0.1	Float	Identity
ISP-03.5H	NumberOfExceptions	[0, …]	<=	0	Integer	Exception
HR-03.4H	NumberOfMissing-PolicyAcknowledgements	[0, …]	<=	0	Integer	Identity
HR-04.3H	NumberOfMissing-Trainings	[0, …]	<=	0	Integer	Identity
HR-05.2H	Revocation-GracePeriod	[0, …]	<=	5	Integer	Revocation-Period
AM-01.4H	Inventory-Uptime	[0…1]	>=	0.99	Float	VirtualMachine
AM-04.1H	NumberOfMissing-Commitments	[0, …]	<=	0	Integer	Identity
PS-02.8H	MaximumSensitive-AccessRequests	[0, …]	<=	0	Integer	Identity
IM-02.5H	IncidentProcessTime	[0, …]	<=	24	Integer	Process

4.4. Security metrics covered by tool

This section deals with the coverage of the 34 high level EUCS requirements by the MEDINA Evidence Management Tools, namely Clouditor, Codyze, VAT, Wazuh, AMOE and GEC. Table 16 summarizes this coverage. The "EUCS Req. ID" cell in green represents that the requirement is covered by the MEDINA Evidence Management Tools, i.e., one or more metrics have been implemented to measure the requirement. The tool that covers the requirement is also signalled with a cell x in green background, and the metrics used to measure the requirement are shown.

For the rest of requirements ("EUCS Req.ID" cell in white), there is a plan or idea to implement the requirement, but it has not yet been realised at the time of writing.

Table 16. Table of metrics covered by each of the MEDINA evidence management tools

EUCS Req.ID	Metric ID	Cld.	Cdz.	VAT	Wzh	AMOE	GEC
OIS-02.4H	MixedDuties	X					X
ISP-03.5H	NumberOfExceptions						X
HR-03.4H	InformationSecurityPolicyAcknowledgementQ1					X	
	NumberOfMissingPolicyAcknowledgements						X
HR-04.3H	NumberOfMissingTrainings						X
HR-05.2H	AccessRightManagementQ1					X	
	RevocationGracePeriod						X
HR-06.2H							
HR-06.3H							
HR-06.5H	NDAQ1					X	
AM-01.4H	AssetMonitoringQ1					X	
	InventoryUptime						X
AM-03.4H							
AM-04.1H	NumberOfMissingCommitments						X
PS-02.8H	AccessControlQ1					X	
	NumberOfMissingCommitments						X
OPS-02.2H	ProvisioningPolicyCheckQ1, ProvisioningPolicyCheckQ2					X	
OPS-05.3H	MalwareProtectionEnabled, NumberofThreatsFound, MalwareProtectionOutput				X		
	MalwareProtectionCheckQ3, AntimalwareScanFrequencyQ1					X	
OPS-07.2H	BackupEnabled, BackupRetentionSet	X					
	BackupMonitoringPolicyCheckQ1					X	
OPS-09.2H	BackupMonitoringPolicyCheckQ2, BackupMonitoringPolicyCheckQ3, BackupMonitoringPolicyCheckQ4, BackupMonitoringPolicyCheckQ5, SystemBackUpStorage03					X	
OPS-12.1H	EventMonitoringPolicyCheckQ1, EventMonitoringPolicyCheckQ2, EventMonitoringPolicyCheckQ3					X	
OPS-12.2H							
OPS-13.1H	AnomalyDetectionEnabled, ActivityLoggingEnabled, ApplicationLoggingEnabled, BootLoggingEnabled, OSLoggingEnabled, BootLoggingRetention, OSLoggingRetention, BootLoggingImmutability	X					
OPS-18.6H	AutomaticUpdatesEnabled, AutomaticUpdatesInterval	X					
	PatchManagementPolicyCheckQ1, PatchManagementPolicyCheckQ2, UpdatePolicyCheckQ1, UpdatePolicyCheckQ2					X	
OPS-21.1H	TLSVersion, WebApplicationFirewallEnabled, L3FirewallEnabled,	X					

EUCS Req.ID	Metric ID	Cld.	Cdz.	VAT	Wzh	AMOE	GEC
	JavaVersion, PHPVersion, PythonVersion, AtRestEncryptionEnabled, BackupEncryptionEnabled						
	TLSVersion, TlsCipherSuites, TlsDHGroups, TlsSignatureAlgorithms		X				
	SystemHardeningPolicyQ1, SystemHardeningPolicyQ2, SystemHardeningPolicyQ3					X	
IAM-03.1H	DeactivateInactiveUsers	X					
IAM-03.2H	SignedCommits PasswordLoginAttemptsQ1		X			X	
IAM-03.5H	PasswordLoginBlockDurationQ1					X	
IAM-03.6H	UnsuccessfulLoginAttemptLogged		X				
CCM-04.1H	CodeSignoff		X				
CCM-05.1H							
PM-04.7H	ProcurementManagementQ1					X	
PM-04.8H							
IM-02.5H	IncidentProcessTime						X
CO-03.5H	ComplianceQ2					X	
CO-03.6H	SecureCryptographicPrimitives ComplianceQ1	X				X	
INQ-03.4H							
PSS-04.2H							

Taking into account all the information shown in Table 16, we can calculate the current level of achievement of the MEDINA KPIs related to metrics, namely KPI 1.1 and KPI 1.2, which were reformulated in July 2022 as follows:

- **KPI 1.1**: Provide realizable metrics for at least 70% of the technical measures referenced in EUCS-High assurance requiring ‘continuous (automated)’ monitoring.
- **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.

As detailed in the previous tables, the MEDINA evidence management tools cover 26 of “the 34” EUCS requirements identified in Section 3.1. And for the remaining 8 requirements, there is some plan or idea to cover them in the next release of the tools (due at M30). As a result, at the time of writing:

KPI 1.1*: As the 34 identified requirements are considered of a “Technical” nature, we can state that MEDINA realizable metrics are provided for 76% of the technical requirements (26/34), which is above the 70% requested.*

***KPI 1.2**: As 9 from the 34 requirements are considered of a "Organizational" nature, we can state that MEDINA has proposed semi-automated evaluation of metrics for 78% of the organizational requirements (7/9), which is above the 50% requested.*

5. Catalogue of Controls and Metrics

The software implementation of the *Catalogue of Controls and Metrics* (aka Catalogue) is based on the information detailed in the previous sections of this deliverable. The Catalogue is one of the main entry points of the MEDINA framework. The target users are mainly CSP compliance managers and auditors.

5.1. Functional description

The main goal of the Catalogue is to have an automated tool where a CSP compliance manager or an auditor can select a security scheme and obtain all the information and guidance related to that security scheme, namely the controls, security requirements, assurance levels, etc. In other words, everything that can be considered as "static" information that appears in the standard. This information has been extended with all the research and implementation work performed in MEDINA, such as Reference TOMs, metrics, similar controls in other schemes, and the self-assessment questionnaires.

Hence, the Catalogue must provide the necessary technological means for the endorsement of any security scheme and their related attributes: security requirements, categories, controls, TOMs (requirements), metrics, evidence, and assurance levels. Furthermore, it provides guidance for the implementation as well as the (self-)assessment of the requirements.

Another functionality that the Catalogue must provide is the filtering of the information based on some values for the attributes like the selection of requirements of a certain assurance level, the selection of requirements from a certain framework or the selection of metrics related to a TOM.

Homogenization of different certification schemes, in the sense of showing the requirements that are equivalent in different security frameworks with reference to the EUCS, is also provided by the Catalogue.

The Catalogue also contains a first implementation of a Questionnaire that allows a CSP to perform a self-assessment of the fulfilment degree of the EUCS standard. The questionnaire has been developed in the context of WP3, initially using excel sheets. It covers all the requirements of EUCS 2022 [2], for all levels of certifications (Basic, Substantial and High), defining one or more questions for each requirement. All this work has been reported in the deliverable D3.2 [4]. The inclusion of the Questionnaire in the Catalogue provides a more flexible tool, allowing the user to introduce the answers in a more automated manner, saving the results electronically, and providing an immediate and visual feedback. The user can select the assurance level for the assessment, and then provide the answer to several questions to check the fulfilment of every requirement involved. It also allows the user to enter comments related to a question, and textual references to locate the evidence supporting the answer given. Finally, it provides a summary dashboard with quantitative values to reflect the degree of fulfilment. Auditors can also have access to the questionnaire and enter non-conformities for each requirement that is not fulfilled.

The Catalogue also provides Reference TOMs. As stated in the Section 3.2, a Reference TOMs is an explanation of how a specific security requirement can be implemented, in a vendor and technology-agnostic way. It includes examples coming from larger CSPs that can be used as inspiration.

Table 17 shows the functional requirements satisfied by this version of the Catalogue, which were documented in D5.2 [3], and updates the status of their implementation in the current prototype in M27.

Table 17. Requirements of the Catalogue (source: D5.2 [3])

Req. ID	Description	Status
RCME.01	The repository should include realizable metrics for at least for the 70% of the TOMs referenced in EUCS-High assurance requiring "continuous (automated)" monitoring	Satisfied
RCME.02	The repository should include realizable metrics for at least for the 70% of the TOMs referenced in EUCS-High assurance requiring "continuous (automated)" monitoring	Satisfied
RCME.03	The repository should include metrics for TOMs for basic (Y3), substantial (Y2) and high assurance levels (Y1)	Satisfied
RCME.04	The definition of the security controls in the repository should be technology agnostic, that is, they must be valid for several different implementations and cannot be technology specific.	Satisfied
RCME.05	The repository should be accessible by the continuous evaluation tools.	Satisfied
RCME.06	The repository as part of the MEDINA framework should support the homogenization of certification schemes, by aligning to the EUCS. Thus, the repository must include information about the coverage of the different similar controls in the different (national) schemes.	Satisfied
RCME.07	When the certification scheme changes in some way (partial changes, requirements, new versions), the risk assurance component has to be notified, or be able to know that something has changed.	Partially
RCME.08	The Catalogue has a GUI to search and show the different content it stores. This GUI is going to be part of the MEDINA Integrated-UI. Enhancements and adaptation to changes in data model are foreseen until the final version of the catalogue.	Satisfied
RCME.09	The Catalogue shall contain a questionnaire that helps a Cloud Service Provider to make a self-assessment of the fulfilment degree of the EUCS standard. This questionnaire will have the following features: 1) Allow the user to select the assurance level for the assessment 2) Include one or more questions for every requirement, of each control in each EUCS category 3) Provide an easy-to-use scale of support (fully/partially/not supported) 4) Allow to enter comments related to a question 5) Allow the user to include textual references for locating the evidence that support the response given to a specific question 6) Provide a dashboard that summarizes the result of the assessment, and provides quantitative values to reflect the degree of fulfilment	Partially
RCME.10	The questionnaire can be used by an auditor to help him in the audit process. For that purpose, the tool can provide some extra functionalities like: 1) Allow to enter non-conformities regarding a question 2) Provide a dashboard that summarizes the result of the audit, including the related comments/non-conformities for each question, as well as quantitative values to reflect the degree of fulfilment	Partially

5.1.1. Fitting into overall MEDINA Architecture

The Catalogue is one of the components of the MEDINA architecture. Figure 1 shows how It interacts with other tools in the MEDINA ecosystem.

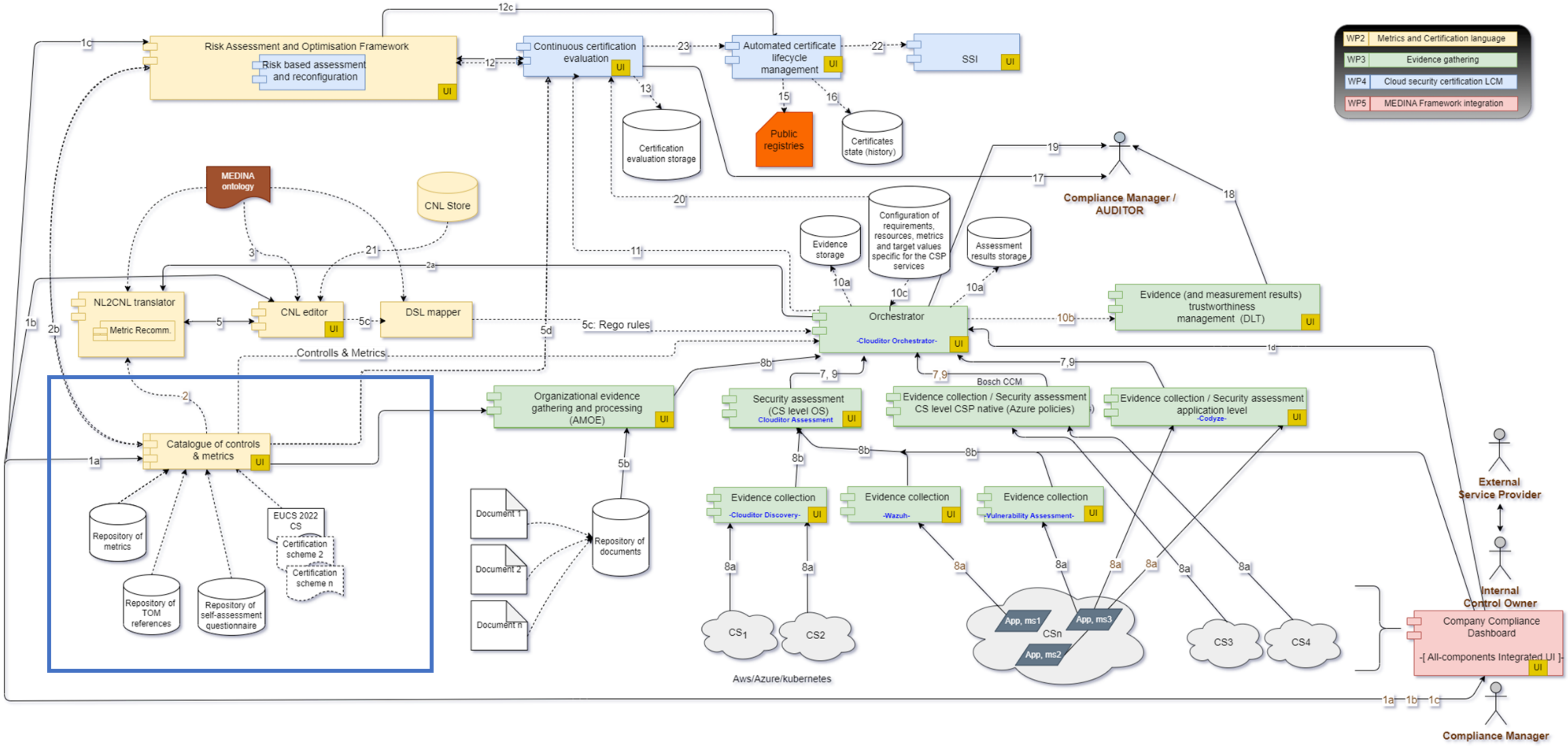

WP2 Metrics and Certification language
WP3 Evidence gathering
WP4 Cloud security certification LCM
WP5 MEDINA Framework integration
Risk Assessment and Optimisation Framework
Risk based assessment and reconfiguration
UI
Continuous certification evaluation
Automated certificate lifecycle management
SSI
12c
1c
12
23
22
13
15
16
Certification evaluation storage
Public registries
Certificates state (history)
19
17
18
Compliance Manager / AUDITOR
20
MEDINA ontology
CNL Store
3
21
11
Evidence storage
Configuration of requirements, resources, metrics and target values specific for the CSP services
Assessment results storage
2a
10a
10c
10a
NL2CNL translator
Metric Recomm.
CNL editor
DSL mapper
5
5c
5d
5c: Rego rules
Orchestrator
-Clouditor Orchestrator-
10b
Evidence (and measurement results) trustworthiness management (DLT)
1d
1b
2b
Controlls & Metrics
8b
7, 9
7,9
7,9
Bosch CCM
2
Organizational evidence gathering and processing (AMOE)
Security assessment (CS level OS)
Clouditor Assessment
Evidence collection / Security assessment CS level CSP native (Azure policies)
Evidence collection / Security assessment application level
-Codyze-
Catalogue of controls & metrics
1a
5b
8b
8b
8b
External Service Provider
Repository of metrics
EUCS 2022 CS
Certification scheme 2
Certification scheme n
Repository of TOM references
Repository of self-assessment questionnaire
Document 1
Document 2
Document n
Repository of documents
Evidence collection
-Clouditor Discovery-
Evidence collection
-Wazuh-
Evidence collection
-Vulnerability Assessment-
8a
8a
8a
8a
8a
8a
8a
8a
Internal Control Owner
CS_1
CS2
App, ms1
App, ms3
CSn
App, ms2
CS3
CS4
Company Compliance Dashboard
-[All-components Integrated UI]-
Aws/Azure/kubernetes
1a
1b
1c
Compliance Manager

Figure 1. Fitting of the Catalogue with other components in MEDINA architecture

The main interactions of the Catalogue with the users and other MEDINA components are as follows:

- **CSP Compliance manager**: the user selects the schema, assurance level, categories, etc. and can endorse a new security scheme through the Catalogue frontend.
- **Auditor:** the user discovers information contained in the Catalogue based on a set of filters through the Catalogue frontend.
- **NL2CNL translator:** requests to the Catalogue the set of requirements selected by a certain user.
- **Orchestrator**: retrieves the necessary information about controls and metrics from the Catalogue.
- **Risk Assessment and Optimization Framework (RAOF):** retrieves the required generic information about the scheme selected by the user (requirements, metrics, metrics-requirements mapping, etc.).
- **Continuous certification evaluation (CCE)**: retrieves the certification specification (requirements, controls and their relations with selected metrics).

5.2. Technical description

This subsection is dedicated to describing the technical specification of the *Catalogue of Controls and Metrics* component. First, we present the main architecture of the prototype, including all its sub-components. Next, the data model used by the Catalogue is presented, describing the different entities used and their attributes. The subsection finishes with the technical specifications of the developed system.

5.2.1. Prototype architecture

The architecture of the Catalogue is based on a micro-services style which splits front-end and back end, so that it is easier to scale for a growing number of users and also to survive infrastructure issues. This also serves as preparation for the exploitation and sustainability phases. Figure 2 shows the architecture diagram of the Catalogue.

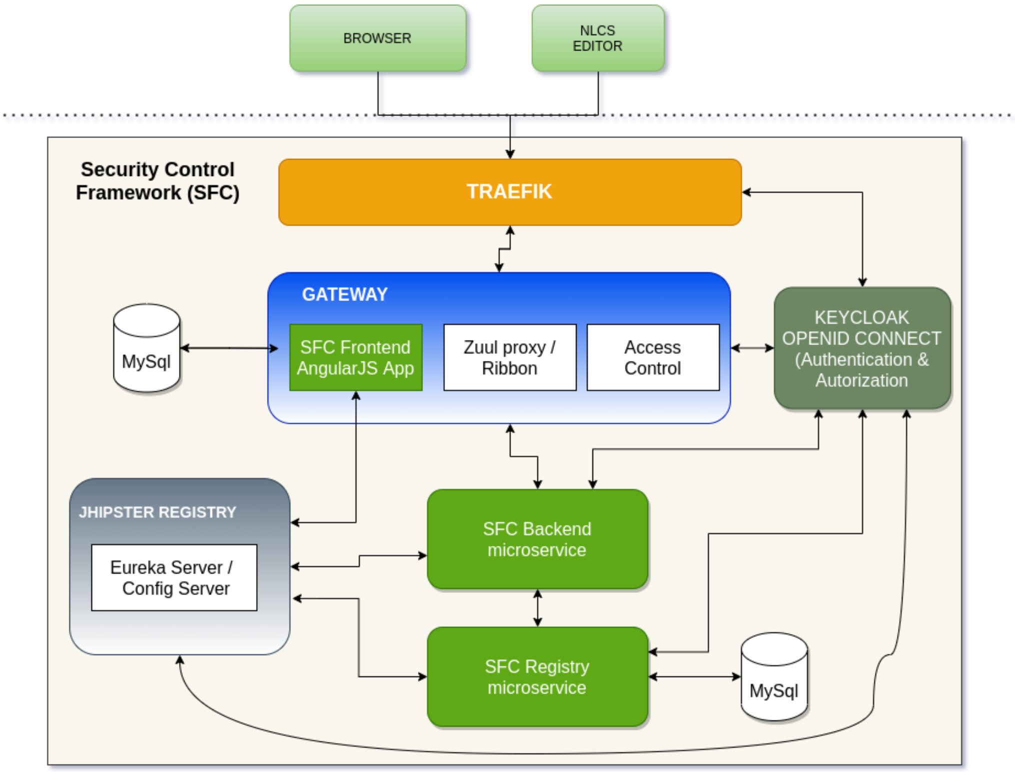

BROWSER
NLCS EDITOR
Security Control Framework (SFC)
TRAEFIK
GATEWAY
SFC Frontend AngularJS App
Zuul proxy / Ribbon
Access Control
KEYCLOAK OPENID CONNECT (Authentication & Autorization
MySql
JHIPSTER REGISTRY
Eureka Server / Config Server
SFC Backend microservice
SFC Registry microservice
MySql

Figure 2. Architecture diagram and components of the Catalogue (SFC)

5.2.1.1. Data Model

Figure 3 shows the different entities (and their attributes) that make up the data model used by the Catalogue component. In the following, we describe the elements that appear in the entity-relation diagram. These descriptions are taken from the MEDINA glossary (see *Appendix 4: MEDINA Glossary*):

Security Control Framework: set of security control categories, namely a scheme. In this case, this entity indicates the schemes / standards covered in MEDINA such as EUCS or BSI C5.

Security Control Category: set of security controls, obtained by grouping together related security controls.

Security Control: a safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. A security control is composed of a control ID, a control name and a control objective.

Similar Control: a control that has been mapped by MEDINA as “equivalent” to an EUCS control in other schemes or standards. The objective is to facilitate the transition from other schemes towards EUCS and vice versa, as well as the reuse of evidence, whenever possible. In the Catalogue, we have defined a list of equivalences among EUCS controls and controls in these other schemas: ISO/IEC 27000, BSI C5:2020, SecNumCloud and Cisco CCF.

TOM (Technical and Organizational Measure): a security requirement that modifies the likelihood or the severity of a risk. It includes the policy, procedures, guidelines, and the organizational practices or structures, and can be of an administrative, technical, managerial or legal nature. In MEDINA TOM is the equivalent of a security requirement and is represented as a requirement ID, requirement objective and the associated assurance level.

TOM reference: a documented good practice that provides the basis for a compliant implementation of a Technical and Organizational Measure. The TOM Reference should be technology-/CSP-agnostic.

Security Metric: an abstract definition that describes the conditions and process for assessing a specific Security Requirement as part of a Security Assessment Rule. The metric does not define the Target Value for the Security Assessment Rule.

Questionnaire: checklist elaborated in MEDINA to develop an assessment model for requirements in the basic/substantial/high level of assurance that can be understood by less experienced compliance managers and CSPs in general. CABs and auditors could also adopt it as guidance.

Assurance level: level of assurance for which the user wants to assess the cloud service. Each question has also an assurance level assigned. The possible values are: basic, substantial and high.

Question: the questionnaire is composed by a series of questions, based on the experience of the auditors, consultants and CSPs that participated in MEDINA, as well as from literature. Multiple questions have been created for each of the requirements in the EUCS framework, hence, more than 900 questions are included in the questionnaire. The questions identify some examples of evidence that the CSP shall submit to the CAB for the evaluation assessment.

Question answer: the answer to each question. It is a closed group that can take one of these values: Fully supported, Partially supported, Not supported, Not applicable.

Questionnaire non-conformities: the non-conformities are deviations from the requirement. In the MEDINA questionnaire, they are textual sentences that can be introduced by an auditor in each requirement.

Questionnaire purpose: we distinguish two different possible purposes for a questionnaire: Self-evaluation or External audit.

Jhi user: the user that creates and answers the questionnaire. Users in MEDINA are centralized by the Keycloak identity manager, where they are and created and managed. The user is linked to a cloud service provider, and has a list of cloud services list associated to him.

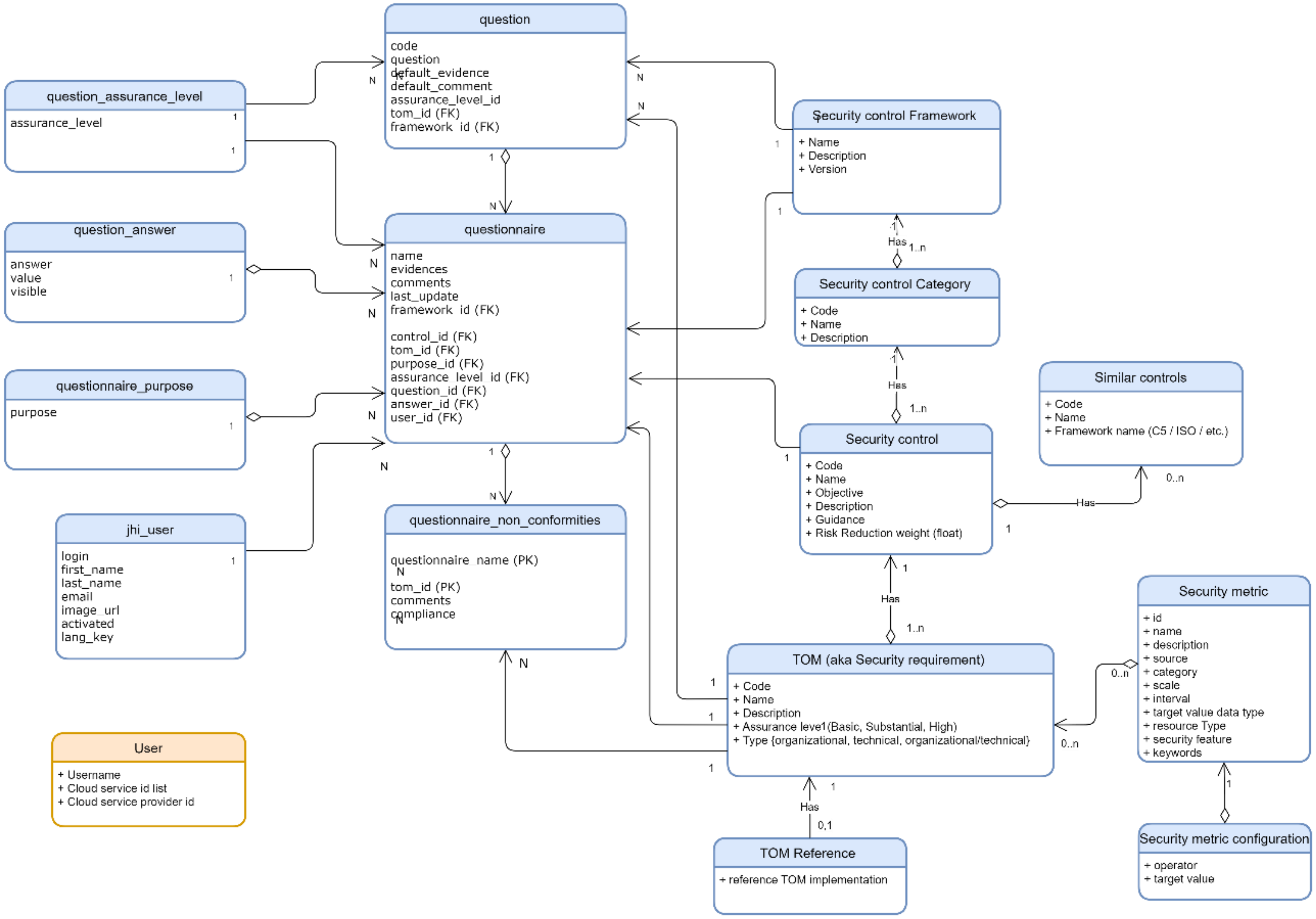


Figure 3. Data Model of the Catalogue

5.2.2. Description of components

The Catalogue is composed by three main components (see Figure 2), the main purpose of which is briefly described as follows.

- **Frontend**: is the graphical user interface of the Catalogue. This frontend allows the user to indicate the requirements to filter and select a set of information related to the existing frameworks, i.e., requirements of a certain assurance level, requirements from a certain framework, metrics related to a TOM, Reference TOMs, etc.
- **Backend :** is the core sub-component of the Catalogue. It performs the actual discovery of the requirements, metrics, etc. from the Security Control Frameworks registry, considering the set of filters established by the user through the UI/ API.
- **Registry**: the Security Control Frameworks registry stores the available list of security frameworks and the related info for a specific CSP. This component also includes the corresponding databases.

Other components of the infrastructure are listed below:

- **Access control**: Keycloak[20] identity and access management is used.
- **Data persistence** in MySQL database.
- **JHipster Registry**: Service discovery that uses Netflix Eureka.

5.2.3. Technical specifications

The Catalogue component has been developed using the JHipster Framework[21], that provides all the needed mechanisms for the implementation of a modern web application based on microservice architecture.[22] Jhipster uses Spring boot for application configuration.

On the client side, the Frontend gateway uses Yeoman[23], Webpack[24], Angular[25] and Bootstrap[26] technologies.

On the server side, the Backend and Registry components use Maven, Spring, Spring MVC REST, Spring Data JPA and Netflix OSS.[27]

5.3. Delivery and usage

5.3.1. Package information

This section describes the main packages of the Catalogue. They are the `cocBackend` - which is the implementation of the Backend component-, and the `cocGateway` – which is the implementation of the Frontend (also called gateway) component-. We also include the `cocMySql` package, due the importance of the scripts that populate the information contained in the Catalogue.

[20] https://www.keycloak.org/

[21] https://www.jhipster.tech

[22] https://www.jhipster.tech/tech-stack/

[23] https://yeoman.io/

[24] https://webpack.js.org/

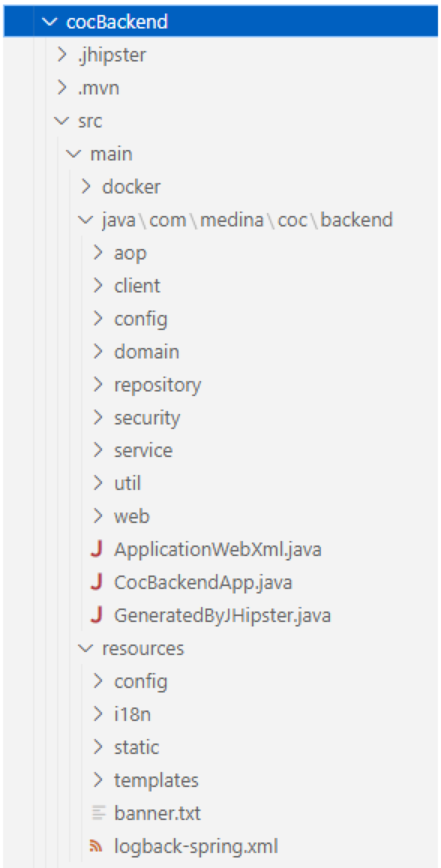
[25] https://angular.io/

[26] https://getbootstrap.com/

[27] https://www.jhipster.tech/microservices-architecture/

5.3.1.1. cocBackend

Figure 4 shows the packages that compose the main structure of the Backend subcomponent of the Catalogue.

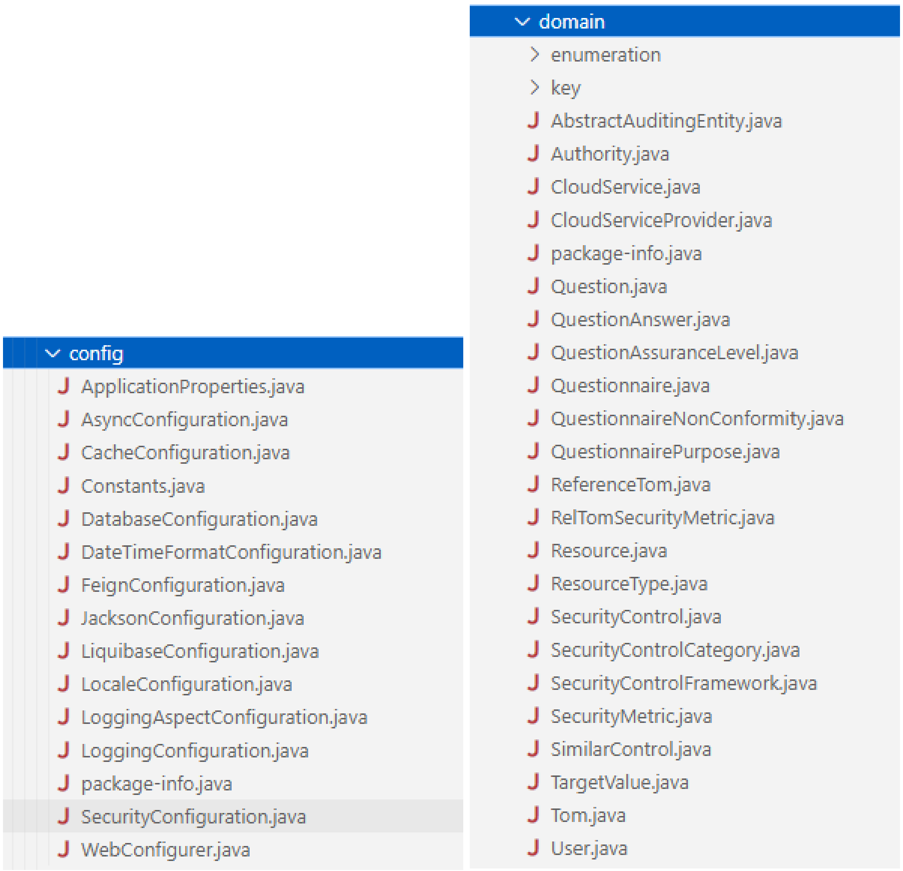


```
∨ cocBackend
  > .jhipster
  > .mvn
  ∨ src
    ∨ main
      > docker
      ∨ java\com\medina\coc\backend
        > aop
        > client
        > config
        > domain
        > repository
        > security
        > service
        > util
        > web
        J ApplicationWebXml.java
        J CocBackendApp.java
        J GeneratedByJHipster.java
      ∨ resources
        > config
        > i18n
        > static
        > templates
        banner.txt
        logback-spring.xml
```

Figure 4. Structure of the Backend subcomponent

Each of these packages has its main purpose and context within the prototype as a whole. In addition, these packages are also composed by several JAVA classes. The main purpose and composition of each package is as follows:

- `com.medina.coc.backend.aop.logging`: This package consists of the `LoggingAspect.java` class that defines the aspect for logging execution of Spring service and repository components.
- `com.medina.coc.backend.aop.client`: This package consists of the `UserFeignClientInterceptor.java` class that implements `RequestInterceptor.java`. This class checks and adds a JWT token to the request header.
- `com.medina.coc.backend.aop.config`: This package contains all the classes related to configuration purposes.
- `com.medina.coc.backend.aop.domain`: This package contains data model classes.



config
- ApplicationProperties.java
- AsyncConfiguration.java
- CacheConfiguration.java
- Constants.java
- DatabaseConfiguration.java
- DateTimeFormatConfiguration.java
- FeignConfiguration.java
- JacksonConfiguration.java
- LiquibaseConfiguration.java
- LocaleConfiguration.java
- LoggingAspectConfiguration.java
- LoggingConfiguration.java
- package-info.java
- SecurityConfiguration.java
- WebConfigurer.java

domain
- enumeration
- key
- AbstractAuditingEntity.java
- Authority.java
- CloudService.java
- CloudServiceProvider.java
- package-info.java
- Question.java
- QuestionAnswer.java
- QuestionAssuranceLevel.java
- Questionnaire.java
- QuestionnaireNonConformity.java
- QuestionnairePurpose.java
- ReferenceTom.java
- RelTomSecurityMetric.java
- Resource.java
- ResourceType.java
- SecurityControl.java
- SecurityControlCategory.java
- SecurityControlFramework.java
- SecurityMetric.java
- SimilarControl.java
- TargetValue.java
- Tom.java
- User.java

Figure 5. Structure of the 'config' and 'domain' packages

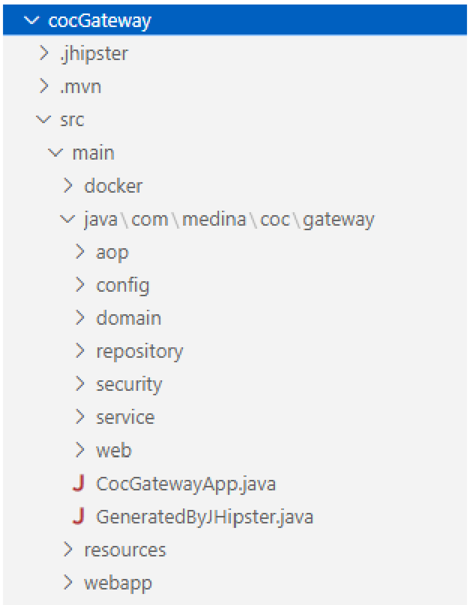
- `com.medina.coc.backend.repository`: This package contains Spring Data SQL repository classes.
- `com.medina.coc.backend.security`: This package contains Spring Security related classes for security management.
- `com.medina.coc.backend.service`: This package contains backend services for CRUD operations and other requirements needed.
- `com.medina.coc.backend.web`: This package contains classes to expose backend rest end points.

5.3.1.2. cocGateway

Figure 6 shows the main structure of the Frontend component, which is composed by two main parts: the JAVA classes related to the Spring boot[28] project to develop the microservices; and the Angular typescript files, used to develop the web application.

[28] https://spring.io/projects/spring-boot

5.3.1.2.1. Spring boot package



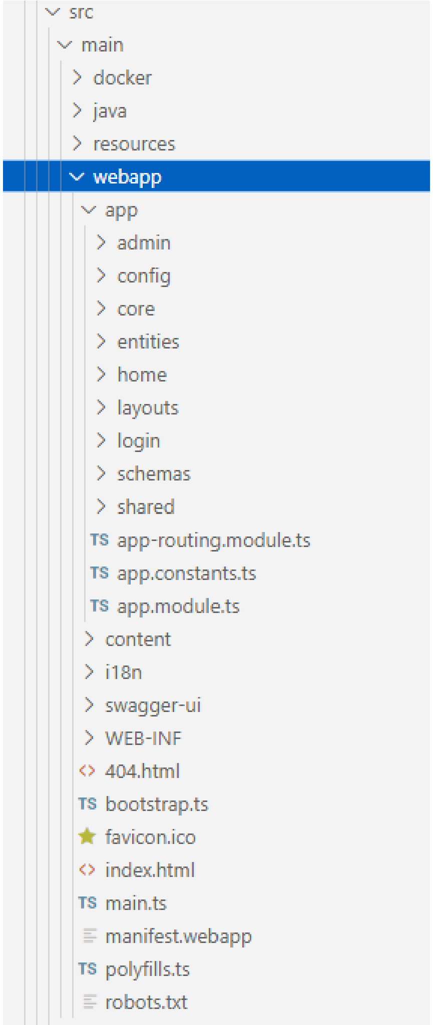
```
⌄ cocGateway
  › .jhipster
  › .mvn
  ⌄ src
    ⌄ main
      › docker
      ⌄ java\com\medina\coc\gateway
        › aop
        › config
        › domain
        › repository
        › security
        › service
        › web
        J CocGatewayApp.java
        J GeneratedByJHipster.java
      › resources
      › webapp
```

Figure 6. Spring boot package

Each of these packages has its main purpose and context within the prototype as a whole. In addition, these packages are also composed by several JAVA classes. The main purpose and composition of each component is as follows:

- `com.medina.coc.frontend.aop.logging`: This package consists of the `LoggingAspect.java` class that defines the aspect for logging execution of Spring service and repository components.
- `com.medina.coc.frontend.config`: This package contains all classes related to configuration purposes.
- `com.medina.coc.frontend.domain`: This package contains user data model and Authority classes.
- `com.medina.coc.frontend.repository`: This package contains Spring Data SQL repository classes for user and security management.
- `com.medina.coc.frontend.security:` This package contains Spring Security related classes for security management.
- `com.medina.coc.frontend.service:` This package contains frontend services for CRUD operations and other requirements needed for user and security management.
- `com.medina.coc.frontend.web:` This package contains classes to expose frontend rest end points for user and security management.

5.3.1.2.2. AngularJS package



```
src
  main
    docker
    java
    resources
    webapp
      app
        admin
        config
        core
        entities
        home
        layouts
        login
        schemas
        shared
        app-routing.module.ts
        app.constants.ts
        app.module.ts
      content
      i18n
      swagger-ui
      WEB-INF
      404.html
      bootstrap.ts
      favicon.ico
      index.html
      main.ts
      manifest.webapp
      polyfills.ts
      robots.txt
```

Figure 7. AngularJS package

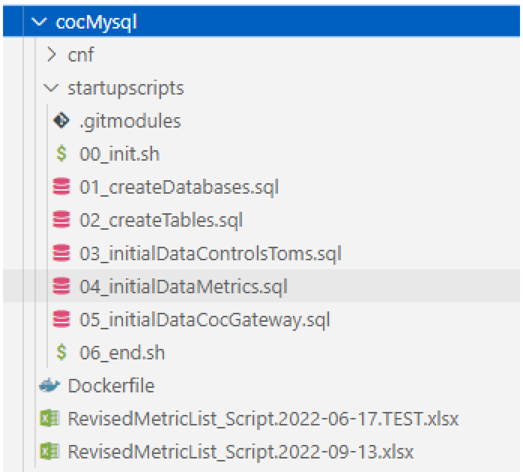
Each of these packages and typescript files has its main objective and context within the prototype as a whole. The main purpose and composition of each file/component is as follows:

- `app/app.constants.ts:` Global application constants.
- `app/app.module.ts:` Declaration of all the needed modules, providers and components loaded in the web application.
- `app/app-routing.module.ts:` Routing configuration.
- `app/admin:` Admin related modules. API documentation module, Gateway route module and user management module.
- `app/config:` Global configuration and constant typescript files.
- `app/core:` Global util files, core models and services.
- `app/entities/cocBackend:` All files related to the Backend data model. services, components and models.
- `app/home:` Home component.
- `app/layout:` Layout components; error, footer, navbar, main and profile components.
- `app/login:` User Login component.
- `app/shared:` Shared module with common components, directives and pipes.
- `content:` Static files of webapp. CSS and images.

- `i18n:` Internationalization files.

5.3.1.3. cocMysql

This package contains the configuration and starting script of the MySQL database. The .sql files are organized hierarchically to (1) create the database; (2) create the tables; (3) load the controls and requirements; (4) load the metrics table and the questionnaires; and (5) configure the gateway.



```
cocMysql
  cnf
  startupscripts
    .gitmodules
    00_init.sh
    01_createDatabases.sql
    02_createTables.sql
    03_initialDataControlsToms.sql
    04_initialDataMetrics.sql
    05_initialDataCocGateway.sql
    06_end.sh
  Dockerfile
  RevisedMetricList_Script.2022-06-17.TEST.xlsx
  RevisedMetricList_Script.2022-09-13.xlsx
```

Figure 8. cocMysql package

5.3.2. Installation instructions

This project is executed in a docker container. There are docker compose files for each environment (development and test). These are the steps to execute this project in a development environment:

1. Clone repository
   git clone https://git.code.tecnalia.com/medina/public/catalogue-of-controls

2. Run docker compose to start JHipster registry and MySQL instances
   docker-compose –env-file .env.dev -f docker-compose-local-dev.yaml up –build -dFrontends

3. Build and deploy the Catalogue backend
   ./mvnw -Pdev,api-docs -DskipTests

4. Build and deploy the Catalogue frontend
   ./mvnw -Pdev,webapp,api-docs -DskipTests

Once docker-compose is successfully deployed, and assuming the following values for SERVER_HOST (192.168.56.1.nip.io) and HTTPS_PORT (8080), we will be able to access the Catalogue services at:

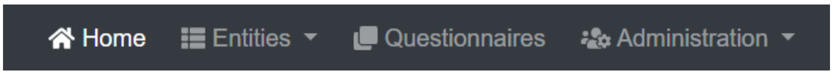
- https://192.168.56.1.nip.io Catalogue
- https://192.168.56.1.nip.io/services/iecbackend/v3/api-docs Catalogue API

Other services that are deployed to help in the development phase are a reverse proxy to manage the network (Traefik[29]), a container manager (Portainer[30]) and a local Certification Authority (CA) to deal with digital certificates:

- https://traefik.192.168.56.1.nip.io (Traefik dashboard)
- https://portainer.192.168.56.1.nip.io (Portainer)
- https://ca.192.168.56.1.nip.io (Tecnalia CA)

5.3.3. User Manual

The *Catalogue of controls and metrics* application includes a menu, that is always accessible in the top area, with all the available options:



The different menu options are the following:

- **Home**: Starting point of the Catalogue.
- **Entities**: Provide access to information about Security Frameworks, Categories, Controls, Similar Controls, Requirements (TOMs), Reference Requirements (Reference TOMs) and Security Metrics.
- **Questionnaires**: Provides access to the self-assessment and external audit questionnaires.
- **Administration**: Provides access to the gateway and REST API information.

5.3.3.1. Home

The *Home* menu option displays a screen with a welcome message and a very brief information about the user who has accessed the application.

5.3.3.2. Entities

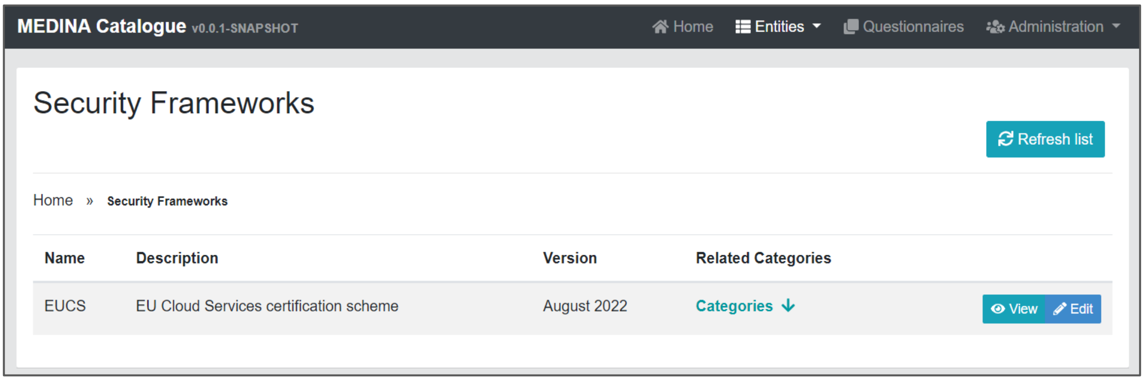
The *Entities* menu option displays a submenu with the following options that will be detailed in below:

- Security Frameworks
- Security Categories
- Security Controls
- Similar Controls
- Requirements
- Reference Requirements
- Security Metrics

5.3.3.2.1. Security Frameworks

The main *Security Frameworks* window (see Figure 9) shows the list of all the registered frameworks in the Catalogue. The current version only includes the EUCS Security Framework.

[29] https://traefik.io/
[30] https://www.portainer.io/



Security Frameworks

Home » Security Frameworks

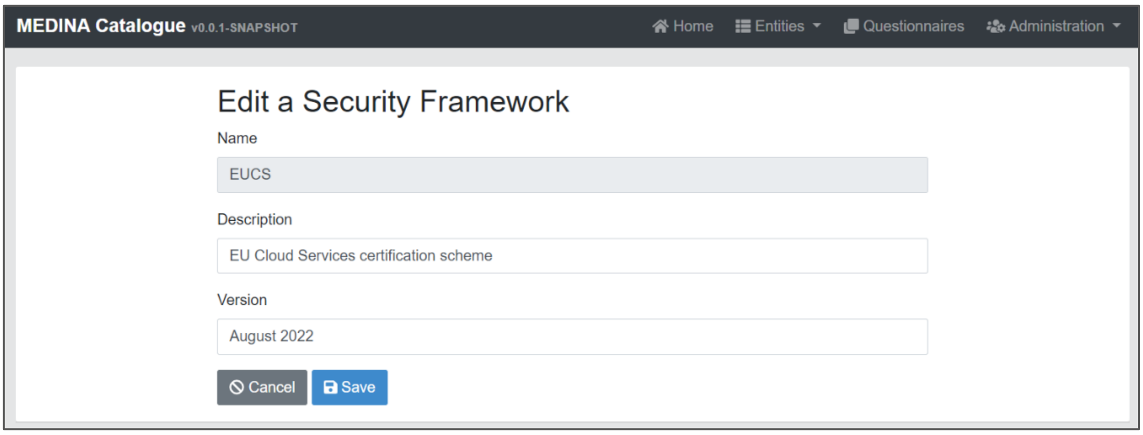
Name	Description	Version	Related Categories
EUCS	EU Cloud Services certification scheme	August 2022	Categories ↓

Figure 9. List of Security Frameworks

The following fields are listed for each Security Framework:

- Name
- Description
- Version

At the right of each Security Framework, two buttons allow to *Edit*/*View* the details of the entity, in this case the Security Framework. In the *Edit* window, only the description and the version fields can be updated[31].



Edit a Security Framework

Name: EUCS

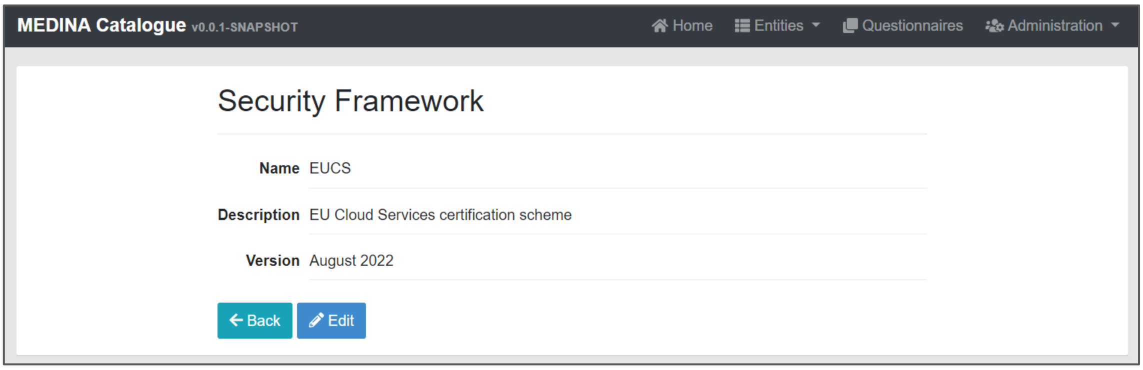
Description: EU Cloud Services certification scheme

Version: August 2022

While clicking on the *View* button, a very similar window, but in this case with view-only fields, is shown[32].

[31] The Edit options are further limited by the role-based access feature, so that some roles can use this option and others cannot.

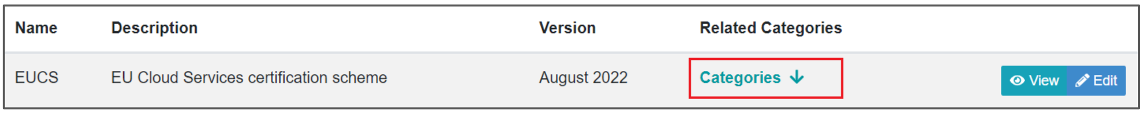
[32] As these *View/Edit* options are repeated in almost all entities, and as the structure of the two windows is quite similar, in the remainder of the manual we will only show one of the two windows.



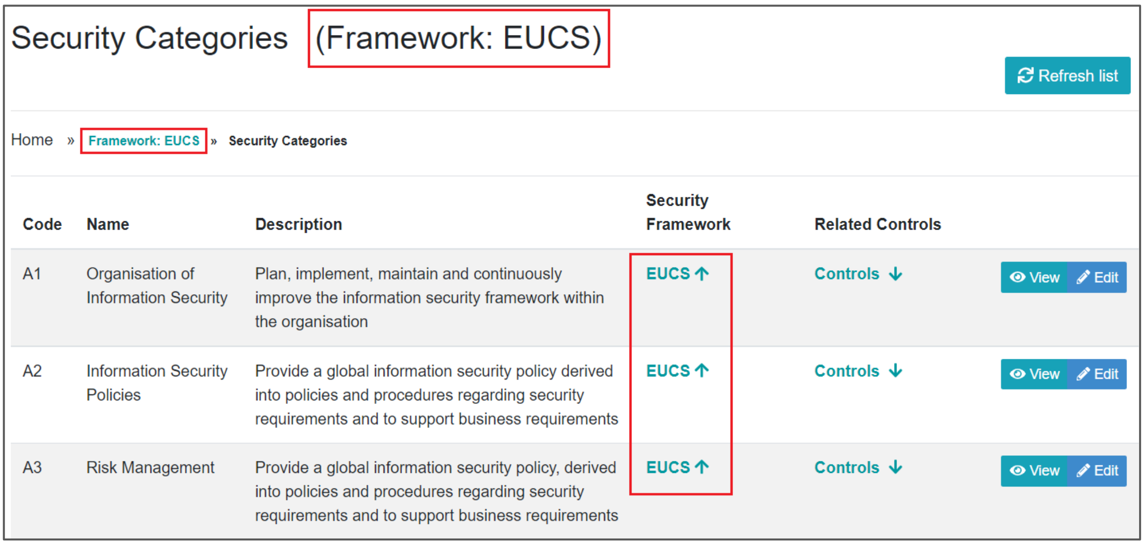
Security Framework

Name	EUCS
Description	EU Cloud Services certification scheme
Version	August 2022

Finally, each Security Framework offers the possibility to access its related Security Categories, by clicking on the following link:



Name	Description	Version	Related Categories	
EUCS	EU Cloud Services certification scheme	August 2022	Categories ↓	View Edit



Security Categories (Framework: EUCS)

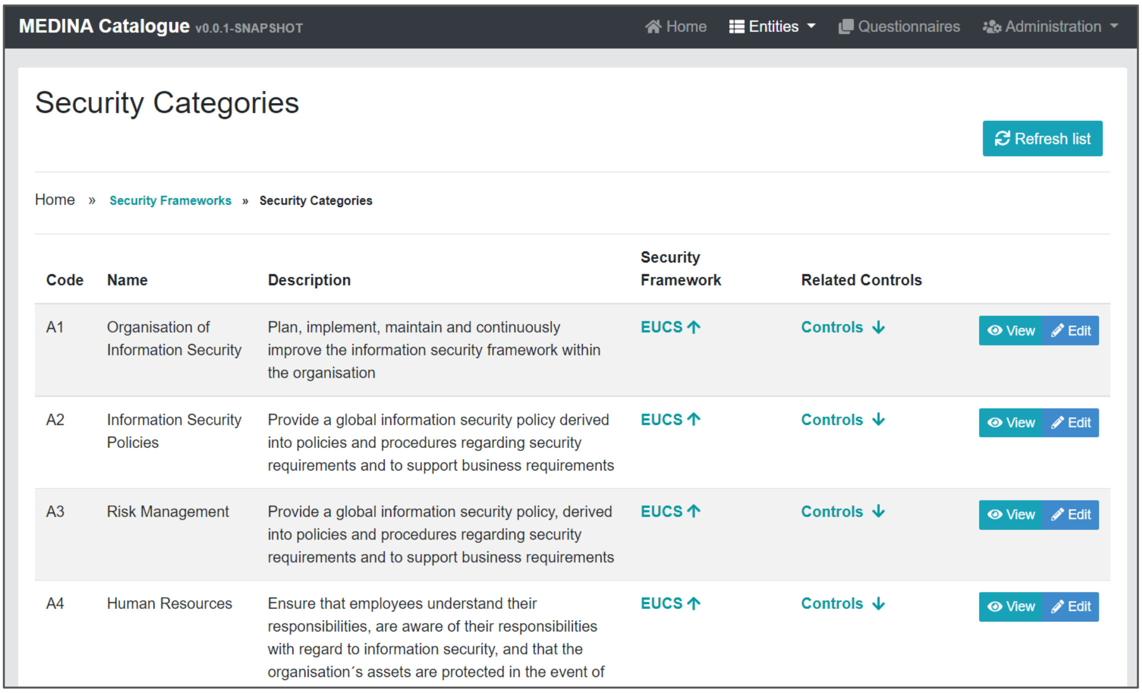
Home » Framework: EUCS » Security Categories

Code	Name	Description	Security Framework	Related Controls	
A1	Organisation of Information Security	Plan, implement, maintain and continuously improve the information security framework within the organisation	EUCS ↑	Controls ↓	View Edit
A2	Information Security Policies	Provide a global information security policy derived into policies and procedures regarding security requirements and to support business requirements	EUCS ↑	Controls ↓	View Edit
A3	Risk Management	Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements	EUCS ↑	Controls ↓	View Edit

Figure 10. Security Categories belonging to the EUCS Framework

5.3.3.2.2. Security Categories

The main *Security Categories* window (see Figure 11) lists all the Security Categories stored in the Catalogue.



Security Categories

Home » Security Frameworks » Security Categories

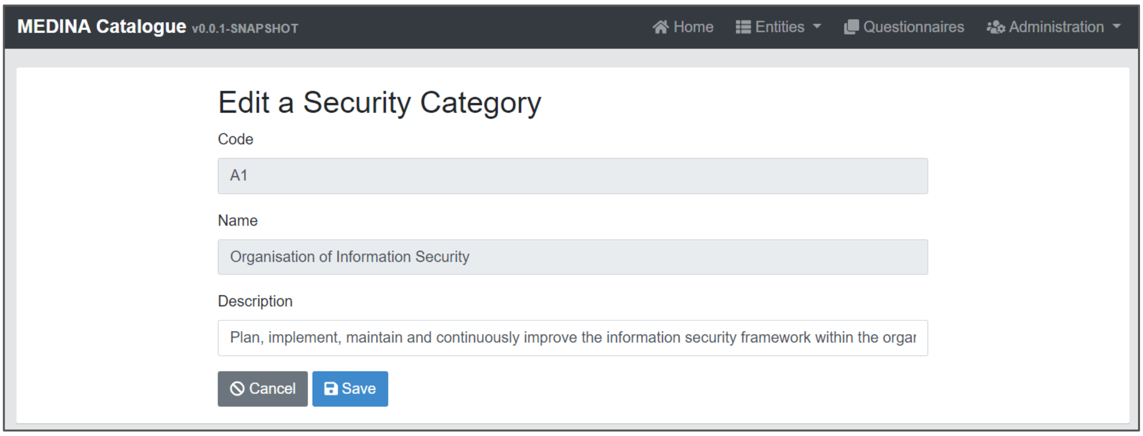
Code	Name	Description	Security Framework	Related Controls
A1	Organisation of Information Security	Plan, implement, maintain and continuously improve the information security framework within the organisation	EUCS ↑	Controls ↓
A2	Information Security Policies	Provide a global information security policy derived into policies and procedures regarding security requirements and to support business requirements	EUCS ↑	Controls ↓
A3	Risk Management	Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements	EUCS ↑	Controls ↓
A4	Human Resources	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation´s assets are protected in the event of	EUCS ↑	Controls ↓

Figure 11. List of Security Categories

The following fields are listed for each Security Category:

- Code
- Name
- Description

As with any other entity in the Catalogue, each Security Category allows to view its detail or edit it. Let's look at the *Edit* window, where only the description can be updated:



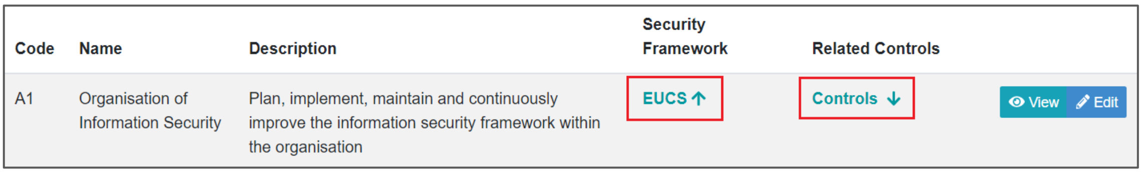
Edit a Security Category

Code: A1

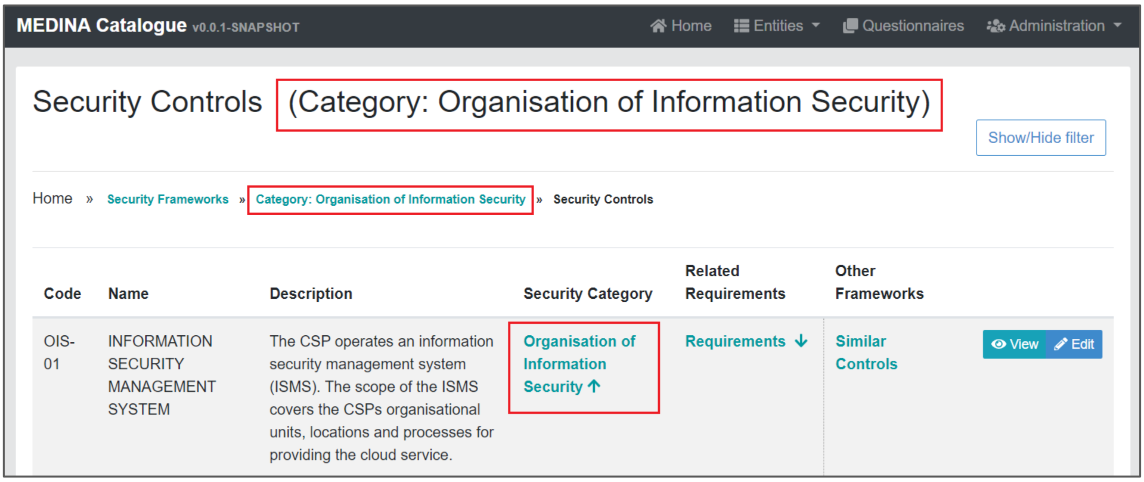
Name: Organisation of Information Security

Description: Plan, implement, maintain and continuously improve the information security framework within the orgar

Finally, for each Security Category in Figure 11, the user can access its related Security Controls or can go back to the Security Frameworks screen, by clicking on the following links:



Code	Name	Description	Security Framework	Related Controls
A1	Organisation of Information Security	Plan, implement, maintain and continuously improve the information security framework within the organisation	EUCS ↑	Controls ↓



Security Controls (Category: Organisation of Information Security)

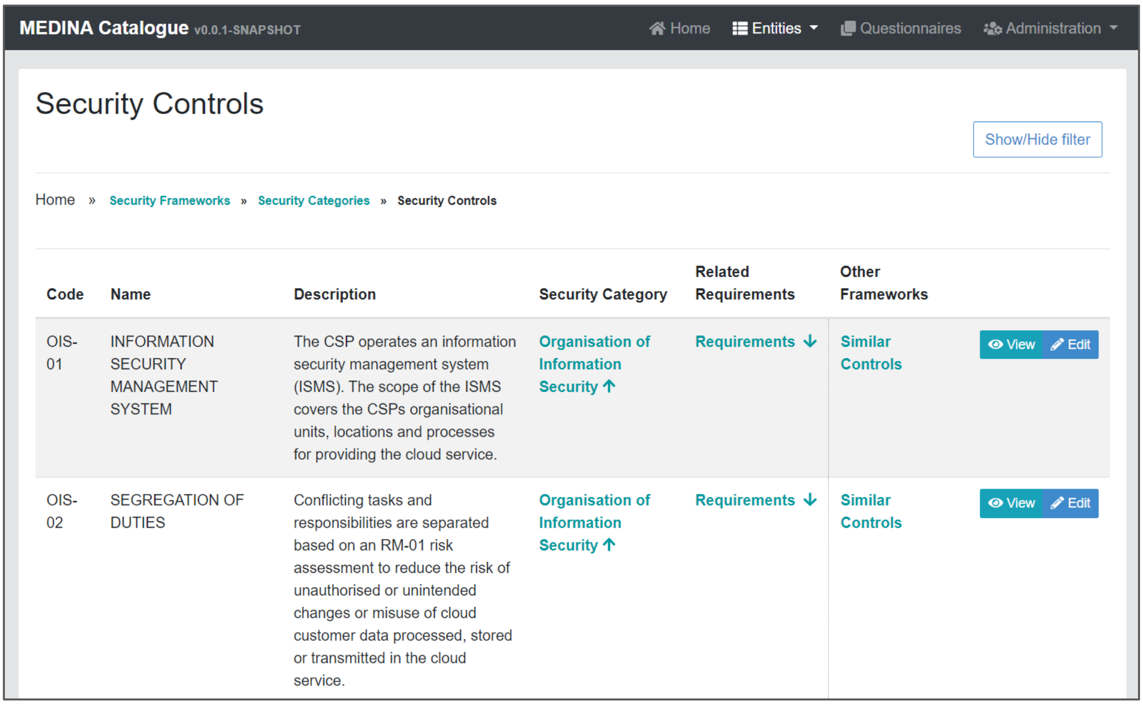
Home » Security Frameworks » Category: Organisation of Information Security » Security Controls

Code	Name	Description	Security Category	Related Requirements	Other Frameworks	
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service.	Organisation of Information Security ↑	Requirements ↓	Similar Controls	View Edit

Figure 12. Security controls belonging to the Security Category "Organisation of Information Security"

5.3.3.2.3. Security Controls

The main *Security Controls* window (see Figure 13) shows all the Security Controls registered in the Catalogue.



Security Controls

Home » Security Frameworks » Security Categories » Security Controls

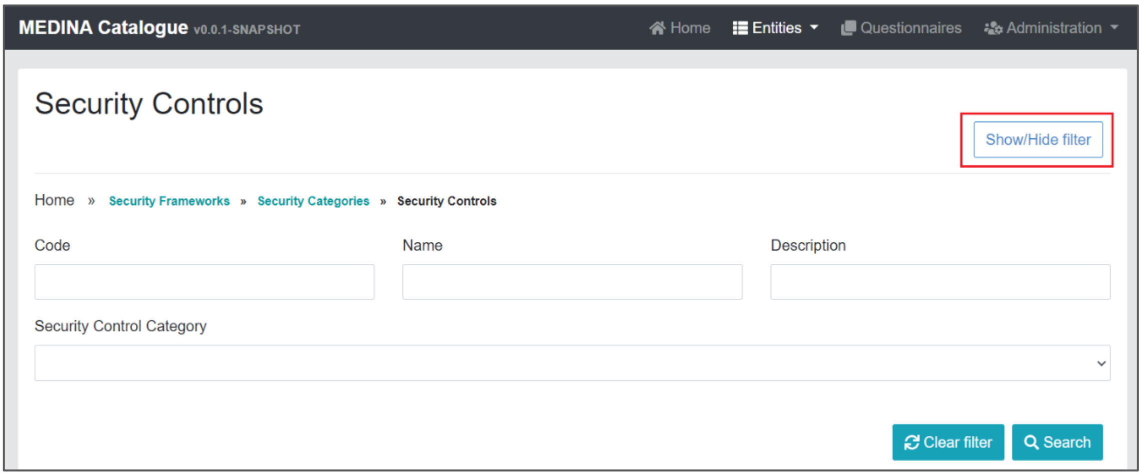
Code	Name	Description	Security Category	Related Requirements	Other Frameworks	
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service.	Organisation of Information Security ↑	Requirements ↓	Similar Controls	View Edit
OIS-02	SEGREGATION OF DUTIES	Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.	Organisation of Information Security ↑	Requirements ↓	Similar Controls	View Edit

Figure 13. List of Security Controls

The following fields are listed for each Security Control:

- Code
- Name
- Description

The list of Security Controls in Figure 13 can be customized using the implemented filters (code, name, description and Security Category):



Security Controls

Home » Security Frameworks » Security Categories » Security Controls

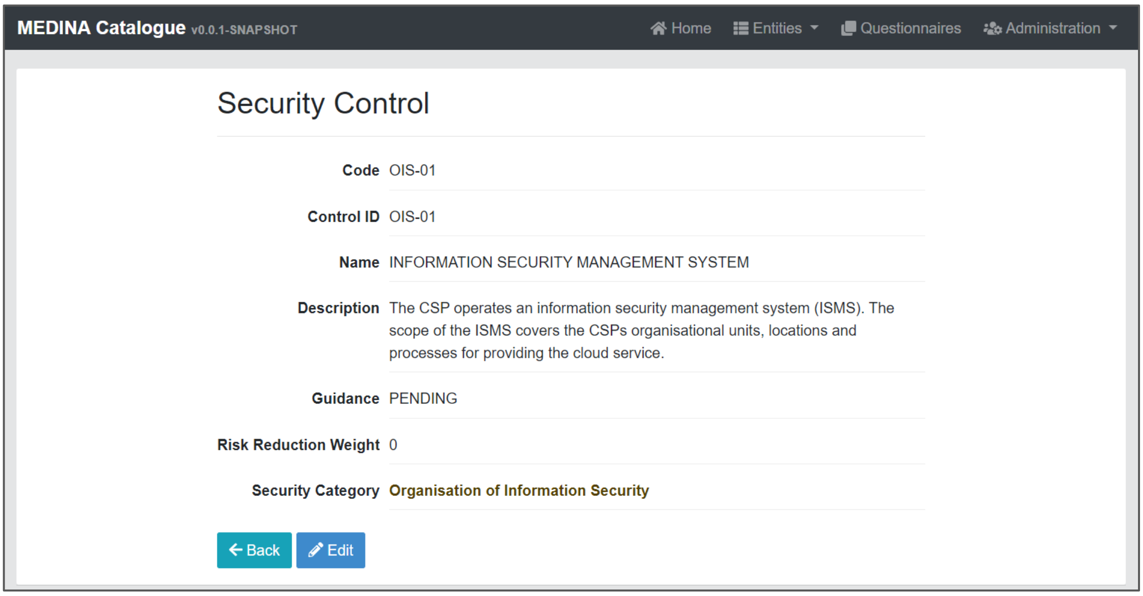
Code

Name

Description

Security Control Category

In Figure 13 each Security Control can be edited and its details can be consulted by clicking on the *View* button:



Security Control

Code OIS-01

Control ID OIS-01

Name INFORMATION SECURITY MANAGEMENT SYSTEM

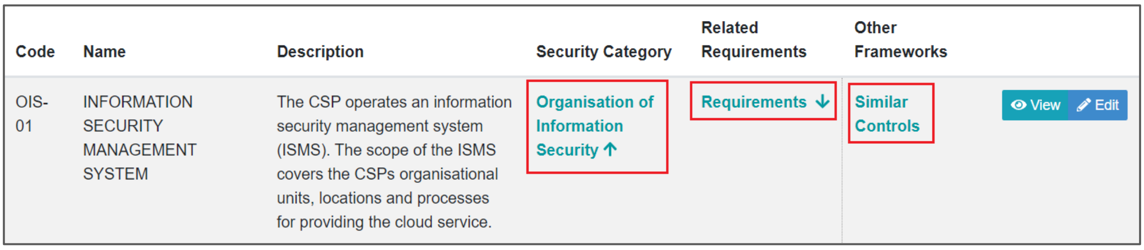
Description The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service.

Guidance PENDING

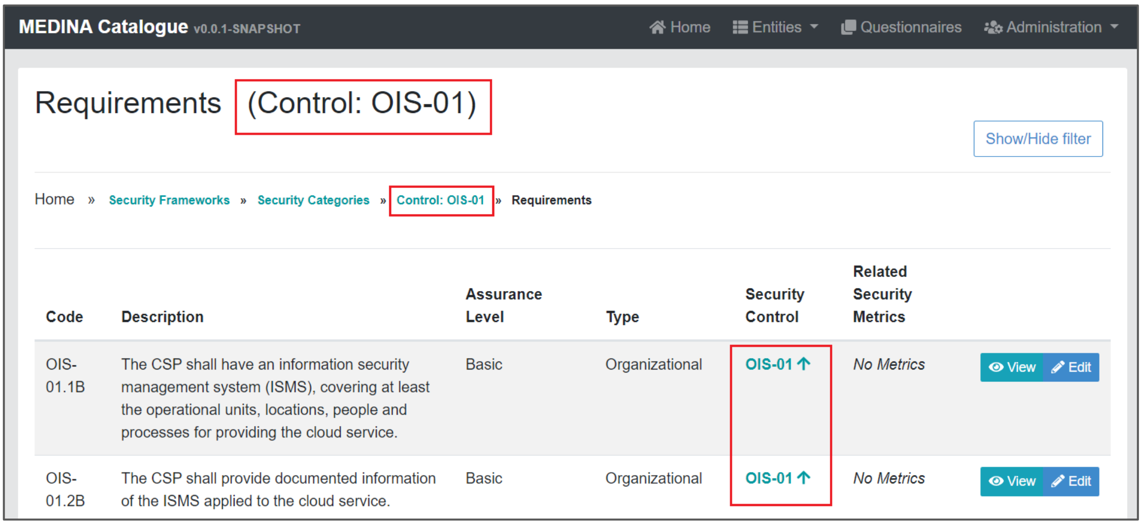
Risk Reduction Weight 0

Security Category Organisation of Information Security

Finally, for each Security Control in Figure 13, the user can go back to its Security Category, can access its related Requirements, or can consult Similar Controls in other frameworks, by clicking on the following links:



Code	Name	Description	Security Category	Related Requirements	Other Frameworks	
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSPs organisational units, locations and processes for providing the cloud service.	Organisation of Information Security ↑	Requirements ↓	Similar Controls	View Edit



Requirements (Control: OIS-01)

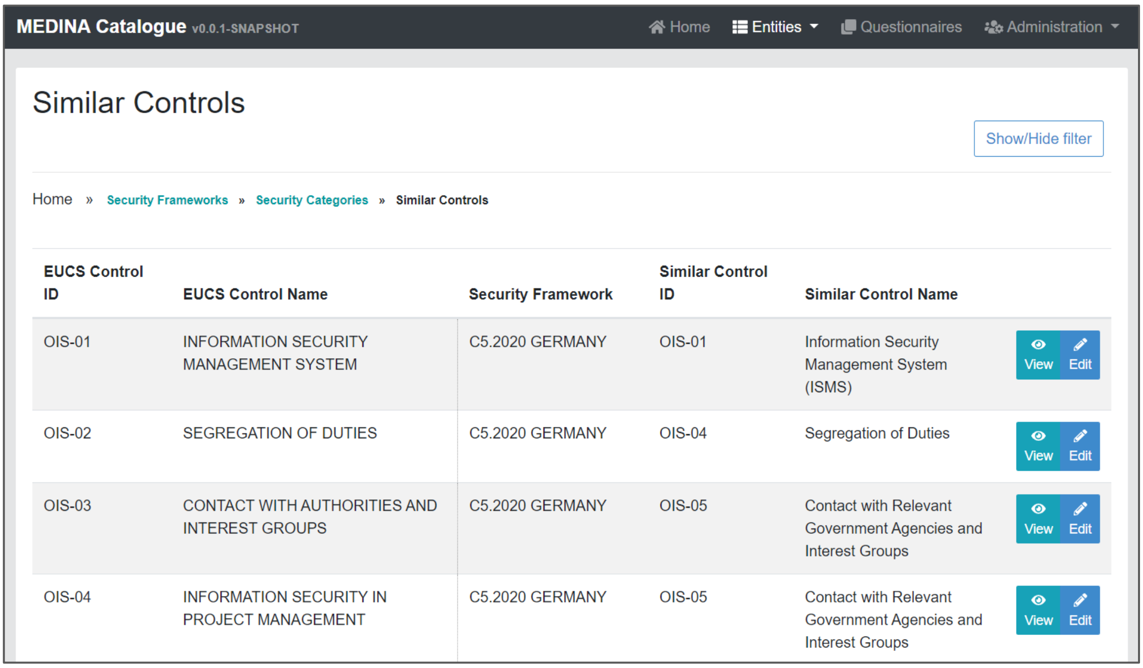
Home » Security Frameworks » Security Categories » Control: OIS-01 » Requirements

Code	Description	Assurance Level	Type	Security Control	Related Security Metrics	
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.	Basic	Organizational	OIS-01 ↑	*No Metrics*	View Edit
OIS-01.2B	The CSP shall provide documented information of the ISMS applied to the cloud service.	Basic	Organizational	OIS-01 ↑	*No Metrics*	View Edit

Figure 14. Requirements belonging to the OIS-01 Security Control

5.3.3.2.4. Similar Controls

The main *Similar Controls* window (see Figure 15) shows the list of Security Controls belonging to other Security Frameworks that are related to the EUCS Security Framework:



Similar Controls

Home » Security Frameworks » Security Categories » Similar Controls

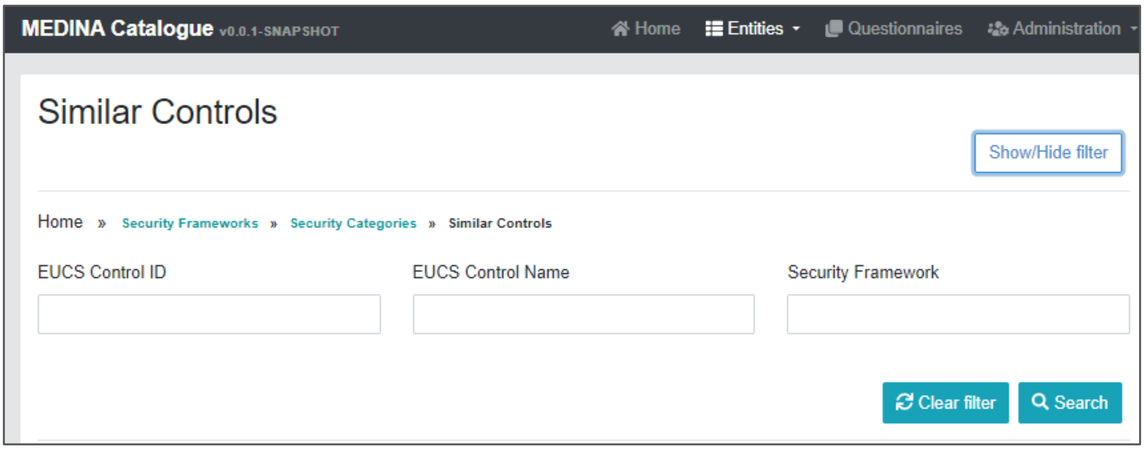
EUCS Control ID	EUCS Control Name	Security Framework	Similar Control ID	Similar Control Name	
OIS-01	INFORMATION SECURITY MANAGEMENT SYSTEM	C5.2020 GERMANY	OIS-01	Information Security Management System (ISMS)	View Edit
OIS-02	SEGREGATION OF DUTIES	C5.2020 GERMANY	OIS-04	Segregation of Duties	View Edit
OIS-03	CONTACT WITH AUTHORITIES AND INTEREST GROUPS	C5.2020 GERMANY	OIS-05	Contact with Relevant Government Agencies and Interest Groups	View Edit
OIS-04	INFORMATION SECURITY IN PROJECT MANAGEMENT	C5.2020 GERMANY	OIS-05	Contact with Relevant Government Agencies and Interest Groups	View Edit

Figure 15. List of Similar Controls

The following fields are listed:

- EUCS Control ID
- EUCS Control Name
- Security Framework (other)
- Similar Control ID
- Similar Control Name

The list of Similar Controls in Figure 15 can be customized using the implemented filters (Control ID, Control name and Security Framework):



Similar Controls

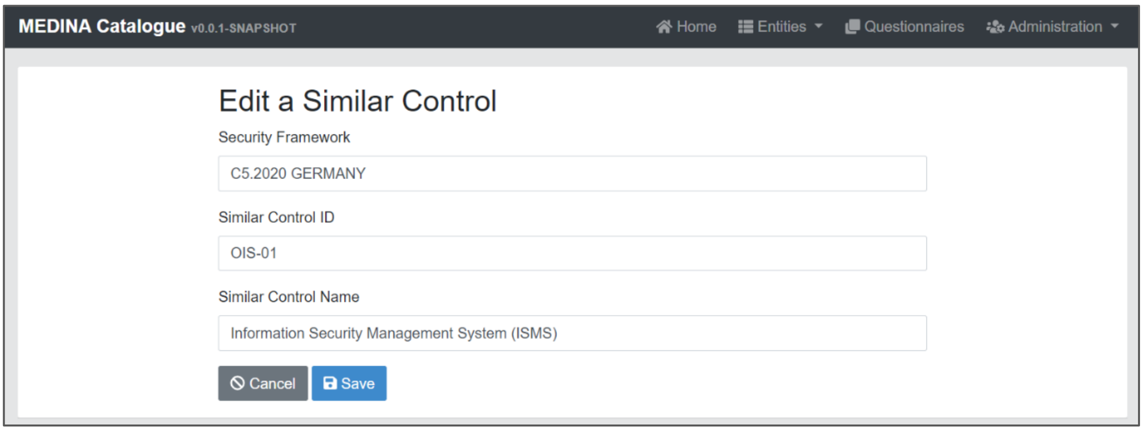
Home » Security Frameworks » Security Categories » Similar Controls

EUCS Control ID

EUCS Control Name

Security Framework

Each Similar Control can be edited and its detail can be consulted. By clicking on the *Edit* button, the Security Framework, Similar Control ID and Similar Control Name fields can be updated:



Edit a Similar Control

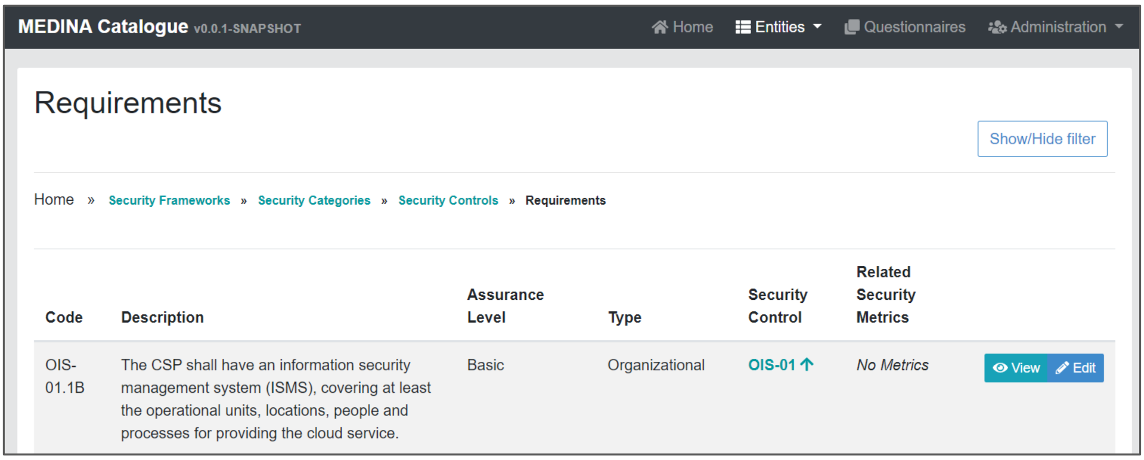
Security Framework: C5.2020 GERMANY

Similar Control ID: OIS-01

Similar Control Name: Information Security Management System (ISMS)

5.3.3.2.5. Requirements

The main *Requirements* window (see Figure 16) shows the list of Requirements registered in the Catalogue.



Requirements

Home » Security Frameworks » Security Categories » Security Controls » Requirements

Code	Description	Assurance Level	Type	Security Control	Related Security Metrics	
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.	Basic	Organizational	OIS-01 ↑	*No Metrics*	View Edit

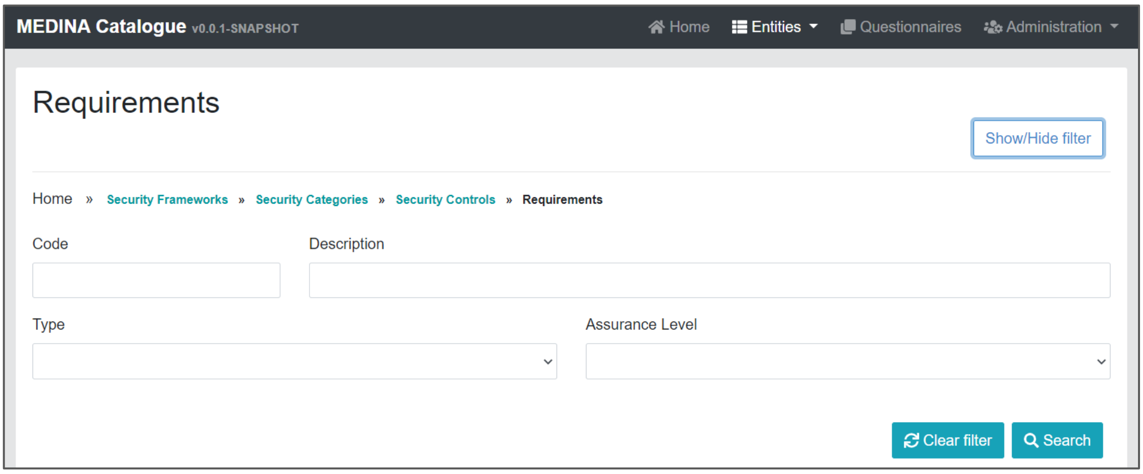
Figure 16. List of Requirements

The following fields are listed for each Requirement:

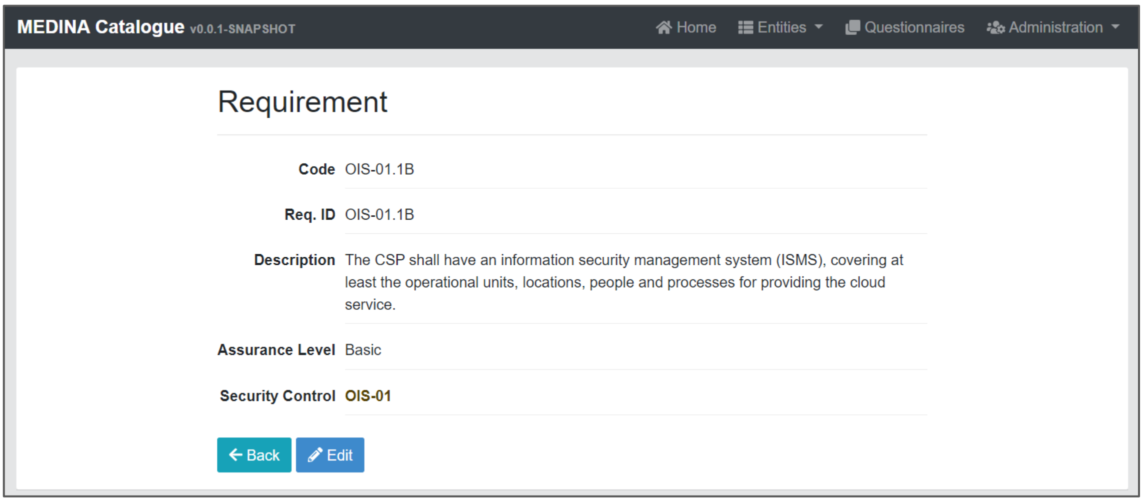
- Code

- Description
- Assurance Level
- Type

The list of requirements in Figure 16 can be customized using the implemented filters (code, description, type and assurance level):

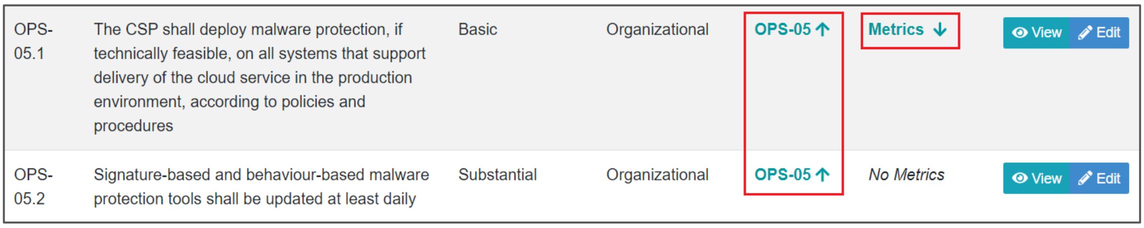


In addition, a Requirement can be edited by clicking on the *Edit* button:

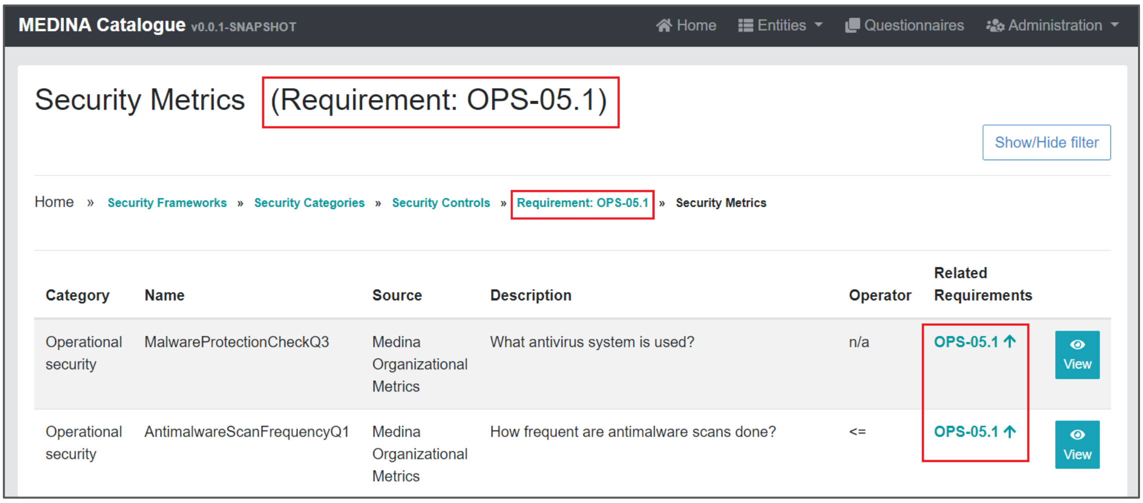


Code	OIS-01.1B
Req. ID	OIS-01.1B
Description	The CSP shall have an information security management system (ISMS), covering at least the operational units, locations, people and processes for providing the cloud service.
Assurance Level	Basic
Security Control	OIS-01

For each Requirement listed in In Figure 16, the user can go back to the Security Controls window or can access its related Security Metrics (if any), by clicking on the following links:



OPS-05.1	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures	Basic	Organizational	OPS-05 ↑	Metrics ↓	View Edit
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial	Organizational	OPS-05 ↑	*No Metrics*	View Edit



Security Metrics (Requirement: OPS-05.1)

Home » Security Frameworks » Security Categories » Security Controls » Requirement: OPS-05.1 » Security Metrics

Category	Name	Source	Description	Operator	Related Requirements
Operational security	MalwareProtectionCheckQ3	Medina Organizational Metrics	What antivirus system is used?	n/a	OPS-05.1 ↑
Operational security	AntimalwareScanFrequencyQ1	Medina Organizational Metrics	How frequent are antimalware scans done?	<=	OPS-05.1 ↑

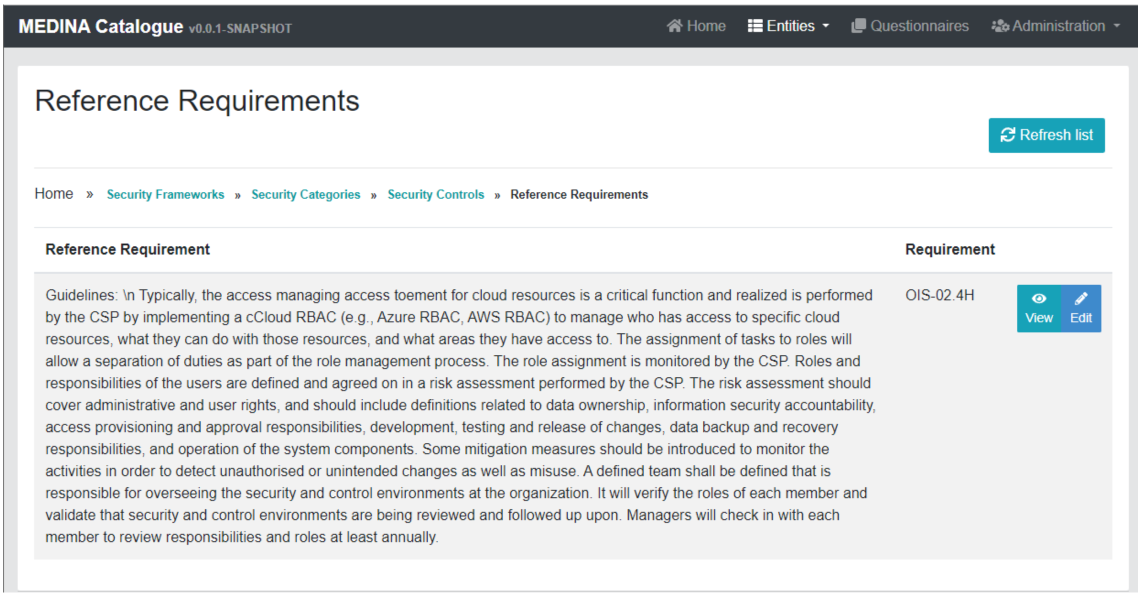
Figure 17. Security Metrics belonging to the OIS-05.1 Requirement

5.3.3.2.6. Reference Requirements

The main *Reference Requirements* window (see Figure 18) shows the list of Reference Requirements registered in the Catalogue.

The following fields are listed for each Reference Requirement:

- Requirement identification
- Some guidelines for the implementation of the requirement



Reference Requirements

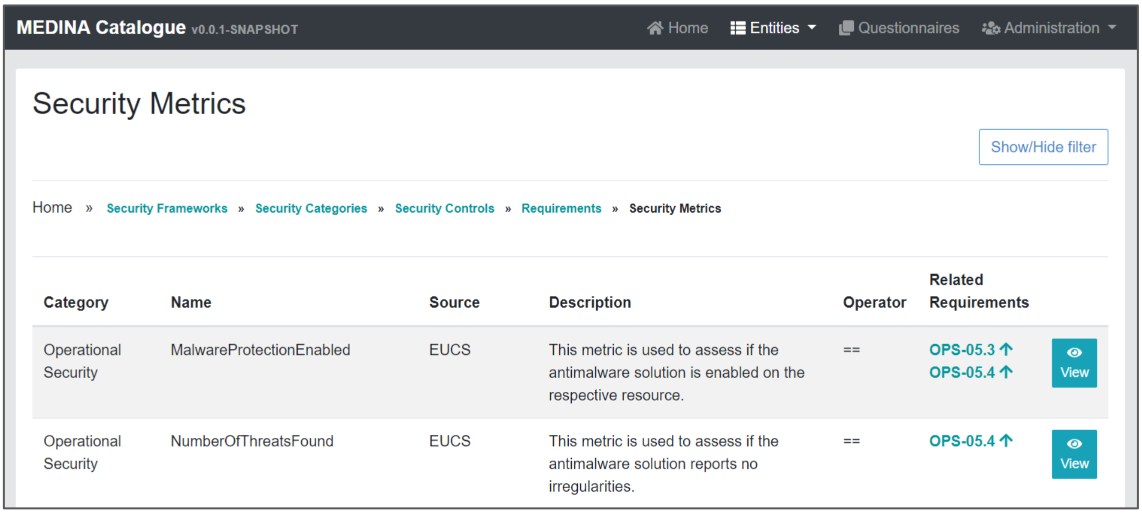
Home » Security Frameworks » Security Categories » Security Controls » Reference Requirements

Reference Requirement	Requirement
Guidelines: \n Typically, the access managing access toement for cloud resources is a critical function and realized is performed by the CSP by implementing a cCloud RBAC (e.g., Azure RBAC, AWS RBAC) to manage who has access to specific cloud resources, what they can do with those resources, and what areas they have access to. The assignment of tasks to roles will allow a separation of duties as part of the role management process. The role assignment is monitored by the CSP. Roles and responsibilities of the users are defined and agreed on in a risk assessment performed by the CSP. The risk assessment should cover administrative and user rights, and should include definitions related to data ownership, information security accountability, access provisioning and approval responsibilities, development, testing and release of changes, data backup and recovery responsibilities, and operation of the system components. Some mitigation measures should be introduced to monitor the activities in order to detect unauthorised or unintended changes as well as misuse. A defined team shall be defined that is responsible for overseeing the security and control environments at the organization. It will verify the roles of each member and validate that security and control environments are being reviewed and followed up upon. Managers will check in with each member to review responsibilities and roles at least annually.	OIS-02.4H

Figure 18. Reference Requirement

5.3.3.2.7. Security Metrics

The main *Security Metrics* screen (see Figure 19) shows the list of all the registered metrics in the Catalogue.



Security Metrics

Home » Security Frameworks » Security Categories » Security Controls » Requirements » Security Metrics

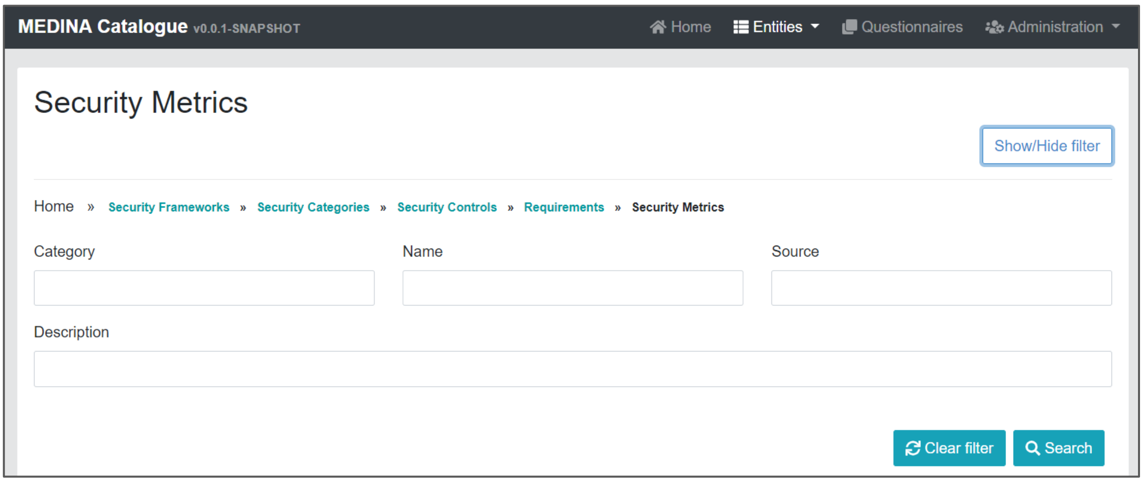
Category	Name	Source	Description	Operator	Related Requirements
Operational Security	MalwareProtectionEnabled	EUCS	This metric is used to assess if the antimalware solution is enabled on the respective resource.	==	OPS-05.3 ↑ OPS-05.4 ↑
Operational Security	NumberOfThreatsFound	EUCS	This metric is used to assess if the antimalware solution reports no irregularities.	==	OPS-05.4 ↑

Figure 19. List of Security Metrics

The following fields are listed for each metric:

- Category
- Name
- Source
- Description
- Operator

The list of Security Metrics in Figure 19 can be customized using the implemented filters (category, name, source and description):



Security Metrics

Home » Security Frameworks » Security Categories » Security Controls » Requirements » Security Metrics

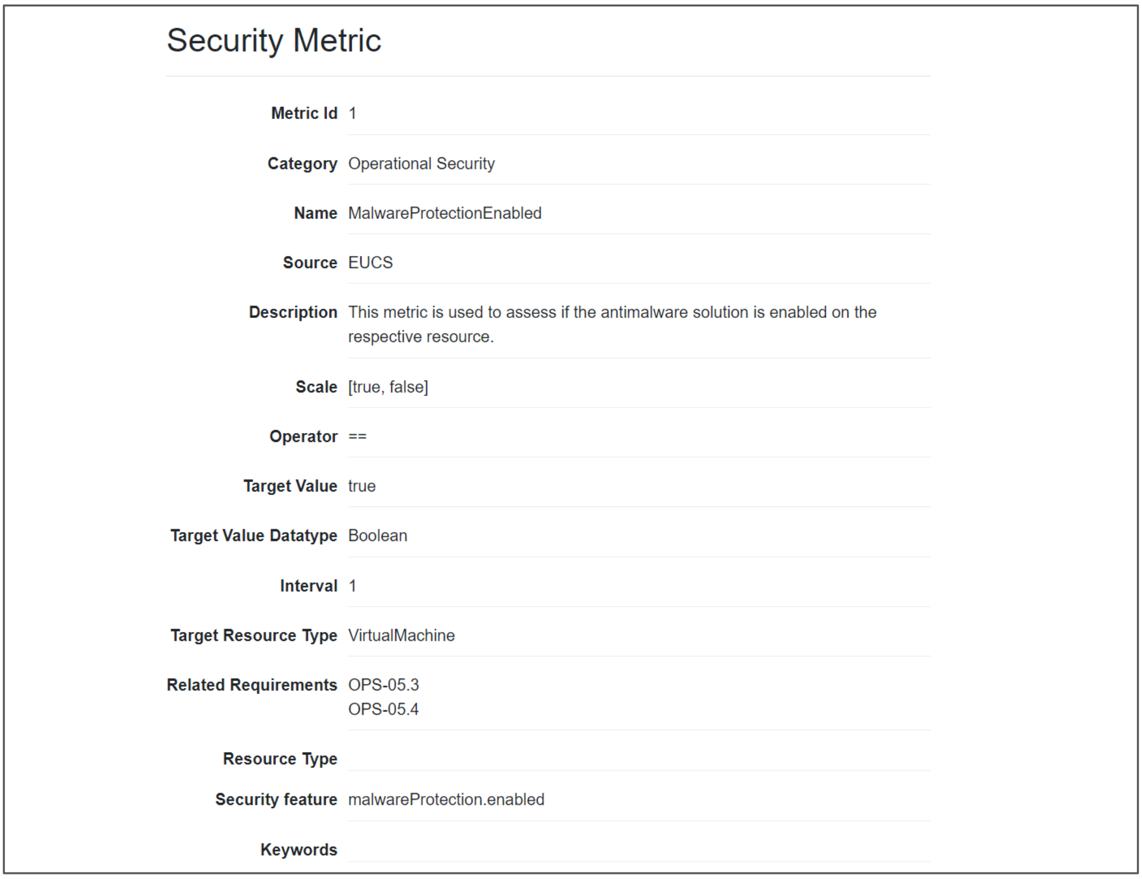
Category

Name

Source

Description

The user can consult the detail of each Security Metric by clicking on the *View* button:



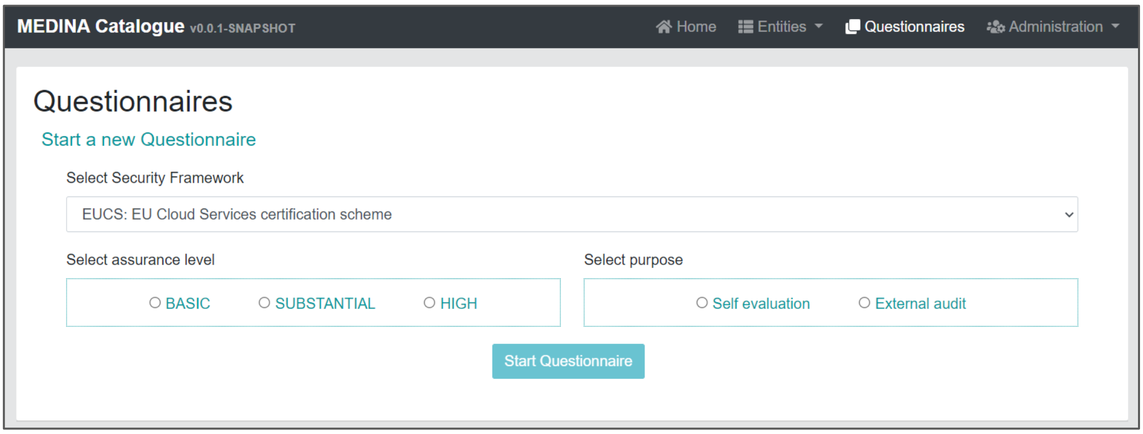
Security Metric

Metric Id	1
Category	Operational Security
Name	MalwareProtectionEnabled
Source	EUCS
Description	This metric is used to assess if the antimalware solution is enabled on the respective resource.
Scale	[true, false]
Operator	==
Target Value	true
Target Value Datatype	Boolean
Interval	1
Target Resource Type	VirtualMachine
Related Requirements	OPS-05.3 OPS-05.4
Resource Type	
Security feature	malwareProtection.enabled
Keywords	

For each metric listed in Figure 19, the user can go to its related requirements by clicking on the corresponding link.

5.3.3.3. *Questionnaires*

The user can create a new questionnaire by clicking on the *Questionnaires* menu option at the top of the window .



Questionnaires

Start a new Questionnaire

Select Security Framework: EUCS: EU Cloud Services certification scheme

Select assurance level: ○ BASIC ○ SUBSTANTIAL ○ HIGH

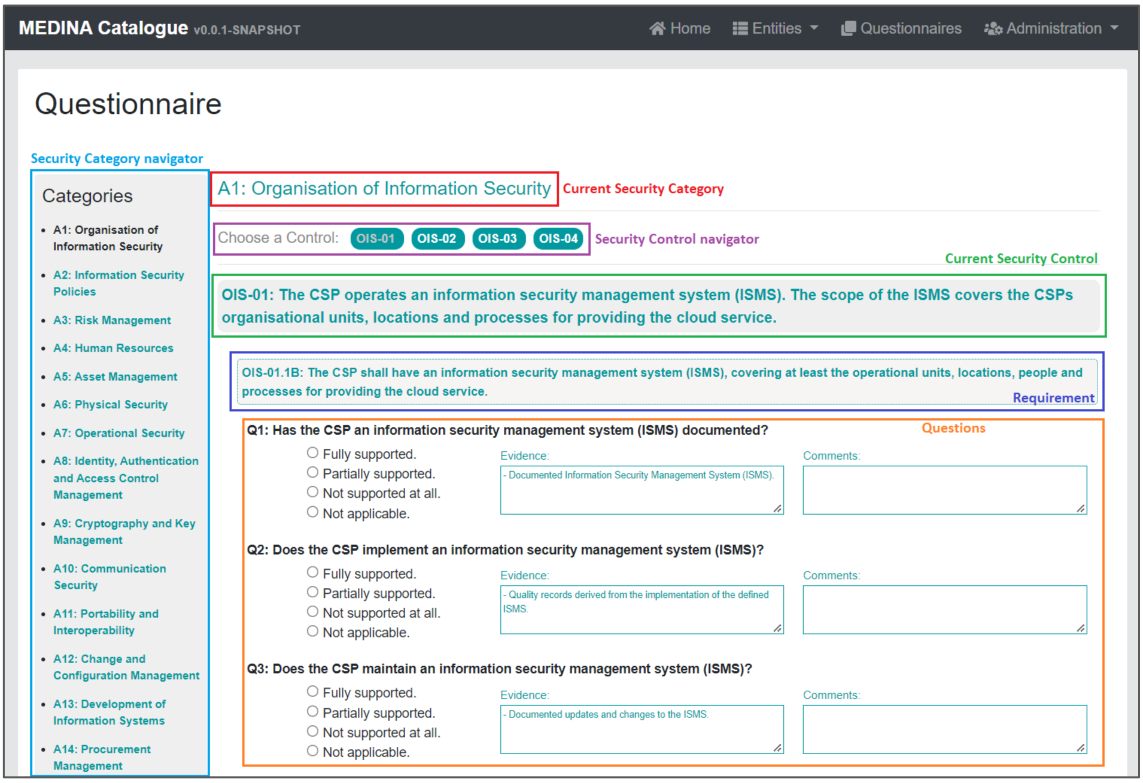
Select purpose: ○ Self evaluation ○ External audit

Figure 20. Start a new Questionnaire

To start a new Questionnaire, the user must fill in the following fields (see Figure 20):

- **Security Framework**: the current version only includes EUCS
- **Assurance level**: BASIC, SUBSTANTIAL or HIGH
- **Purpose**: Self-evaluation or External audit

When the user clicks on *Start Questionnare* button a new Questionnaire is created, and the window in Figure 21 is displayed. The panel on the left consists of a navigator through which the different Security Categories of the Security Framework can be accessed.


MEDINA Catalogue v0.0.1-SNAPSHOT
Home
Entities
Questionnaires
Administration
Security Category navigator
Current Security Category
Security Control navigator
Current Security Control
Requirement
Questions

Questionnaire

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

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

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

OIS-01.1B: 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: Has the CSP an information security management system (ISMS) documented?

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

Evidence: - Documented Information Security Management System (ISMS).

Comments:

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

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

Evidence: - Quality records derived from the implementation of the defined ISMS.

Comments:

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

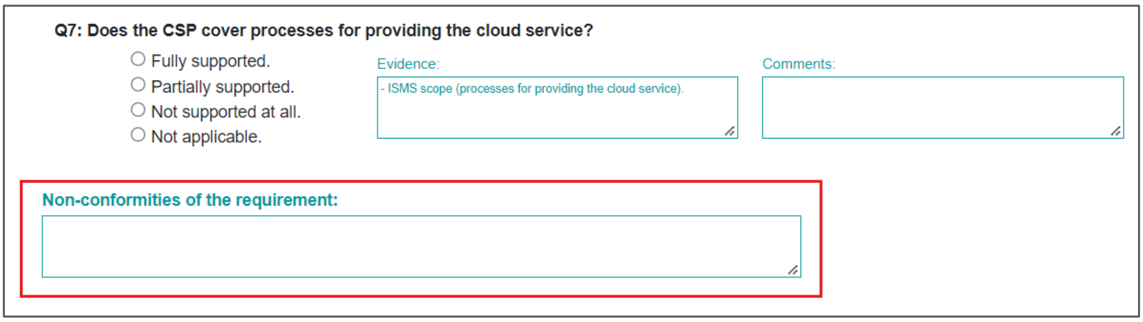
○ Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - Documented updates and changes to the ISMS.

Comments:

Figure 21. Questionnaire structure

Each page corresponds to a Security Control, and includes a Security Control navigator (see Figure 21), all the Requirements belonging to the Security Control and its associated questions, as well as a field at the end of the Requirement to indicate non-conformities:



Q7: Does the CSP cover processes for providing the cloud service?

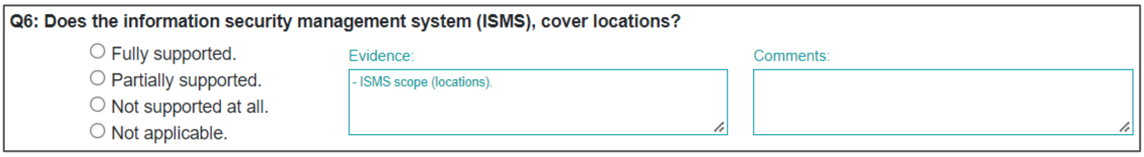
○ Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - ISMS scope (processes for providing the cloud service).

Comments:

Non-conformities of the requirement:

In addition, each question includes a field to record the evidence and add comments:



Q6: Does the information security management system (ISMS), cover locations?

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

Evidence: - ISMS scope (locations).

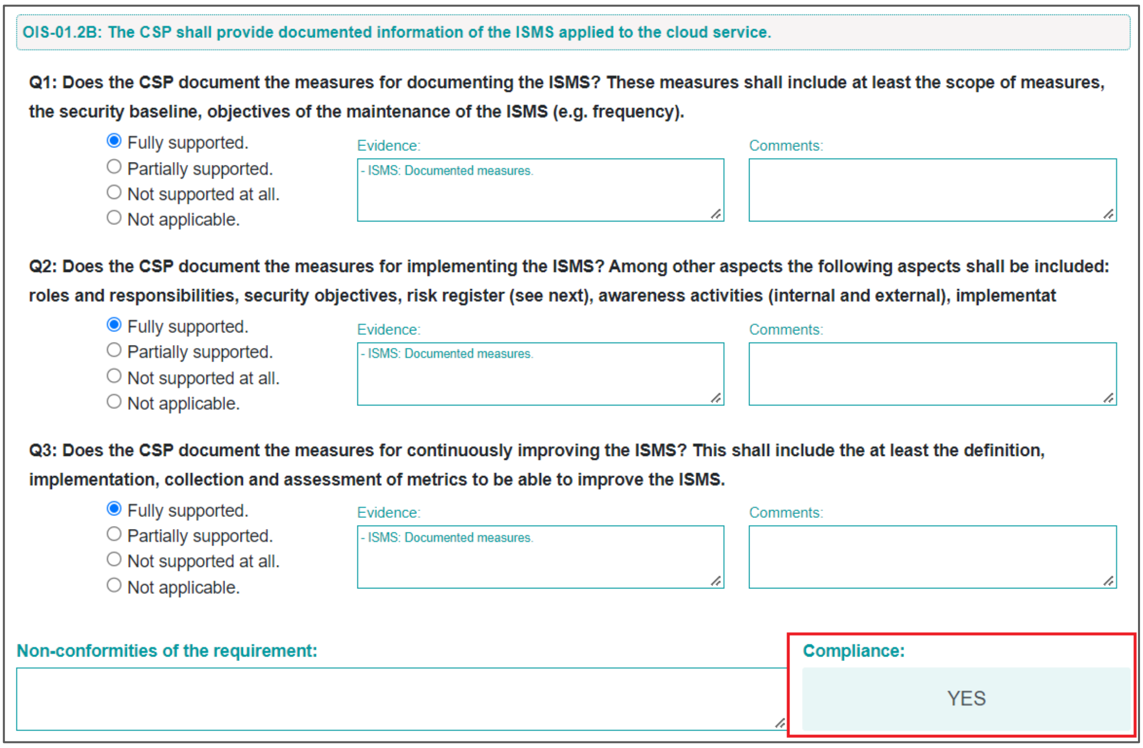
Comments:

Each question has four possible answers:

- Fully supported
- Partially supported

- Not supported at all
- Not applicable

Once all the questions of a Requirement have been answered, the degree of Compliance of the Requirement is calculated and displayed at the bottom of the screen:



OIS-01.2B: The CSP shall provide documented information of the ISMS applied to the cloud service.

Q1: Does the CSP document the measures for documenting the ISMS? These measures shall include at least the scope of measures, the security baseline, objectives of the maintenance of the ISMS (e.g. frequency).

● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - ISMS: Documented measures.

Comments:

Q2: Does the CSP document the measures for implementing the ISMS? Among other aspects the following aspects shall be included: roles and responsibilities, security objectives, risk register (see next), awareness activities (internal and external), implementat

● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - ISMS: Documented measures.

Comments:

Q3: Does the CSP document the measures for continuously improving the ISMS? This shall include the at least the definition, implementation, collection and assessment of metrics to be able to improve the ISMS.

● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - ISMS: Documented measures.

Comments:

Non-conformities of the requirement:

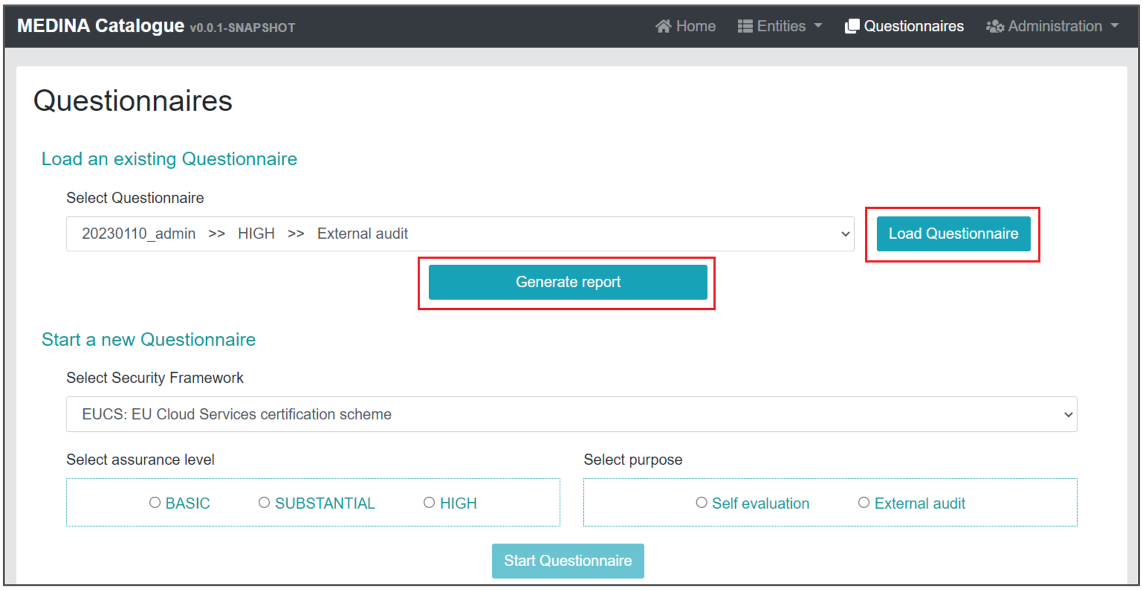
Compliance: YES

The compliance vale of a requirement is calculated according to the following criteria:

Answers	Compliance
All “Fully supported” or “Not applicable”	YES
All “Not supported at all” or “Not applicable”	NO
All “Not applicable”	N/A
Any “Not supported at all”	PARTIAL
Any “Partially supported”	PARTIAL

Finally, at the bottom of the page there are some buttons to *Exit* the Questionnaire, go to the *Previous*/*Next* Security Control and *Save* the Questionnaire:

When there is at least one Questionnaire stored in the Catalogue (see Figure 22), the user can select the previously created Questionnaire to load for further edition (see Figure 23).



Questionnaires

Load an existing Questionnaire

Select Questionnaire: 20230110_admin >> HIGH >> External audit

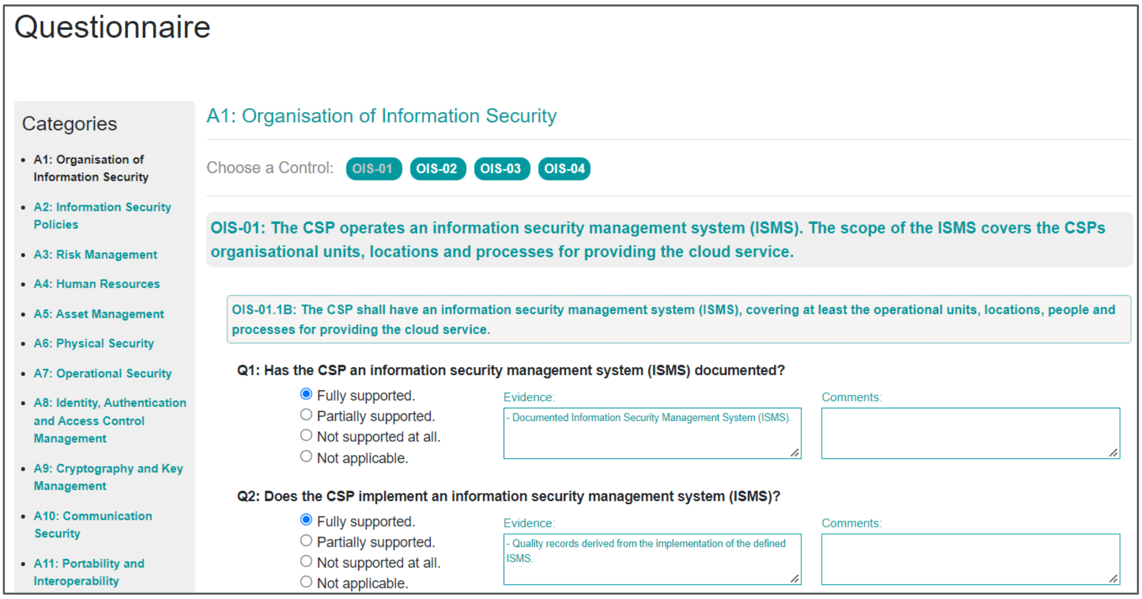
Start a new Questionnaire

Select Security Framework: EUCS: EU Cloud Services certification scheme

Select assurance level: ○ BASIC ○ SUBSTANTIAL ○ HIGH

Select purpose: ○ Self evaluation ○ External audit

Figure 22. Load an existing Questionnaire



Questionnaire

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

A1: Organisation of Information Security

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

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

OIS-01.1B: 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: Has the CSP an information security management system (ISMS) documented?

● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - Documented Information Security Management System (ISMS).

Comments:

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

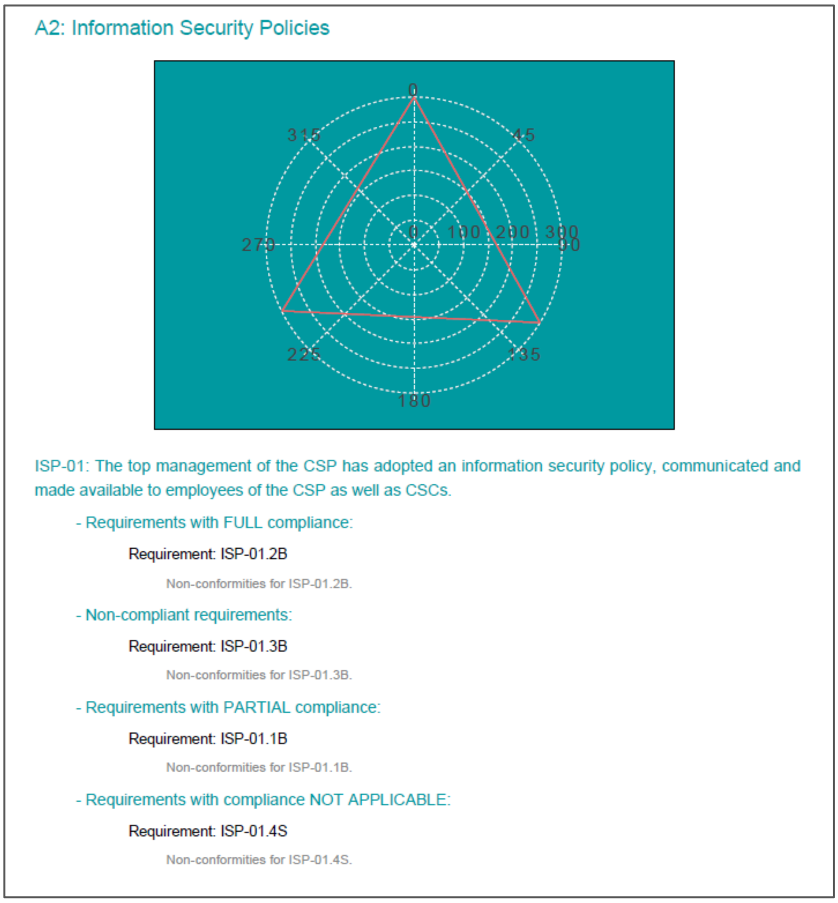
● Fully supported.
○ Partially supported.
○ Not supported at all.
○ Not applicable.

Evidence: - Quality records derived from the implementation of the defined ISMS.

Comments:

Figure 23. Edit an existing Questionnaire

By clicking on the *Generate report* button in Figure 22, a report containing the evaluation results in PDF format is stored in the file system. A screenshot of a section of the report is shown in the next Figure 24.



A2: Information Security Policies

ISP-01: The top management of the CSP has adopted an information security policy, communicated and made available to employees of the CSP as well as CSCs.

- Requirements with FULL compliance:

Requirement: ISP-01.2B

Non-conformities for ISP-01.2B.

- Non-compliant requirements:

Requirement: ISP-01.3B

Non-conformities for ISP-01.3B.

- Requirements with PARTIAL compliance:

Requirement: ISP-01.1B

Non-conformities for ISP-01.1B.

- Requirements with compliance NOT APPLICABLE:

Requirement: ISP-01.4S

Non-conformities for ISP-01.4S.

Figure 24. Report of the questionnaire

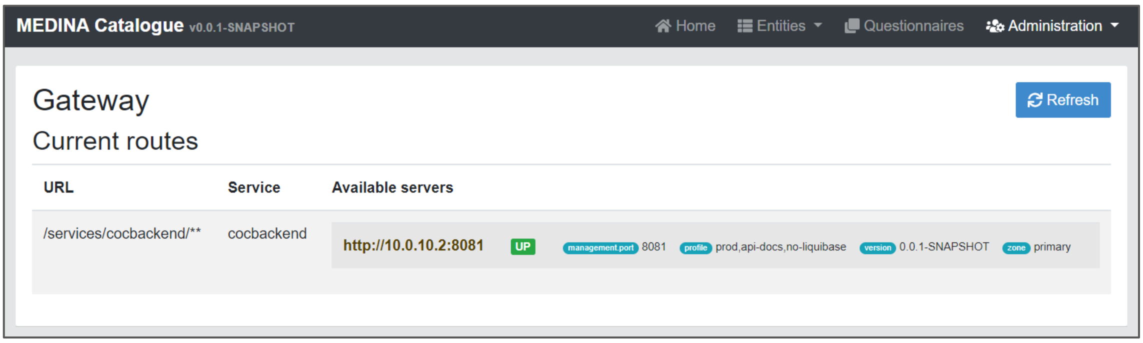
5.3.3.4. Administration

The Administration menu option displays the following submenu options, that will be detailed below:

- Gateway
- API

5.3.3.4.1. Gateway

The Gateway screen shows the status of all the available microservices that make up the Catalogue architecture.



Gateway

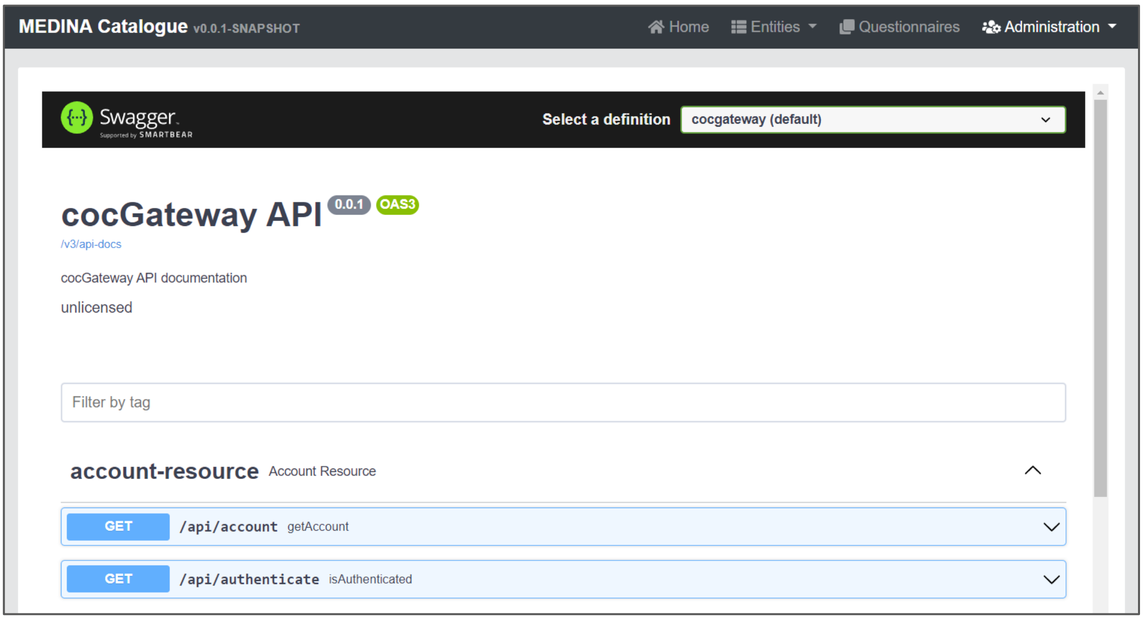
Current routes

URL	Service	Available servers
/services/cocbackend/**	cocbackend	http://10.0.10.2:8081 UP management.port 8081 profile prod,api-docs,no-liquibase version 0.0.1-SNAPSHOT zone primary

Figure 25. Administration menu – Gateway

5.3.3.4.2. API

The API menu option opens a Swagger User Interface to operate with the available REST API in the Catalogue.



cocGateway API

/v3/api-docs

cocGateway API documentation

unlicensed

account-resource Account Resource

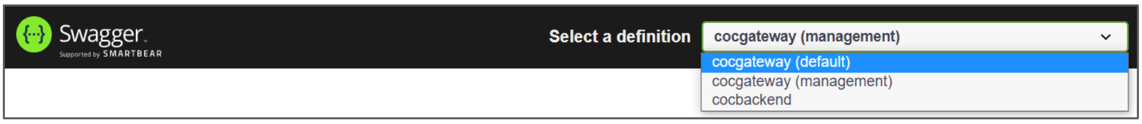
GET /api/account getAccount

GET /api/authenticate isAuthenticated

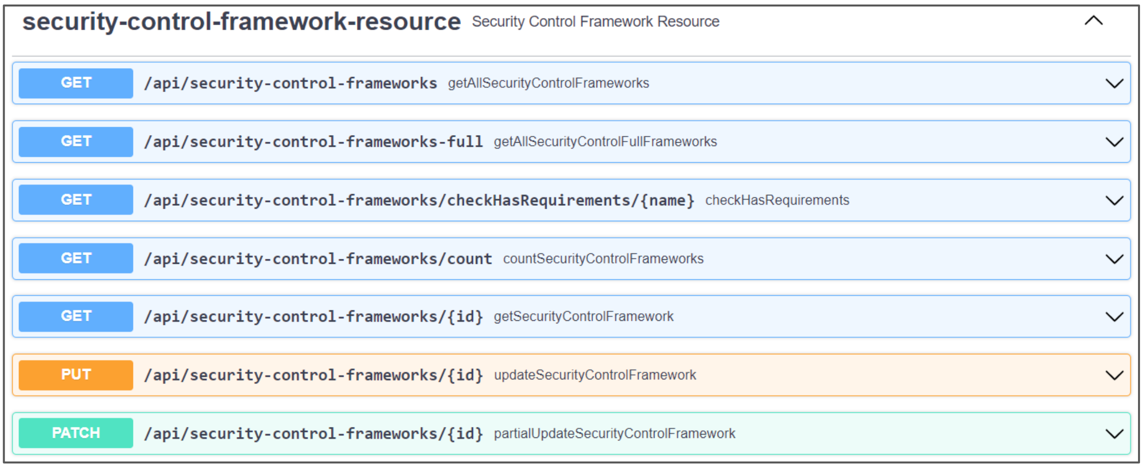
Figure 26. Administration menu – API

Both the Backend and the Frontend subcomponents have their own independent REST API, that can be consulted by choosing the corresponding option in the select box:

- **Frontend**: cocgateway (default)
- **Backend**: cocbackend



Through the Backend API, operations on the Entities (Security Frameworks, Security Categories, Security Controls, Similar Controls, Requirements, Reference Requirements and Security Metrics) and on the Questionnaires can be executed. For example, the available operations for Security Frameworks are:



security-control-framework-resource Security Control Framework Resource

GET /api/security-control-frameworks getAllSecurityControlFrameworks

GET /api/security-control-frameworks-full getAllSecurityControlFullFrameworks

GET /api/security-control-frameworks/checkHasRequirements/{name} checkHasRequirements

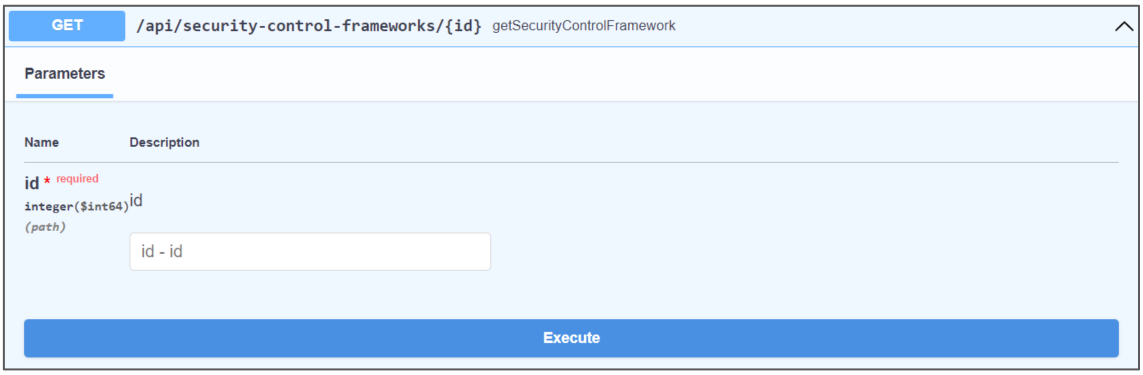
GET /api/security-control-frameworks/count countSecurityControlFrameworks

GET /api/security-control-frameworks/{id} getSecurityControlFramework

PUT /api/security-control-frameworks/{id} updateSecurityControlFramework

PATCH /api/security-control-frameworks/{id} partialUpdateSecurityControlFramework

And following the same example, the operation to obtain all the information about a Security Framework given its ID is:



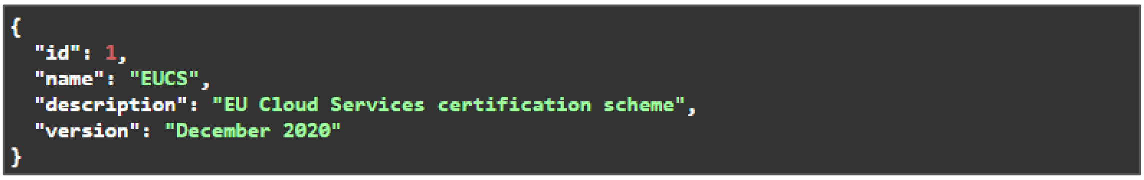
GET /api/security-control-frameworks/{id} getSecurityControlFramework

Parameters

Name	Description
id * required integer($int64) (path)	id id - id

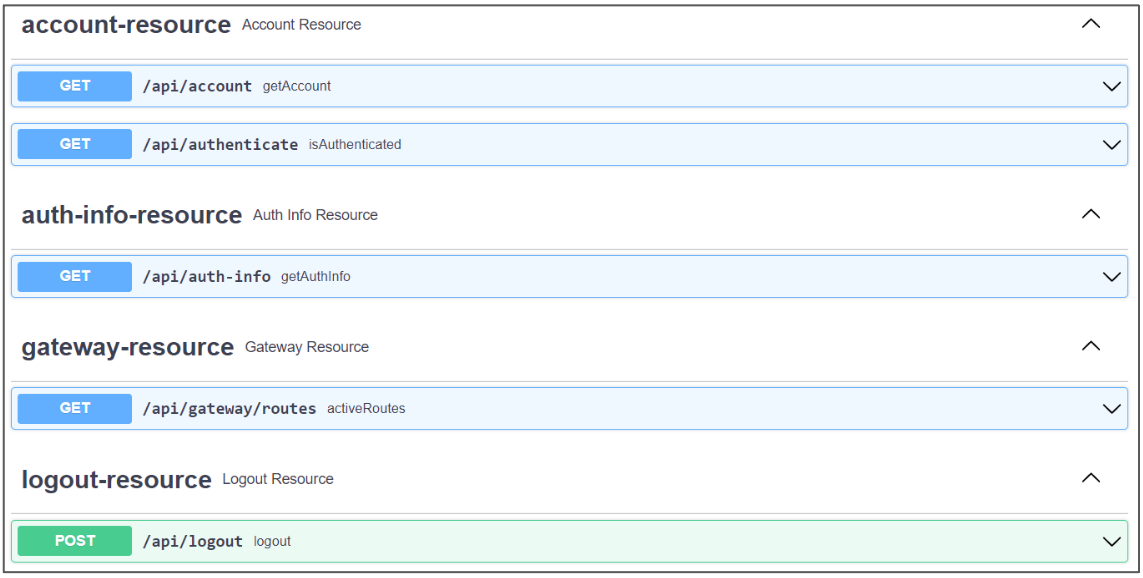
Execute

Entering a Security Framework ID and clicking on *Execute*, the result obtained is:



```
{
  "id": 1,
  "name": "EUCS",
  "description": "EU Cloud Services certification scheme",
  "version": "December 2020"
}
```

Finally, the Frontend API is mainly used to operate on users and accounts:



account-resource Account Resource

GET /api/account getAccount

GET /api/authenticate isAuthenticated

auth-info-resource Auth Info Resource

GET /api/auth-info getAuthInfo

gateway-resource Gateway Resource

GET /api/gateway/routes activeRoutes

logout-resource Logout Resource

POST /api/logout logout

5.3.4. Licensing information

This component is offered under Apache 2.0 license. The license files and more detailed information can be found in the GitLab repository[33].

5.3.5. Download

The code is available at the public GitLab repository of the MEDINA project:

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

[33] https://git.code.tecnalia.com/medina/public/catalogue-of-controls

6. Conclusions

This deliverable has presented the second version of the MEDINA Catalogue. A main difference with the previous version is that the EUCS draft in which it is based has been upgraded to the August 2022 version of the European draft candidate EUCS.

We have presented a comparative analysis of five schemes, namely EUCS, ISO/IEC 27000 family (27002, 27017), BSI C5, SecNumCloud and Cisco CCF, in different dimensions such as the categories, structure, levels and conformity assessment method. Also, a mapping of the controls among the different schemes has been elaborated.

As a second accomplishment, we have presented an updated set of Reference TOMs for "the 34" requirements – those identified with the assurance level high and requiring 'continuous (automated)' monitoring – in the August 2022 version of the European draft candidate EUCS. A Reference TOMs is a sort of implementation guidance that is vendor and technology agnostic.

A total of 152 metrics has been elicited at this stage, coming from literature and other European projects but also from MEDINA partners. Although most metrics are linked to a high-level assurance requirement, there are some that either have a more general purpose or are compliant with a lower level of assurance requirement, but which are measured by the MEDINA tools. The list of metrics developed at this stage of the project for the 34 requirements is presented, as well as the coverage of those metrics by the MEDINA Evidence management tools. All metrics have been described following the same structure. They all have a defined data type, data range, interval, and formula. The complete list and details of the metrics elicited can be found in *Appendix 2: MEDINA Security metrics*.

The document also includes the functional and technical description of the second version of the *Catalogue of Controls and Metrics* component, and an updated set of the Catalogue requirements defined in D5.2 [3]. The main change of the Catalogue functionality with respect to the previous version is the inclusion of the self-assessment Questionnaires developed in the context of WP3, which include questions for the evaluation of the whole set of EUCS requirements. In addition, the Catalogue implements the update of controls and requirements from the EUCS 2020 draft version to a new draft version (August-2022) and the development of a new set of MEDINA metrics. A complete user manual for the tool is included.

In the remaining months until the final integration of the MEDINA Framework some work is planned to improve the Catalogue component and better integrate it with the other MEDINA components. Communication with the SATRA tool will be finished, the role-based access will be implemented in addition to the current user authentication, and the questionnaire feature will be polished.

7. References

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

[2] ENISA, “EUCS – Cloud Services Scheme,” Draft version provided by ENISA (August 2022) - not intended for being used outside the context of MEDINA, 2022.

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

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

[5] ENISA, “EUCS – Cloud Services Scheme,” [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. [Accessed January 2023].

[6] 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.

[7] ENISA, "AHWG Members," [Online]. Available: https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG02/ahwg02_members. [Accessed January 2023].

[8] CSPCERT Working Group, “Recommendations for the implementation of the CSP Certification scheme,” 2019. [Online]. Available: https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view. [Accessed January 2023].

[9] BSI - German Federal Office for Information Security, “C5:2020,” 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf;jsessionid=5ABF69FC06697133A79E093720DCF888.2_cid502?__blob=publicationFile&v=1. [Accessed January 2023].

[10] ANSSI, “SecNumCloud – Referentiel,” ANSSI, 2022. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf.

[11] International Standards Organisation, “ISO /IEC 27002: 2013 - Information technology - Security techniques - Code of practice for information security management”.

[12] International Standards Organisation, “ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements,” 2013.

[13] International Standards Organization, “ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services”.

[14] International Standard on Assurance Engagements;, “INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS 3000 - ASSURANCE ENGAGEMENTS OTHER THAN AUDITS OR REVIEWS OF HISTORICAL FINANCIAL INFORMATION”.

[15] International Standards Organization, “ISO/IEC 17065:2012(en) - Conformity assessment — Requirements for bodies certifying products, processes and services,” 2021.

[16] BSI - German Federal Office for Information Security;, “Cloud Computing Compliance Controls Catalogue (C5),” 2016. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf;jsessionid=0A26465CAC7891AC14E23B835AB952BC.2_cid369?__blob=publicationFile&v=3. [Accessed January 2023].

[17] BSI - German Federal Information Office, "Referencing Cloud Computing Compliance Criteria Catalogue (C5) to International Standards," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020_Reference_Tables.xlsx?__blob=publicationFile&v=1. [Accessed January 2023].

[18] International Auditing and Assurance Standards Board (IAASB);, “AUDITING INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3402: ASSURANCE REPORTS ON CONTROLS AT A SERVICE ORGANIZATION”.

[19] Cisco Systems, Inc., “Cisco Cloud Controls Framework,” 2022. [Online]. Available: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html. [Accessed January 2023].

[20] MEDINA Consortium, «D2.4 Specification of the Cloud Security Certification Language-v2,» 2022.

[21] Tech Target, “Cloud Security Posture Management,” [Online]. Available: https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM. [Accessed January 2023].

[22] Fugue, "Fugue," [Online]. Available: https://www.fugue.co/cloud-security-posture-management. [Accessed January 2023].

[23] Palo alto networks;, "Prisma cloud," [Online]. Available: https://www.paloaltonetworks.com/resources/datasheets/cloud-security-posture-management. [Accessed January 2023].

[24] Amazon, "Compliance Validation for Amazon RDS," [Online]. Available: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/RDS-compliance.html. [Accessed January 2023].

[25] Amazon, "AWS Security, Identity and Compliance," [Online]. Available: https://aws.amazon.com/es/architecture/security-identity-compliance/?achp_ftd1&cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc. [Accessed January 2023].

[26] S. Harvey, “Why Should Your Employees Sign a Policy Acknowledgement Form?,” [Online]. Available: https://kirkpatrickprice.com/blog/why-should-your-employees-sign-a-policy-acknowledgement-form/. [Accessed January 2023].

[27] Center for information security, “6.2 Establish an Access Revoking Process,” [Online]. Available: https://controls-assessment-specification.readthedocs.io/en/stable/control-6/control-6.2.html. [Accessed January 2023].

[28] Atlantic Software Technologies, “Adaptive Non-Disclosure Agreement (NDA) Manager,” [Online]. Available: https://appsource.microsoft.com/en-us/product/web-apps/atlantic-software.adaptive-nda-az?tab=overview. [Accessed January 2023].

[29] The Balance Careers, “Employee Confidentiality and Non-Disclosure Agreements,” [Online]. Available: https://www.thebalancecareers.com/what-to-look-for-in-an-employee-confidentiality-agreement-2061955. [Accessed January 2023].

[30] ENISA, “EUCS Guidelines,” Draft version provided by ENISA (November 2021) - not intended for being used outside the context of MEDINA, 2021.

[31] Center for Internet Security, “Inventory and Control of Software Assets,” [Online]. Available: https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/. [Accessed January 2023].

[32] Teksetra, “Server Decommissioning Checklist: 11 Simple Steps,” [Online]. Available: https://resources.blmtechnology.com/server-decommissioning-checklist. [Accessed January 2023].

[33] Center for Internet Security, «CIS Control 8: Audit Log Management,» [En línea]. Available: https://www.cisecurity.org/controls/audit-log-management/. [Último acceso: January 2023].

[34] FedRAMP, "FedRAMP Continuous Monitoring Strategy Guide," 2018. [Online]. Available: https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf. [Accessed January 2023].

[35] Gartner, “Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services,” [Online]. Available: https://www.gartner.com/en/documents/3886773/comparing-the-use-of-casb-cspm-and-cwpp-solutions-to-pro. [Accessed January 2023].

[36] Merrian Webster, “Definition of metric,” [Online]. Available: https://www.merriam-webster.com/dictionary/metric. [Accessed January 2023].

[37] NIST, “NIST 800-55r1,” 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf. [Accessed January 2023].

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

[39] CORDIS, “Certification infrastrUcture for MUlti-Layer cloUd Services,” [Online]. Available: https://cordis.europa.eu/project/id/318580/es. [Accessed January 2023].

[40] CORDIS, “Accountability For Cloud and Other Future Internet Services,” [Online]. Available: https://cordis.europa.eu/project/id/317550/es. [Accessed January 2023].

[41] CORDIS, “Secure Provisioning of Cloud Services based on SLA management,” [Online]. Available: https://cordis.europa.eu/project/id/610795/es. [Accessed January 2023].

[42] L. SWEENEY, “k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY,” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 05, pp. 5577-570, 2002.

[43] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam, “L-diversity: Privacy beyond k-anonymity,” *ACM Transactions on Knowledge Discovery from Data,* vol. 1, no. 1, 2007.

[44] N. Li, T. Li y S. Venkatasubramanian, «t-Closeness: Privacy Beyond k-Anonymity and l-Diversity,» de *2007 IEEE 23rd International Conference on Data Engineering*, 2007.

[45] C. Dwork, «Differential Privacy,» de *Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science*, vol. 4052, Springer, Berlin, Heidelberg., 2006.

[46] Center for Internet Security, “Center for Internet Security,” [Online]. Available: https://www.cisecurity.org/. [Accessed January 2023].

[47] CEN CENELEC, “Three level approach for a set of information security and cyber security requirements for cloud services,” DRAFT, 2023.

[48] Internationa Standards Organization, "ISO/IEC 17788:2014 - Information technology — Cloud computing — Overview and vocabulary," 2014.

[49] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations - NIST Special Publication 800-53. rev 4,” 2014.

[50] International Standards Organization, “ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements,” 2013.

[51] Internationa Standards Organization, “ISO/IEC 27000:2018 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary”.

[52] MEDINA Consortium, “D2.3 Specification of the Cloud Security Certification Language-v1,” 2021.

[53] ENISA, “EUCS – Cloud Services Scheme,” [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. [Accessed January 2023].

Appendix 1: Security Requirements relevant for continuous assessment – Description

This appendix provides the detailed list of "the 34" requirements. That is, the requirements in the draft EUCS in its version from August 2022 [2] that are within the scope of MEDINA for continuous assessment[34].

Domain:	A1
Category:	ORGANISATION OF INFORMATION SECURITY
T Objective:	Plan, implement, maintain and continuously improve the information security framework within the organisation.
Control ID:	OIS-02
Control:	SEGREGATION OF DUTIES
Control Objective:	Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.
ReqID:	OIS-02.4H
Requirement:	**The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.**
Assurance Level:	High

Domain:	A2
Category:	INFORMATION SECURITY POLICY
Objective:	Provide appropriate mechanisms for cloud customers
Control ID:	ISP-03
Control:	Exceptions
Control Objective:	Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.
ReqID:	ISP-03.5H
Requirement:	**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.**
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-03
Control:	EMPLOYEE TERMS AND CONDITIONS
Control Objective:	The CSP's employees are required by the employment terms and conditions to comply with applicable policies and procedures relating to information security, and to the CSP's code of ethics, before being granted access to any CSC data or system components under the responsibility of the CSP used to provide the cloud service in the production environment.
ReqID:	HR-03.4H
Requirement:	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**

[34] 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

	the verification of this acknowledgement shall be automatically monitored in the processes and automated systems used to grant access rights to employees.
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-04
Control:	SECURITY AWARENESS AND TRAINING
Control Objective:	The CSP operates a target group-oriented security awareness and training program, which is completed by all employees of the CSP on a regular basis.
ReqID:	HR-04.3H
Requirement:	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.**
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-05
Control:	TERMINATION OR CHANGE IN EMPLOYMENT
Control Objective:	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.
ReqID:	HR-05.2H
Requirement:	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.**
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-06
Control:	CONFIDENTIALITY AGREEMENTS
Control Objective:	Non-disclosure or confidentiality agreements are in place with employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them, in accordance with local legislation and regulation.

ReqID:	HR-06.2H
Requirement:	The agreements shall be accepted by external service providers and suppliers when the contract is agreed, **and this acceptation shall be automatically monitored**.
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-06
Control:	CONFIDENTIALITY AGREEMENTS
Control Objective:	Non-disclosure or confidentiality agreements are in place with employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them, in accordance with local legislation and regulation.
ReqID:	HR-06.3H
Requirement:	The agreements shall be accepted by internal employees of the CSP before authorisation to access CSC data is granted, **and this acceptation shall be automatically monitored.**
Assurance Level:	High

Domain:	A4
Category:	HUMAN RESOURCES
Objective:	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination
Control ID:	HR-06
Control:	CONFIDENTIALITY AGREEMENTS
Control Objective:	Non-disclosure or confidentiality agreements are in place with employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them, in accordance with local legislation and regulation.
ReqID:	HR-06.5H
Requirement:	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 acceptation shall be automatically monitored**.
Assurance Level:	High

Domain:	A5
Category:	ASSET MANAGEMENT
Objective:	Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle
Control ID:	AM-01
Control:	ASSET INVENTORY
Control Objective:	The CSP has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.
ReqID:	AM-01.4H
Requirement:	**The CSP shall automatically monitor the process performing the inventory of assets to guarantee it is up-to-date.**
Assurance Level:	High

Domain:	A5
Category:	ASSET MANAGEMENT
Objective:	Identify the organisation’s own assets and ensure an appropriate level of protection throughout their lifecycle
Control ID:	AM-03
Control:	COMMISSIONING AND DECOMMISSIONING OF HARDWARE
Control Objective:	Procedures for the commissioning and decommissioning of hardware assets used in the provision of the cloud service are documented, communicated and implemented, ensuring the proper configuration before commissioning and the proper deletion of data during decommissioning.
ReqID:	AM-03.4H
Requirement:	**The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.**
Assurance Level:	High

Domain:	A5
Category:	ASSET MANAGEMENT
Objective:	Identify the organisation’s own assets and ensure an appropriate level of protection throughout their lifecycle
Control ID:	AM-04
Control:	ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS
Control Objective:	The CSP’s employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the CSP has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service. Any assets handed over are returned upon termination of employment.
ReqID:	AM-04.1H
Requirement:	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.**
Assurance Level:	High

Domain:	A6
Category:	PHYSICAL SECURITY
Objective:	Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations
Control ID:	PS-02
Control:	PHYSICAL SITE ACCESS CONTROL
Control Objective:	Physical access through the security perimeters are subject to access control measures that match each security area’s requirements and that are supported by an access control system.
ReqID:	PS-02.8H
Requirement:	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.**
Assurance Level:	High

Domain:	A7
Category:	OPERATIONAL SECURITY

Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-02
Control:	CAPACITY MANAGEMENT – MONITORING
Control Objective:	The capacities of critical resources such as IT resources are monitored.
ReqID:	OPS-02.2H
Requirement:	**The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards.**
Assurance Level:	High

Domain:	A7
Category:	OPERATIONAL SECURITY
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-05
Control:	PROTECTION AGAINST MALWARE – IMPLEMENTATION
Control Objective:	Malware protection is deployed and maintained on systems that provide the cloud service.
ReqID:	OPS-05.3H
Requirement:	**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.**
Assurance Level:	High

Domain:	A7
Category:	OPERATIONAL SECURITY
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-07
Control:	Data backup and recovery – monitoring
Control Objective	The proper execution of data backups is monitored.
ReqID:	OPS-07.2H
Requirement:	**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.**
Assurance level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-09
Control:	DATA BACKUP AND RECOVERY – STORAGE

Control Objective:	Backup data is stored at an appropriately remote location.
ReqID:	OPS-09.2H
Requirement:	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.**
Assurance Level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-12
Control:	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS
Control Objective:	Logs are monitored to identify events that may lead to security incidents.
ReqID:	OPS-12.1H
Requirement:	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.
Assurance Level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-12
Control:	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS
Control Objective:	Logs are monitored to identify events that may lead to security incidents.
ReqID:	OPS-12.2H
Requirement:	**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).**
Assurance Level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-13
Control:	LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION
Control Objective:	The confidentiality, integrity and availability of logging and monitoring data are protected with measures adapted to their specific use.
ReqID:	OPS-13.1H

Requirement:	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.**
Assurance Level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-18
Control:	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS
Control Objective:	Online registers are used to identify and publish known vulnerabilities.
ReqID:	OPS-18.6H
Requirement:	**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.**
Assurance Level:	High

Domain:	A7
Category:	Operational Security
Objective:	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Control ID:	OPS-21
Control:	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING
Control Objective:	System components are hardened to reduce their attack surface and eliminate potential attack vectors
ReqID:	OPS-21.1H
Requirement:	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.**
Assurance Level:	High

Domain:	A8
Category:	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT
Objective:	Limit access to information and information processing facilities
Control ID:	IAM-03
Control:	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS
Control Objective:	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.
ReqID:	IAM-03.1H
Requirement:	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 IAM-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.
Assurance Level:	High

Domain:	A8
Category:	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT
Objective:	Limit access to information and information processing facilities
Control ID:	IAM-03
Control:	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS
Control Objective:	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.
ReqID:	IAM-03.2H
Requirement:	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 IAM-02, based on the risks of the accounts, associated access rights and authentication mechanisms, **and automatically monitor its application.**
Assurance Level:	High

Domain:	A8
Category:	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT
Objective:	Limit access to information and information processing facilities
Control ID:	IAM-03
Control:	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS
Control Objective:	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.
ReqID:	IAM-03.5H
Requirement:	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 IAM-02 for user accounts, **and automatically monitor its application.**
Assurance Level:	High

Domain:	A8
Category:	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT
Objective:	Limit access to information and information processing facilities
Control ID:	IAM-03
Control:	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS
Control Objective:	Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.
ReqID:	IAM-03.6H
Requirement:	**The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to authorized persons, as relevant.**
Assurance Level:	High

Domain:	A12
Category:	CHANGE AND CONFIGURATION MANAGEMENT
Objective:	Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service
Control ID:	CCM-04
Control:	APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT

Control Objective:	Changes to the cloud services are approved before being deployed in the production environment.
ReqID:	CCM-04.1H
Requirement:	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.**
Assurance Level:	High

Domain:	A12
Category:	CHANGE AND CONFIGURATION MANAGEMENT
Objective:	Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service
Control ID:	CCM-05
Control:	PERFORMING AND LOGGING CHANGES
Control Objective:	Changes to the cloud services are performed through authorized accounts and traceable to the person or system component who initiated them.
ReqID:	CCM-05.1H
Requirement:	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.**
Assurance Level:	High

Domain:	A14
Category:	PROCUREMENT MANAGEMENT
Objective:	Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements
Control ID:	PM-04
Control:	MONITORING OF COMPLIANCE WITH REQUIREMENTS
Control Objective:	Monitoring mechanisms are in place to ensure that third-parties comply with their regulatory and contractual obligations.
ReqID:	PM-04.7H
Requirement:	**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).**
Assurance Level:	High

Domain:	A14
Category:	PROCUREMENT MANAGEMENT
Objective:	Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements
Control ID:	PM-04
Control:	MONITORING OF COMPLIANCE WITH REQUIREMENTS
Control Objective:	Monitoring mechanisms are in place to ensure that third parties comply with their regulatory and contractual obligations.
ReqID:	PM-04.8H

Requirement:	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.
Assurance Level:	High

Domain:	A15
Category:	INCIDENT MANAGEMENT
Objective:	Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents
Control ID:	IM-02
Control:	PROCESSING OF SECURITY INCIDENTS
Control Objective:	A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.
ReqID:	IM-02.5H
Requirement:	**The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures.**
Assurance Level:	High

Domain:	A17
Category:	COMPLIANCE
Objective:	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements
Control ID:	CO-03
Control:	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM
Control Objective:	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.
ReqID:	CO-03.5H
Requirement:	**Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions.**
Assurance Level:	High

Domain:	A17
Category:	COMPLIANCE
Objective:	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements
Control ID:	CO-03
Control:	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM
Control Objective:	Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.
ReqID:	CO-03.6H
Requirement:	**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.**
Assurance Level:	High

Domain:	A19
Category:	DEALING WITH INVESTIGATION REQUESTS FROM G
Objective:	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data

Control ID:	INQ-03
Control:	CONDITIONS FOR ACCESS TO OR DISCLOSURE OF DATA IN INVESTIGATION REQUESTS
Control Objective:	Investigators only have access to the data required for their investigation after validation of the legality of their request.
ReqID:	INQ-03.4H
Requirement:	**The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.**
Assurance Level:	High

Domain:	A20
Category:	PRODUCT SECURITY
Objective:	Provide appropriate mechanisms for cloud customers
Control ID:	PSS-04
Control:	IMAGES FOR VIRTUAL MACHINES AND CONTAINERS
Control Objective:	Services for providing and managing virtual machines and containers to customers include appropriate protection measures.
ReqID:	PSS-04.2H
Requirement:	**An integrity check shall be performed, automatically monitored and reported to the CSC if the integrity check fails.**
Assurance Level:	High

Appendix 2: MEDINA Security metrics

This appendix presents the definition of all the metrics developed in MEDINA. Some of them are related to “the 34” requirements and some are not. Each metric has been defined to be covered by at least one of the MEDINA tools. At the time of writing, a total of 152 metrics has been defined. We divide the list into two sets: “Technical metrics”, which are measured by the Clouditor, VAT, Wazuh and Codyze tools; and “Organizational metrics”, which are measured by the AMOE tool.

Technical metrics

#	ReqID	Control	Source	Metric	Description	Scale	Op.	Target Value	Value Datatype	Int (h)	Resource Type	Security Feature
1	OPS-05.3H	Protection against malware – implementation	EUCS	MalwareProtectionEnabled	This metric is used to assess if the antimalware solution is enabled on the respective resource	[true, false]	==	true	Boolean	1	VirtualMachine	malwareProtection.enabled
2	OPS-05.3H	PROTECTION AGAINST MALWARE – IMPLEMENTATION	EUCS	NumberOfThreatsFound	This metric is used to assess if the antimalware solution reports no irregularities	[0, ...]	==	0	Integer	1	VirtualMachine	malwareProtection.numberOfThreatsFound
3	OPS-07.2H	DATA BACKUP AND RECOVERY – MONITORING	EUCS	BackupEnabled	This metric is used to assess if backups are enabled for a cloud service/asset	[true, false]	==	true	Boolean	1	Storage	backup.enabled
4	OPS-07.2H	DATA BACKUP AND RECOVERY – MONITORING	EUCS	BackupRetentionSet	This metric is used to assess the configured backup retention (days) on a cloud service/asset	[0, ...]	>	35	Integer	24	Storage	backup.retentionPeriod
5	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	AnomalyDetectionEnabled	This metric is used to assess if Anomaly Detection is enabled for the cloud service/asset	[true, false]	==	true	Boolean	1	NetworkService	anomalyDetection.enabled
6	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	ActivityLoggingEnabled	This metric is used to assess if activity logs are enabled for the cloud service/asset.	[true, false]	==	true	Boolean	1	VirtualMachine	activityLogging.enabled
7	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	ApplicationLoggingEnabled	This metric is used to assess if Application logs are enabled for the cloud service/asset.	[true, false]	==	true	Boolean	1	VirtualMachine	applicationLogging.enabled
8	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	BootLoggingEnabled	This metric is used to assess if Boot logs are enabled for the cloud service/asset.	[true, false]	==	true	Boolean	1	VirtualMachine	bootLogging.enabled
9	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	OSLoggingEnabled	This metric is used to assess if OS logs are enabled for the cloud service/asset.	[true, false]	==	true	Boolean	1	VirtualMachine	oSLogging.enabled
10	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	BootLoggingRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0, ..., 99]	>	7	Integer	1	VirtualMachine	bootLogging.retentionPeriod
11	OPS-13.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	OSLoggingRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0, ..., 99]	>	7	Integer	1	VirtualMachine	oSLogging.retentionPeriod
12	OPS-18.6H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	EUCS	AutomaticUpdatesEnabled	This metric is used to assess if automatic updates are enabled for the cloud service/asset	[true, false]	==	true	Boolean	24	VirtualMachine	automaticUpdates.enabled
13	OPS-18.6H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	EUCS	AutomaticUpdatesInterval	This metric is used to assess the update interval of automatic updates for the cloud service/asset	[1, ..., 365]	<=	7	Integer	24	VirtualMachine	automaticUpdates.interval
14	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	TLSVersion	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks	[1.0, 1.1, 1.2, 1.3]	>	1.2	String	1	NetworkService	transportEncryption.tlsVersion
15	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	WebApplicationFirewallEnabled	This metric is used to assess if a cloud service/asset has enabled WAF functionalities	[true, false]	==	true	Boolean	1	LoadBalancer	accessRestrictions.webApplicationFirewall.enabled
16	CKM-02.1B	ENCYPTION OF DATA IN TRANSIT	EUCS	TransportEncryptionEnabled	This metric is used to assess if the cloud service/asset accepts encrypted connections	[true, false]	==	true	Boolean	1	StorageService	httpEndpoint.transportEncryption.enabled

17	CKM-02.1S	ENCYPTION OF DATA IN TRANSIT	EUCS	TransportEncryptionEnforced	This metric is used to assess if the cloud service/asset enforces encrypted connections	[true, false]	==	true	Boolean	1	StorageService	httpEndpoint.transportEncryption.enforced
18	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	L3FirewallEnabled	This metric is used to assess if a service-level ACL has been enabled on a cloud service/asset	[true, false]	==	true	Boolean	1	StorageService	l3Firewall.enabled
19	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	JavaVersion	This metric is used to assess the Java Runtime version used by the cloud service/asset	[< 11, 11]	==	11	String	24	Function	
20	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	PHPVersion	This metric is used to assess the PHP version used by the cloud service/asset	[< 7.4, 7.4]	==	7.4	String	24	Function	
21	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	PythonVersion	This metric is used to assess the Python version used by the cloud service/asset	[< 3.8, 3.8]	==	3.8	String	#	Function	
22	OPS-05.3H	PROTECTION AGAINST MALWARE – IMPLEMENTATION	EUCS	MalwareProtectionOutput	This metric states whether automatic notifications are enabled (e.g. e-mail) about malware threats. This relates to EUCS' definition of "continuous monitoring"	[true, false]	==	true	Boolean	1	VirtualMachine	malwareProtection.applicationLogging.loggingService
23	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	AtRestEncryptionEnabled	This metric is used to assess if encryption at rest has been enabled on a cloud service / asset	[true, false]	==	true	Boolean	1	Storage	atRestEncryption.enabled
24	OPS-21.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	BackupEncryptionEnabled	Check if data is backed up in encrypted, state-of-the-art form	[true, false]	==	true	Boolean	1	Storage	atRestEncryption.enabled
25	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	TlsCipherSuites	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks	(*)	<=	(*)	ArrayOfString		Application	
26	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	TlsDHGroups	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks	(**)	<=	(**)	ArrayOfString		Application	
27	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	TlsSignatureAlgorithms	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks	(***)	<=	(***)	ArrayOfString		Application	
28	IAM-03.1H	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	EUCS	DeactivateInactiveUsers	This metric is used to assess if inactive user accounts are deactivated within a reasonable time frame	[0, …]	<=	90	Integer	#	Identity	
29	OPS-13.1H	LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION	EUCS	BootLoggingImmutability		[true, false]	==	true	Boolean	1	StorageService	loggingService.Storage.Immutability.enabled
30	OIS-02.4H	SEGREGATION OF DUTIES	EUCS	MixedDuties	This metric is used to assess if permissions are sufficiently separated between users	[0, …, 1]	<=	0.1	Float	#	Identity	
31	CO-03.6H	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	EUCS	SecureCryptographicPrimitives	This metric is used to assess whether an application uses state-of-the-art cryptographic primitives when performing cryptographic operations	[true, false]	==	true	Boolean	1	Application	
32	CCM-04.1H	APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	EUCS	CodeSignoff	This metric is used to assess whether additions to the source code of a cloud service contains a signoff in the Git commit message.	[true, false]	==	true	Boolean	1	Application	
33	CCM-04.1H	APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	EUCS	SignedCommits	This metric is used to assess whether additions to the source code of a cloud service contains a valid signature.	[true, false]	==	true	Boolean	1	Application	

34	IAM-03.6H	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	EUCS	UnsuccesfulLoginAttemptLogged	This metric is used to assess whether an application reports unsuccessful logging attempts	[true, false]	==	true	Boolean	1	Application	

Organizational metrics

#	ReqID	Control	Source	Metric	Description	Keywords	Scale	Op.	Target Value	Value Datatype	Int (h)	Resource Type
35	AM-01.1H	ASSET INVENTORY	EUCS	AssetManagementPolicy01	Which topics are comprised by the defined asset management policy?	Asset management, inventory management, asset, inventory, ownership, decommissioning	n/a	in	[inventory, ownership, decommissioning, none]	String	720	PolicyDocument
36	AM-01.1H	“	EUCS	AssetManagementPolicy02	Which topics are defined for the secure management of physical assets?	Asset management, inventory management, asset, physical assets, disk, server, components, destruction	n/a	in	[procurement, destruction, none]	String	720	PolicyDocument
37	AM-01.1H	“	EUCS	AssetManagementPolicy03	Which asset information is kept in the inventory?	Services, IP address, databases, inventory, assets, VM, application, asset management	n/a	in	[services, IP addresses, databases, VM, application, service plan instances, database instances]	String	720	PolicyDocument
38	AM-01.4H	“		AssetMonitoringQ1	Where are the assets registered and managed?	Inventory, assets, management	n/a	n/a	n/a	String		PolicyDocument
39	BC-01.1B	BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY	EUCS	BusinessContinuityPolicy01	Which external policies are referenced for business continuity?	BCM, business continuity, recovery	n/a	n/a	n/a	n/a		PolicyDocument
40	BC-02.1H	BUSINESS IMPACT ANALYSIS PROCEDURES	EUCS	BusinessContinuityPolicy02	For which risks are defined business continuity plans?	BCM, business continuity, risks, plans	n/a	n/a	n/a	n/a		PolicyDocument
41	BC-03.1H	BUSINESS CONTINUITY AND CONTINGENCY PLANNING	EUCS	BusinessContinuityPolicy03	Which architectural aspects are defined in the business continuity plan?	BCM, business continuity, redundancy, availability, multi-datacenter architecture	n/a	in	[multi-datacenter architecture, other, none]	n/a		PolicyDocument
42	CCM-01.1H	Change and Configuration Management	EUCS	ChangeManagementPolicy01	Which change management policies need to be reviewed by cloud customers?	Change management, SLA	n/a	n/a	n/a	n/a	720	PolicyDocument
43	CKM-01.1H	ENCRYPTION OF DATA IN TRANSIT	EUCS	EncryptionPolicyQ7	What TSL version is accepted?	Encryption mechanisms, protocols, default domains and their TLS-profiles	n/a	in	[TLS 1.1,TLS 1.2,TLS 1.3, tls v1.1 and v1.2, tls version 1.2e]			PolicyDocument
44	CKM-01.1H	ENCRYPTION OF DATA IN TRANSIT	EUCS	EncryptionPolicyQ8	What minimum certificate key length is required?	Encryption mechanisms, certificate	n/a	>=	2048	Integer		PolicyDocument

45	CKM-01.1H	POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT	EUCS	EncryptionPolicyQ4	What minimum key length must the Advanced Encryption Algorithm (AES) standard have?	AES, encryption mechanisms, mobile devices, portable devices	n/a	=	256-bit	String		PolicyDocument
46	CKM-01.1H	“	EUCS	EncryptionPolicyQ5	What Advanced Encryption Algorithm (AES) standard should be used?	AES, encryption mechanisms, mobile devices, portable devices	n/a	=	AES256	String		PolicyDocument
47	CKM-01.1H	“	EUCS	EncryptionPolicyQ9	What hash type is required?	Encryption mechanisms, hash	n/a	in	[SHA256,SHA-384, SHA-512,SHA-512/256]	n/a		PolicyDocument
48	CKM-01.1H	“	EUCS	EncryptionPolicyQ12	Which policy is to be used for browsers?	Encryption mechanisms, security policy, browser, data in transit	n/a	=	HSTS	String		PolicyDocument
49	CKM-01.1H	“	EUCS	EncryptionPolicyCheckQ1	How are passwords or keys encrypted?	Password, cryptography, data at rest protection		in	[MD5, SHA256]	String		PolicyDocument
50	CKM-01.1H	“	EUCS	EncryptionPolicyCheckQ2	How are APIs encrypted?	Encryption, cryptography, data at rest protection		in	[TSL, SSL]	String		PolicyDocument
51	CKM-01.1H	POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT	EUCS	EncryptionPolicyCheckQ3	What encryption type is used?	Encryption, cryptography, data at rest protection		in	[TSL, SSL]	String		PolicyDocument
52	CKM-01.1H	POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT	EUCS	EncryptionPolicyCheckQ4	Which TLS features are defined in the policy?	Encryption, best practice, TLS, secure configuration. Transport layer encryption	n/a	in	[TLS profiles]	String	720	PolicyDocument
53	CKM-01.1H	POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT	EUCS	EncryptionPolicyQ6	How must mobile and portable devices be encrypted?	Encryption mechanisms, mobile devices, portable devices	n/a	in	[password, passcode, Touch-ID, Face-ID]	n/a		PolicyDocument
54	CKM-02.1H	ENCRYPTION OF DATA IN TRANSIT	EUCS	EncryptionPolicyQ11	What type of web services must encrypt data in transit?	Encryption mechanisms, web services , data in transit	n/a	in	[storage of sensitive or confidential information, transaction of sensitive or confidential information, user logons]	n/a		PolicyDocument
55	CKM-02.2H	ENCRYPTION OF DATA IN TRANSIT	EUCS	EncryptionDataTransitPolicyQ1	Which endpoint protection mechanism is defined for data in transit?	Encryption, cryptography, data in transit, protection, PKI, payload, SSL, TLS, transport layer encryption, encrypted endpoints	n/a	in	[encrypted endpoints, none]	String	720	PolicyDocument

56	CKM-02.2H	ENCRYPTION OF DATA IN TRANSIT	EUCS	EncryptionDataTransitPolicyQ2	Which encryption mechanisms are not explicitly supported for data in transit?	Encryption, cryptography, data in transit not supported, TLS – HPKP – HTTP Public Key Pinning	n/a	in	[TLS – HPKP, HPKP, HTTP Public Key Pinning]	String	720	PolicyDocument
57	CKM-03.1H	ENCRYPTION OF DATA AT REST	EUCS	EncryptionDataRestPolicyQ1	Which up-front data encryption mechanism is defined?	Encryption, cryptography, data at rest, protection, PKI, data at rest protection	n/a	in	[PKI, public key infrastructure, none]	String	720	PolicyDocument
58	CKM-04.1H	SECURE KEY MANAGEMENT	EUCS	EncryptionKeyPolicy01	Which encryption key parameters are in the scope of the management policy?	Encryption, key management, key length, standards	n/a	in	[key lengths, cipher suites, CRL checks, none]	String		PolicyDocument
59	CKM-04.1H	“	EUCS	DigitalCertPolicy01	Which verifiable certificated are supported for Certification Authorities?	Digital certificates, PKI, CA, x509, certificate authorities, publicly verifiable	n/a	in	[publicly verifiable certificates]	String	720	PolicyDocument
60	CKM-04.1H	“	EUCS	DigitalCertPolicy02	Which digital certificates are allowed for user facing services?	Digital certificates, PKI, CA, x509, wildcard, user facing certificates	n/a	n/a	n/a	n/a	720	PolicyDocument
61	CKM-04.1H	“	EUCS	DigitalCertPolicy03	What is the validity period of wildcard digital certificates?	Digital certificates, validity period, duration, wildcard, user facing certificates	years	<=	3	Integer	720	PolicyDocument
62	CO-01.1H	IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS	EUCS	CompliancePolicy01	How are compliance policies revised for updates?	Compliance, planning, requirements	n/a	n/a	n/a	n/a		PolicyDocument
63	CO-01.4H	“	EUCS	CompliancePolicy02	Which mechanisms are implemented to periodically monitor compliance requirements?	Audits, reviews, compliance	n/a	in	[audits]	String		PolicyDocument
64	CO-01.4H	“	EUCS	CompliancePolicy03	Which additional certifications are in scope of the compliance requirements?	Certification, compliance, security review and audit, iso 27001	n/a	in	[iso 27001, bsi c5, secnumcloud, fedramp, pci, hippa]	String		PolicyDocument
65	CO-02.1H	POLICY FOR PLANNING AND CONDUCTING AUDITS	EUCS	CompliancePolicy04	Which customer-side security checks are defined?	Audit right, customer, penetration testing by customers	n/a	in	[penetration tests, audits, none]	String		PolicyDocument
66	CO-03.5H		EUCS	ComplianceQ2	How is the internal compliance procedure defined?	Compliance, monitoring, vulnerabilities, report, expert, assessment	n/a	n/a	n/a	String		PolicyDocument
67	CO-03.6H		EUCS	ComplianceQ1	How are vulnerabilities monitored and reported?	Compliance, monitoring, vulnerabilities, report, expert, assessment	n/a	n/a	n/a	String		PolicyDocument

68	CS-01.1H	TECHNICAL SAFEGUARDS	EUCS	NetworkSecurityPolicy01	Which network-level attacks are mitigated by the implemented mechanisms?	Network security, DoS, DdoS, proxy, IDS, Denial of service protection	n/a	in	[dos, denial of service]	Integer	720	PolicyDocument
69	CS-02.1H	SECURITY REQUIREMENTS TO CONNECT WITHIN THE CSP'S NETWORK	EUCS	NetworkAccessPolicy01	Which security mechanism protects access to administrative networks?	VPN, network access, virtual private network, RAS, segmentation	n/a	n/a	n/a	n/a	720	PolicyDocument
70	CS-03.1H	MONITORING OF CONNECTIONS WITHIN THE CSP'S NETWORK	EUCS	TrustedNetworkPolicy01	Which process exists for determining the trustworthiness of network connections?	Whitelisting, trusted networks, filtering	n/a	n/a	n/a	n/a	720	PolicyDocument
71	CS-05.1H	TRAFFIC SEGREGATION IN SHARED NETWORK ENVIRONMENTS	EUCS	TrafficSegregationPolicy01	Which traffic segregation policy is defined?	Network, security layer, micro segmentation	n/a	n/a	n/a	n/a	720	PolicyDocument
72	DOC-01.1H	GUIDELINES AND RECOMMENDATIONS FOR CLOUD CUSTOMERS	EUCS	RecommendationCustomer01	Which aspects are covered in the security recommendations for customers?	Guidelines, best practices, cloud customer, references to secure coding guidelines	n/a	in	[secure devops, secdevops, devopssec, security controls in the development life-cycle]	String		PolicyDocument
73	DOC-01.1H	“	EUCS	GuidelinesCloudCustomersQ1	Which customer guidelines are defined for password management?	Password, storage, manager, cryptographic, customer, consumer, responsibility, complexity	n/a	n/a	n/a	n/a	720	PolicyDocument
74	DOC-01.1H	“	EUCS	GuidelinesCloudCustomersQ2	Which customer guidelines are defined for identity management?	Identity management, customer, consumer, responsibility, authentication, identity management services	n/a	n/a	n/a	n/a	720	PolicyDocument
75	DOC-01.1H	“	EUCS	GuidelinesCloudCustomersQ3	Which customer guidelines are defined for asset management?	Asset management, customer, consumer, responsibility, inventory, software license, asset management	n/a	n/a	n/a	n/a	720	PolicyDocument
76	DOC-02.1H	LOCATIONS OF DATA PROCESSING AND STORAGE	EUCS	DataLocationPolicy01	Which data location regions are defined for compliance?	Data location, compliance, geographical	n/a	n/a	n/a	n/a		PolicyDocument
77	HR-03.4H		EUCS	InformationSecurityPolicyAcknowledgementQ1	Which system monitors the acknowledgement of the information security policy?	Information security policy, acknowledge, employee	n/a	n/a	n/a	String		PolicyDocument
78	HR-05.2H		EUCS	AccessRightManagementQ1	Which system monitors the access rights?	Access rights, account management	n/a	n/a	n/a	String		PolicyDocument
79	HR-06.5H		EUCS	NDAQ1	How are non-disclosure agreements monitored?	NDA, non-disclosure, agreement,	n/a	n/a	n/a	String		PolicyDocument

80	IAM-01.1H	POLICIES FOR ACCESS CONTROL TO INFORMATION	EUCS	PoliciesForAccessControlQ1	Which processes are documented for users with privileged access?	Authorization, access, privilege, PAM, IAM, IdM, management	n/a	n/a	n/a	n/a	720	PolicyDocument
81	IAM-01.1H	POLICIES FOR ACCESS CONTROL TO INFORMATION	EUCS	PoliciesForAccessControlQ2	Which regulation mandates the management of access rights?	Authorization, access, directive, regulation, IAM, IdM, access control, secure credentials management	n/a	n/a	n/a	n/a	720	PolicyDocument
82	IAM-03.2H	PROTECTION AND STRENGTH OF CREDENTIALS	EUCS	PasswordLoginAttemptsQ1	How many consecutive login attempts are allowed?	Password	n/a	<=	50	Integer		PolicyDocument
83	IAM-03.5H	“	EUCS	PasswordLoginBlockDurationQ1	How long is an account blocked after failed logins?	Login, block, lock, management, password, authentication, access	n/a	>=	1	Integer		PolicyDocument
84	IAM-08.1H	“	EUCS	PasswordPolicyQ1	Which parameters define the password policy?	Password, complexity, rotation, entropy, renewal, credentials	n/a	n/a	n/a	n/a	720	PolicyDocument
85	IAM-08.1H	“	EUCS	PasswordPolicyQ2	What is the passwords maximum age according to the password policy?	Password, age, maximum	days	<=	90	Integer	720	PolicyDocument
86	IAM-08.1H	“	EUCS	PasswordPolicyQ3	What is the passwords rotation frequency?	Password, rotation, renewal	n/a	<=	4	Integer	720	PolicyDocument
87	IAM-08.1H	“	EUCS	PasswordPolicyQ4	Which requirements exist for password managers?	Password, storage, manager, cryptographic, password policy	n/a	n/a	n/a	n/a	720	PolicyDocument
88	IAM-08.1H	“	EUCS	PasswordLengthQ1	How long should passwords be?	Password	characters	>=	5	Integer		PolicyDocument
89	IAM-08.1H	“	EUCS	PasswordReuseQ1	What measures are taken to prohibit password reuse?	Password	n/a	n/a	n/a	n/a		PolicyDocument
90	IM-01.2H	POLICY FOR SECURITY INCIDENT MANAGEMENT	EUCS	IncidentManagementPolicy01	Which team is in charge of handling security incidents?	Incident Management, CERT	n/a	in	[CERT]	String		PolicyDocument
91	IM-02.1H	PROCESSING OF SECURITY INCIDENTS	EUCS	IncidentManagementPolicy09	How are sources of information considered for identifying incidents?	Incident identification, sources, security-relevant	n/a	in	[multi-phase, internal, external]	String		PolicyDocument
92	IM-02.1H	PROCESSING OF SECURITY INCIDENTS	EUCS	IncidentManagementPolicy10	Which process is in place to analyse a potential incident?	Incident management, triage, analysis	n/a	in	[triage, other, none]	n/a		PolicyDocument
93	IM-02.4H	POLICY FOR SECURITY INCIDENT MANAGEMENT	EUCS	IncidentManagementPolicy8	How often must the Incident Management plan be tested?	Incident Management, CERT	year	<=	1	Integer		PolicyDocument

94	IM-04.1H	USER'S DUTY TO REPORT SECURITY INCIDENTS	EUCS	IncidentManagementPolicy6	When must staff report potential security and privacy issues?	Incident Management, Incident Management general information	n/a	=	immediately	String		PolicyDocument
95	IM-04.3H	“	EUCS	IncidentManagementPolicy5	To whom must staff report potential security and privacy issues?	Incident Management, Incident Management general information	n/a	in	[CERT, single point of contact]	n/a		PolicyDocument
96	IM-04.3H	“	EUCS	IncidentManagementPolicy02	Which approach is used for reporting incidents to the CSP?	Single Point of Contact, Single Point of Information (SpoI)	n/a	in	[Single Point of Contact, Single Point of Information]	String		PolicyDocument
97	IM-05.1H	INVOLVEMENT OF CLOUD CUSTOMERS IN THE EVENT OF INCIDENTS	EUCS	IncidentManagementPolicy11	How is guaranteed the user involvement for incident management?	Customer involvement, incident management, customer cooperation	n/a	n/a	n/a	n/a		PolicyDocument
98	IM-05.2H	“	EUCS	IncidentManagementPolicy12	When are users notified of relevant incidents?	Customer, notifications, incident	n/a	=	timely	String		PolicyDocument
99	IM-07.1H	INCIDENT EVIDENCE PRESERVATION	EUCS	IncidentManagementPolicy03	Which entity maintains the evidence related to cyberincidents?	CSP, customer, shared, evidence collection	n/a	in	[CSP, customer, shared responsibility]	String		PolicyDocument
100	IM-07.4H	INCIDENT EVIDENCE PRESERVATION	EUCS	IncidentManagementPolicy13	Which entity coordinates the forensic investigation?	Forensic, incident management	n/a	in	[CERT]	String		PolicyDocument
101	ISP-02.1H	Security Policies and Procedures	EUCS	RoleDefinitionQ1	Which roles and responsibilities are defined by the security policy?	Roles, stakeholders, provider, consumer, costumer, shared responsibility model, stakeholders and roles	n/a	n/a	n/a	n/a	720	PolicyDocument
102	ISP-02.1H	Security Policies and Procedures	EUCS	RoleDefinitionQ2	Which responsibilities are defined for the Cloud Platform Provider?	Roles, platform, hyperscaler, stakeholders and roles, cloud platform provider	n/a	n/a	n/a	n/a	720	PolicyDocument
103	ISP-02.1H	Security Policies and Procedures	EUCS	RoleDefinitionQ3	Which responsibilities are defined for the Cloud Service Provider?	Roles, provider, CSP, stakeholders and roles, cloud service provider	n/a	n/a	n/a	n/a	720	PolicyDocument
104	ISP-02.1H	Security Policies and Procedures	EUCS	RoleDefinitionQ4	Which responsibilities are defined for the Cloud Service Consumer?	Roles, consumer, customer, CSC, stakeholders and roles, cloud (service) consumer / customer	n/a	n/a	n/a	n/a	720	PolicyDocument
105	OPS-02.2H	CAPACITY MANAGEMENT – MONITORING	EUCS	ProvisioningPolicyCheckQ1	How is the provisioning of cloud services handled?	Cloud service documentation	n/a	n/a	n/a	n/a		PolicyDocument
106	OPS-02.2H	CAPACITY MANAGEMENT – MONITORING	EUCS	ProvisioningPolicyCheckQ2	How is the provisioning documented?	Cloud service documentation	n/a	n/a	n/a	n/a		PolicyDocument
107	OPS-04.1H	PROTECTION AGAINST MALWARE – POLICIES	EUCS	MalwareProtectionCheckQ1	Which core CSP services are covered by malware protection?	Malware, protection, antivirus, documentation	n/a	n/a	n/a	n/a	720	PolicyDocument
108	OPS-04.1H	PROTECTION AGAINST MALWARE – POLICIES	EUCS	MalwareProtectionCheckQ2	How are malware-related events stored?	Malware, protection, antivirus, logs, management, central, malware protection	n/a	in	[centrally, descentral, distributed, central]	String	720	PolicyDocument

109	OPS-04.1H	PROTECTION AGAINST MALWARE – POLICIES	EUCS	MalwareProtectionCheckQ4	Which malware-related events are communicated to the customer?	Malware, protection, antivirus, logs, management, malware events, customer, consumer	n/a	n/a	n/a	n/a	720	PolicyDocument
110	OPS-05.3H	PROTECTION AGAINST MALWARE – IMPLEMENTATION	EUCS	MalwareProtectionCheckQ3	What antivirus system is used?	Malware, protection, antivirus, documentation, malware protection	n/a	n/a	n/a	n/a		PolicyDocument
111	OPS-05.3H	PROTECTION AGAINST MALWARE – IMPLEMENTATION	EUCS	AntimalwareScanFrequencyQ1	How frequent are antimalware scans done?	Antimalware, scans, irregularities	days	<=	10	Float		PolicyDocument
112	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	SystemBackUpPolicyQ01	Which algorithm is used to encrypt the backup data?	Backup, encryption	n/a	n/a	n/a	n/a		PolicyDocument
113	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	SystemBackUpPolicyQ02	Who is allowed to access the backed-up data?	Backup, access	n/a	n/a	n/a	n/a		PolicyDocument
114	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	SystemBackUpPolicyQ03	Who is allowed to restore backups?	Backup, access, restore	n/a	=	administrative users	String		PolicyDocument
115	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	SystemBackUpPolicyQ05	How often are backups made?	Backup, schedule	days	=	1	Integer		PolicyDocument
116	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	BackupPolicyQ1	Which backup procedures apply to CSP systems	backup, restore, automation, periodical	n/a	n/a	n/a	n/a	720	PolicyDocument
117	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	BackupPolicyQ2	How is managed the backup service?	Backup, centralized	n/a	n/a	n/a	n/a	720	PolicyDocument
118	OPS-06.1H	DATA BACKUP AND RECOVERY – POLICIES	EUCS	BackupPolicyQ3	Are there backup services for cloud customers?	Backup, customer, consumer, backup and restore process	n/a	in	[no, yes]	String	720	PolicyDocument
119	OPS-07.1H	DATA BACKUP AND RECOVERY – MONITORING	EUCS	SystemBackUpMonitoringQ01	What is the automatic backup procedure?	Backup, procedure	n/a	n/a	n/a	n/a		PolicyDocument
120	OPS-07.2H	DATA BACKUP AND RECOVERY – MONITORING	EUCS	BackupMonitoringPolicyCheckQ1	What measures are used to monitor the execution of data backups?	Backup	n/a	n/a	n/a	n/a		PolicyDocument
121	OPS-08.1H	DATA BACKUP AND RECOVERY – REGULAR TESTING	EUCS	DataRestoreTestFrequencyQ1	How frequently is the data restoring process tested?	Data, restore	days	<=	100	Float		PolicyDocument
122	OPS-08.1H	DATA BACKUP AND RECOVERY – REGULAR TESTING	EUCS	SystemBackUpTesting01	How often is the procedure checked?	Backup, restore procedure	n/a	=	annually	String		PolicyDocument
123	OPS-08.3H	DATA BACKUP AND RECOVERY – REGULAR TESTING	EUCS	SystemBackUpTesting02	How are restore mistakes dealt with?	Backup, monitoring	n/a	=	by the administrator	String		PolicyDocument
124	OPS-09.1H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	SystemBackUpStorage01	Where are backups stored?	Backup, storage	n/a	=	second SSD disk	String		PolicyDocument
125	OPS-09.2H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	BackupMonitoringPolicyCheckQ2	How is backup data transmitted?	Backup, data, transmission	n/a	n/a	n/a	n/a		PolicyDocument
126	OPS-09.2H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	BackupMonitoringPolicyCheckQ3	How is the transmission of backup data verified?	Backup, data, transmission	n/a	n/a	n/a	n/a		PolicyDocument
127	OPS-09.2H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	BackupMonitoringPolicyCheckQ4	How often is the transmission of backups done?	Backup, data, transmission	days	<=	1	Float		PolicyDocument
128	OPS-09.2H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	BackupMonitoringPolicyCheckQ5	How are backup transmissions documented?	Backup, data, transmission, backup and restore process	n/a	n/a	n/a	n/a		PolicyDocument

129	OPS-09.2H	DATA BACKUP AND RECOVERY – STORAGE	EUCS	SystemBackUpStorage03	How is the storage process monitored?	Backup, storage	n/a	=	manually by the admin	String		PolicyDocument
130	OPS-10.1H	LOGGING AND MONITORING – POLICIES	EUCS	LoggingMonitoringPolicyQ1	Which security monitoring data is continuously assessed?	Logging, monitoring, policy	n/a	n/a	n/a	n/a	720	PolicyDocument
131	OPS-10.1H	LOGGING AND MONITORING – POLICIES	EUCS	LoggingMonitoringPolicyQ2	In which type of facility are security event logged?	Logging, monitoring, policy, monitoring and logging	n/a	in	[central logging facility, descentralized logging facility]	String	720	PolicyDocument
132	OPS-10.1H	LOGGING AND MONITORING – DERIVED DATA MANAGEMENT	EUCS	LoggingMonitoringDerivedPolicyQ1	Are security events stored for derived data?	Logging, monitoring, policy, derived data, customer data, PII, monitoring and logging	n/a	in	[yes, no, does not]	String	720	PolicyDocument
133	OPS-12.1H	LOGGING AND MONITORING – IDENTIFICATION OF EVENTS	EUCS	EventMonitoringPolicyCheckQ1	Which functional events are monitored by the SIEM?	Logging, monitoring, metrics, events, availability, performance	n/a	in	[availability, performance, all, none]	String	720	PolicyDocument
134	OPS-12.1H	“	EUCS	EventMonitoringPolicyCheckQ2	In which type of facility are SIEM events stored?	Logging, monitoring, SIEM, central, Security Information and Event Management	n/a	in	[centrally, descentral, distributed, central]	String	720	PolicyDocument
135	OPS-12.1H	“	EUCS	EventMonitoringPolicyCheckQ3	Which actions are taken with detected security events?	Logging, monitoring, SIEM, CERT, incident, forensic	n/a	n/a	n/a	n/a	720	PolicyDocument
136	OPS-13.3H	LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION	EUCS	LogDataRetentionTimeQ1	How long is log data stored?	Logging, retention	days	<=	100	Float		PolicyDocument
137	OPS-13.3H	“	EUCS	LogDataRetentionTimeQ2	When is log data deleted?	Logging, deletion	days	<=	100	Float		PolicyDocument
138	OPS-17.1B	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS OF PROCEDURES	EUCS	IncidentPolicyCheckQ1	How are vulnerabilities managed by the corresponding team?	Incident, vulnerability management, central, technical vulnerability management	n/a	in	[centrally, descentral, distributed, central]	String		PolicyDocument
139	OPS-17.1B	“	EUCS	IncidentAnalysisFrequencyQ1	How often are procedures for vulnerabilities and incidents analysed?	Incident, vulnerability, frequency	months	<=	30	Float		PolicyDocument
140	OPS-17.1B	“	EUCS	VulnerabilityScanQ1	Which is the coverage of defined web vulnerability scans?	Whitelisted, all, URLs, none	n/a	n/a	n/a	n/a	720	PolicyDocument
141	OPS-18.6H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS	EUCS	PatchManagementPolicyCheckQ1	Which subsystems are covered by the patch management process?	Partial, full, every, none, patch management	n/a	in	[every, none, partial]	String	720	PolicyDocument
142	OPS-18.6H	“	EUCS	PatchManagementPolicyCheckQ2	Which vulnerabilities are prioritized for systems that cannot be patched?	None, critical, all, “no-patch”-approach	n/a	in	[critical, none, all, medium, severe]	String	720	PolicyDocument
143	OPS-18.6H	“	EUCS	UpdatePolicyCheckQ1	Which update mechanisms are there?	Update, patch	n/a	n/a	n/a	n/a		PolicyDocument

144	OPS-18.6H	“	EUCS	UpdatePolicyCheckQ2	How are systems and patches updated?	Update, patch, patch management	n/a	n/a	n/a	n/a		PolicyDocument
145	OPS-19.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION	EUCS	VulnerabilityManagementPolicyQ1	How does vulnerability information is gathered and forwarded?	Vulnerability management, manual, automated, semi-automated, technical vulnerability management	n/a	in	[automated, manual, semi-automated]	String	720	PolicyDocument
146	OPS-19.1H	“	EUCS	VulnerabilityManagementPolicyQ2	Which sources of information are used for web vulnerability scans?	Vulnerability management, policy, CERT, PSIRT, security advisories, third party, OWASP, web vulnerability scanning, vulnerability scans	n/a	in	[OWASP-Top-Ten, OWASP-Top10, other, none]	String	720	PolicyDocument
147	OPS-21.1H	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	EUCS	SystemHardeningPolicyQ1	Which sources shall we used to guarantee the hardening of software?	Hardening, operating system, server, component, trusted sources	n/a	n/a	n/a	n/a	720	PolicyDocument
148	OPS-21.1H	“	EUCS	SystemHardeningPolicyQ2	Which systems are covered by the system hardening?	Hardening, scan, coverage, full, partial	n/a	n/a	n/a	n/a	720	PolicyDocument
149	OPS-21.1H	“	EUCS	SystemHardeningPolicyQ3	What is the penetration test frequency?	Annual, monthly, quarterly, hardening verification, server hardening, server and component hardening	n/a	in	[yearly, annual, periodic, monthly, quarterly]	String	720	PolicyDocument
150	PI-01.2B	DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES	EUCS	IOInterfacesPolicy01	Which functionalities are defined for output interfaces?	Customer data, capabilities, base services	n/a	in	[secure data export, none]	n/a		PolicyDocument
151	PM-04.7H		EUCS	ProcurementManagementQ1	How is the availability of system components documented?	Monitoring, configuration, availability, component	n/a	n/a	n/a	String		PolicyDocument
152	PS-02.8H		EUCS	AccessControlQ1	Where is access control monitored and regulated?	Access control	n/a	n/a	n/a	String		PolicyDocument

Appendix 3: Extended mapping of security controls

This appendix provides an extended mapping of the controls related to "the 34 requirements" using the MEDINA mapping and the Cisco CCF [19]. In the table, the mapping made in MEDINA is coloured in orange, and the mapping extracted from Cisco CCF correspond to the white cells. Due to space constraints, standards mapped by Cisco CCF are identified by a number. See coding at the end of the table.

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
OIS-02	OIS-04	6.1 6.2	5.3	CLD.6.3.1	CCF 91	CC1.3, CC2.2, CC3.1, CC3.2, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2				Clause 4.3, Clause 5.1(c), Clause 5.2, Clause 5.3, Clause 6.1.1, Clause 7.5.1, Clause 7.5.2	A.6.1.1, A.18.2.1, A.18.2.2, A.18.2.3		CLD.6.3.1					OIS-01, OIS-03, OIS-04, SP-03	CM-4, MA-5, PL-1, PS-1, SA-3, SA-5, SC-1, SI-1	org.1, org.3, mp.info.2			6.1.1, 18.2.1, 18.2.2, 18.2.3, 3.1.2.1, 3.1.2.3, 3.1.3.1, 3.1.3.2, 3.1.3.3, 3.1.3.4, 3.1.5.4, 3.1.5.5, 3.1.6.1, 3.1.6.2, 4.4.1.1, 4.4.1.2, 4.4.1.3, 4.4.4.1, 4.4.5.1, 4.4.5.3, 4.4.6.1, 4.5.1.1, 4.5.1.2 4.5.2.2 4.5.2.7 4.5.3.1 4.6.1.2 4.6.2.1 4.8.1.1 4.8.2.1	1.1.5.a, 1.1.5.b, 12.4.a, 12.4.b, 12.5, 12.5.1, 12.5.2, 12.5.2, 12.5.4, 12.10.3, 12.10.4	1-1-P-1-1, 1-1-T-1-1, 1-4-1, 1-5-2, 1-9-3-1, 1-9-4-2, 1-1-1, 1-2-1, 1-2-2, 1-2-3 , 1-3-2, 1-4-2, 1-9-1, 1-9-2	6.2.B	X	X	X	X	39
ISP-03	SP-03				CCF 108													SP-03		org.1, org.2			4.4.5.3, 4.9.1.1, 3.1.4.2	1.1.6.a, 1.1.6.b, 1.1.6.c							
HR-03	HR-02	**7.2**	6.2		CCF 120	CC1.1, CC1.5, CC2.2					A.7.1.2, A.7.2.1, A.8.1.3, A.11.2.8, A.16.1.2, A.18.1.2							HR-02, HR-05, AM-02, AM-03, AM-05, SIM-04	PL-4, PS-6	org.2, op.exp.2, mp.per.2	mp.per.1	mp.per.1	7.1.2, 7.2.1, 8.1.3, 8.1.3.2, 9.4.2.1, 11.2.8, 18.1.2, 4.5.2.1	12.3, 12.3.1, 12.3.5, 12.3.6	1-4-P-1-3, 1-4-T-1-1, 1-3-1	5.12.A, 6.2.C, 6.2.D, 6.2.E, 6.2.J, 6.2.O	X	X	X	X	1625, 0435, 0258, 0820, 1146, 0821, 0824
HR-04	HR-03		6.3		CCF 123	CC6.7					A.6.2.1, A.6.2.2, A.9.2.4								AC-19, MP-7	org.4, mp.eq.3, mp.s.1			6.2.1, 9.1.2, 9.2.4		2-5-P-1-1, 2-5-P-1-2, 2-6-3-1, 2-6-3-2, 2-6-3-4, 1-10-3-2, 2-5-1, 2-5-2, 2-6-1, 2-6-2, 2-6-4, 5-1-2, 5-1-3-6	6.2.B, 6.2.F	X	X	X	X	1533, 1195, 1085, 0863, 0864, 1365, 1366, 0874, 1082, 1083

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
HR-05	HR-05	**7.5**	6.5		CCF 120 CCF 165	CC1.1, CC1.5, CC2.2					A.7.1.2, A.7.2.1, A.8.1.3, A.11.2.8, A.16.1.2, A.18.1.2 A.8.1.4		CLD.8.1.5					HR-02, HR-05, AM-02, AM-03, AM-05, SIM-04	PL-4, PS-6 PS-4	org.2, op.exp.2, mp.per.2	mp.per.1	mp.per.1	7.1.2, 7.2.1, 8.1.3, 8.1.3.2, 9.4.2.1, 11.2.8, 18.1.2, 4.5.2.1 8.1.4	12.3, 12.3.1, 12.3.5, 12.3.6 12.5.4	1-4-P-1-3, 1-4-T-1-1, 1-3-1 1-4-P-2-1	5.12.A, 6.2.C, 6.2.D, 6.2.E, 6.2.J, 6.2.O	X	X	X	X	1625, 0435, 0258, 0820, 1146, 0821, 0824 430, 1626
HR-06	HR-06		6.2 6.6		CCF 118 CCF 119	CC1.1, CC1.5, CC2.2					A.7.1.2, A.7.2.1, A.8.1.3, A.11.2.8, A.13.2.4, A.14.2.7, A.15.1.2, A.15.1.3, A.16.1.2, A.18.1.1, A.18.1.2							HR-02, HR-05, HR-06, DEV-02, SSO-01, SIM-04	PL-4, PS-6, PS-7, SA-9	org.1, org.2, mp.per.2	op.ext.1, mp.per.1	op.ext.1, mp.per.1	7.1.1.11, 7.1.2, 7.2.1, 7.3.1, 8.1.3.1, 13.2.4, 14.2.7, 15.1.2, 15.1.3, 18.1.2	12.3, 12.3.1, 12.3.5	1-4-P-1-3, 1-4-T-1-1, 1-9-3-1, 2-1-3, 2-1-4, 1-9-1, 1-9-2	5.12.A, 5.12.B, 5.12.D, 6.2.C, 6.2.D, 6.2.E, 6.2.G, 6.2.J, 6.2.L, 6.2.M, 6.2.N, 6.2.O, 6.2.Q	X	X	X	X	1625, 1631, 0435, 0264
AM-01	AM-01	8.1.1. 8.1.2	5.9		CCF 52	CC6.1, CC6.5					A.8.1.1, A.8.1.2, A.8.2.1, A.8.2.2							AM-01, OPS-10	CM-8	op.pl.1, op.pl.2, op.exp.1, mp.if.7, mp.eq.3, mp.si.1, mp.info.2			8.1.1, 8.1.2, 8.2.1, 8.2.2	1.1.2.a, 1.1.2.b, 1.1.3, 1.1.4.a, 1.1.4.b, 1.1.4.c, 2.4.a, 2.4.b, 9.6.1, 9.7, 9.7.1, 9.9, 9.9.1.a, 9.9.1.b, 9.9.1.c, 12.3.3, 12.3.4	2-1-P-1-1, 2-5-P-1-1, 2-1-T-1-1, 1-9-5, 2-1-1	6.2.D	X	X	X	X	0336, 0159, 1543, 1493, 1243, 1301
AM-03	AM-03 AM-04	8.1.4	7.10		CCF 48	CC6.4, CC6.5	A1.2				A.5.1.1, A.5.1.2, A.6.2.2, A.8.1.2, A.8.1.4, A.8.2.3, A.8.3.2, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.13.2.1, A.13.2.3							SP-01, AM-02, AM-03, AM-04, AM-05, PI-03	MA-2, MA-4, MP-6	org.2, org.4, op.pl.1, op.pl.2, op.exp.4, mp.if.7, mp.si.5, mp.info.2, mp.s.1	op.ext.2	op.ext.2	5.1.1, 5.1.2, 6.2.2, 8.2.3, 11.2.5, 11.2.6, 11.2.7, 11.2.7.4.PB, 11.2.8, 13.2.1, 13.2.3, 4.5.4.5		2-2-P-1-10, 2-5-P-1-3, 2-5-P-1-4, 2-13-P-1-3, 2-17-P-3-1, 2-5-T-1-1, 2-6-T-1, 2-6-3-3, 2-14-3-4, 1-3-3, 1-3-4, 2-3-1, 2-3-4	5.14.F, 6.2.A, 6.2.B, 6.2.D, 6.2.E, 6.2.G, 6.2.J, 6.2.L, 6.2.Q	X	X	X	X	0310, 0944, 0305, 0307, 1600, 1642
AM-04	AM-05		5.11 5.12	CLD 8.1.5	CCF 48	CC6.4, CC6.5	A1.2				A.5.1.1, A.5.1.2, A.6.2.2, A.8.1.2, A.8.1.4, A.8.2.3, A.8.3.2, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.13.2.1, A.13.2.3							SP-01, AM-02, AM-03, AM-04, AM-05, PI-03	MA-2, MA-4, MP-6	org.2, org.4, op.pl.1, op.pl.2, op.exp.4, mp.if.7, mp.si.5, mp.info.2, mp.s.1	op.ext.2	op.ext.2	5.1.1, 5.1.2, 6.2.2, 8.2.3, 11.2.5, 11.2.6, 11.2.7, 11.2.7.4.PB, 11.2.8, 13.2.1, 13.2.3, 4.5.4.5		2-2-P-1-10, 2-5-P-1-3, 2-5-P-1-4, 2-13-P-1-3, 2-17-P-3-1, 2-5-T-1-1, 2-6-T-1, 2-6-3-3, 2-14-3-4, 1-3-3, 1-3-4, 2-3-1, 2-3-4	5.14.F, 6.2.A, 6.2.B, 6.2.D, 6.2.E, 6.2.G, 6.2.J, 6.2.L, 6.2.Q	X	X	X	X	0310, 0944, 0305, 0307, 1600, 1642

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
PS-02	PS-03 PS-04	**11.2**	5.1 5.15 7.2		CCF 35	CC6.1, CC6.4, CC6.5					A6.2.2, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6, A.13.1.1, A.13.1.2							PS-01, PS-03, PS-04, PS-06	MA-5, MP-2, PE-1, PE-2, PE-3, PE-6, PE-16	org.4, op.pl.2, mp.if.1, mp.if.2, mp.eq.3, mp.si.3	op.mon.1	op.mon.1	6.2.2, 11.1.1, 11.1.2, 11.1.3, 11.1.5, 11.1.6, 13.1.1, 13.1.2	9.1, 9.1.1.a, 9.1.1.b, 9.1.1.c, 9.5	2-13-P-1-1, 2-14-3-1, 2-14-3-2, 2-14-3-3, 2-14-3-5, 2-14-1, 2-14-2, 2-3-2, 2-12-1, 2-12-2, 2-14-1, 2-14-2	6.2.B, 6.2.J, 6.2.L, 6.2.Q	X	X	X	X	1053, 0813, 1074, 0164, 1530, 1296, 1626, 0810
OPS-02	OPS-02		8.6		CCF 254	CC3.2	A1.1				A6.1.5, A.12.1.3, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1							PS-02, PS-06, OPS-01, OPS-02, OPS-03, OPS-09, OPS-17	CP-1, CP-2, CP-4, CP-10		op.ext.2, op.cont.1	op.ext.2, op.cont.1	12.1.3, 12.1.3.9.PB, 13.1.1.5, 17.1.1, 17.1.2, 17.1.3, 17.2.1			6.2.K	X	X	X	X	1581, 1435
OPS-05	OPS-05	12.4	8.7		CCF 262	CC3.2, CC6.1, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4					A.12.2.1, A.12.4.1							OPS-04, OPS-05, DEV-10, PSS-02	CA-2, CA-7, RA-5, SI-2, SI-3	op.acc.6, op.exp.6, mp.s.1			12.2.1, 13.2.1.2, 14.1.2, 14.1.3, 14.2.6, 18.1.3	5.1, 5.1.1, 5.1.2, 5.2.a, 5.2.b, 5.2.c, 5.2.d, 5.3.a, 5.3.b, 5.3.c	2-14-P-1-1, 2-16-P-3-2, 2-3-3-1, 2-5-3-8, 2-4-3-4, 2-3-1, 2-3-2, 2-3-4, 2-4-1, 2-4-2, 2-4-3-4, 5-1-2, 5-1-3-10	6.2.K	X	X	X	X	1417, 0657, 0917, 1390, 1656
OPS-07	OPS-07	12.4	8.13		CCF 18	CC7.4, CC7.5, CC9.1	A1.2, A1.3				A.12.2.1, A.12.3.1, A.17.2.1							OPS-06, OPS-07, OPS-08, PI-02	CP-9, CP-10	mp.info.9	mp.eq.9	op.exp.10, op.ext.9, mp.eq.9	12.3.1, 17.2.1	12.10.1.a, 12.10.1.b	2-9-3-1, 2-15-3-2, 2-9-1, 2-9-2	6.2.K	X	X	X	X	1574, 1511
OPS-09	OPS-09	12.4	8.13 8.14		CCF 19	CC7.4, CC7.5, CC9.1	A1.2, A1.3				A.12.2.1, A.12.3.1, A.17.1.2, A.17.1.3, A.17.2.1							PS-02, OPS-06, OPS-07, OPS-09	CP-9, CP-10	mp.info.9	mp.eq.9, mp.info.9	op.ext.9, mp.eq.9, mp.info.9	12.3.1, 17.1.2, 17.1.3, 17.2.1		2-8-P-1-1, 2-8-P-1-2, 2-9-3-1, 2-9-1, 2-9-2		X	X	X	X	1547, 1511
OPS-12	OPS-13	12.1 12.6	8.16		CCF 109													OPS-11, OPS-12, OPS-16, PSS-04		mp.info.6			16.1.7, 18.1.4		2-6-P-1-3	5.2.G, 5.14.E	X	X	X	X	47
OPS-13	OPS-12 OPS-14	12.1 12.6	8.15		CCF 239	CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1					A6.1.3, A.10.1.1, A.12.4.1, A.12.4.2, A.12.4.3, A.14.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7							OPS-10, OPS-13, OPS-17, OPS-21, PSS-03, PSS-04	AU-2, AU-3, AU-5, AU-6, AU-9, AU-12, CA-1, CA-7, IR-4, IR-5, IR-6, IR-9, SI-4, SI-5	op.exp.8, op.mon.2, mp.per.3, mp.eq.3	op.exp.7, op.exp.9, op.mon.2	op.exp.7, op.exp.9, op.mon.2	6.1.3, 12.4.1, 12.4.2, 12.4.3, 14.1.1, 16.1.4, 16.1.5, 16.1.6, 16.1.7, 3.1.5.4	10.2, 10.2.3, 10.2.4, 10.2.6, 10.5.3, 10.5.4, 10.6, 10.6.1.a, 10.6.1.b, 10.6.2.a, 10.6.2.b, 10.6.3.a, 10.6.3.b, 10.8.a, 10.8.b, 10.8.1.a, 10.8.1.b, 10.9, 12.5.5, 12.10.3, 12.10.6, A1, A1.3, A1.4	2-11-P-1-5, 2-11-P-1-6, 2-11-P-1-7, 2-12-P-1-4, 2-12-P-1-6, 2-12-P-1-8, 2-11-T-1-1, 2-11-T-1-2, 2-12-3-1, 2-12-3-2, 2-13-3-3, 2-12-3-4, 2-13-3-1, 2-13-3-2, 2-13-3-3, 2-12-1, 2-12-2, 2-12-4, 2-13-1, 2-13-2, 5-1-2, 5-1-3-3	6.2.B, 6.2.G, 6.2.K, 6.2.M, 6.2.O	X	X	X	X	0120, 0125, 1213, 1631, 0580, 1405, 1228, 0670, 0123, 0582, 1536, 1537, 0585, 1651, 1652, 1660, 1662, 1677, 1683, 1714, 1715

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
OPS-18	PSS-03				CCF 87	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC5.3, CC9.1				Clause 4.1, Clause 4.2, Clause 4.3, Clause 5.1, Clause 5.2, Clause 6.1.1, Clause 6.1.2, Clause 6.1.3, Clause 6.2, Clause 7.4, Clause 7.5.1, Clause 7.5.2, Clause 8.1, Clause 8.2, Clause 8.3, Clause 9.1, Clause 9.3,	A.6.1.1, A.6.1.4, A.6.1.5, A.12.6.1, A.14.1.1, A.14.1.2, A.15.1.1, A.15.1.2, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3		CLD.12.4.5					OIS-01, OIS-03, OIS-06, OIS-07, SP-03, OPS-18, OPS-20, OPS-22, COS-01, COS-03, PSS-03	CA-2, CA-2 (1), CM-4, PS-2, RA-1	op.pl.1, op.pl.3	op.pl.2, op.cont.1	op.pl.2, op.cont.1	6.1.1, 6.1.1.13.P, 6.1.5, 6.3.1.P, 12.6.1, 14.1.1, 15.1.1, 17.1.1, 17.1.2, 17.1.3, 3.1.2.1, 3.1.2.2, 3.1.2.3, 3.1.3.1, 3.1.4.1, 3.1.4.2, 3.1.4.3, 3.1.4.4, 4.4.1.1, 4.4.2.1, 4.4.3.1, 4.4.4.1, 4.4.5.1, 4.4.5.2, 4.4.6.1, 4.4.7.1, 4.4.7.2, 4.4.7.3, 4.4.7.4, 4.4.8.1, 4.4.8.2, 4.4.8.3, 4.4.8.4,		1-2-P-1-1, 1-2-P-1-3, 1-2-T-1-1, 1-2-T-1-3, 1-5-1, 1-5-2, 1-5-4, 2-1-6, 2-5-3-4, 1-1-2, 1-8-1, 2-5-4, 2-10-1, 2-10-2, 5-1-2, 5-1-3-8	6.2.B, 6.2.K, 6.2.M, 6.2.N, 6.2.O	X	X	X	X	1163, 1563, 1564, 0336, 1238
OPS-21	OPS-23	12.9			CCF 272	CC6.6, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4					A.12.6.1, A.13.1.1							OPS-05, OPS-18, OPS-19, OPS-20, OPS-22, OPS-23, COS-01, COS-02, SSO-01, PSS-02, PSS-03	MA-2, SI-2	op.pl.2, op.acc.7, op.exp.4, mp.com.3	op.exp.3, op.ext.2, mp.sw.2	op.exp.3, op.ext.2, mp.sw.2	9.4.4, 12.5.1.1, 12.5.1.15, 12.6.1, 12.6.1.10	1.2.2.a, 1.2.2.b, 2.2.a, 2.2.b, 2.2.c, 2.2.d, 2.2.2.a, 2.2.2.b, 2.2.3, 2.2.5.a, 2.2.5.b, 2.2.5.c, 6.2.a, 6.2.b	2-3-P-1-1, 2-3-P-1-3, 2-3-P-1-4, 2-3-P-1-5, 2-14-P-1-1, 2-3-3-3, 2-10-3-4, 2-10-3-5, 1-6-2-1, 1-6-2-2, 1-6-3-5, 2-4-1, 2-4-2, 2-4-3-4, 2-5-1, 2-5-2, 2-10-1, 2-10-2, 5-1-2, 5-1-3-8, 5-1-3-9	6.2.K, 6.2.L, 6.2.Q	X	X	X	X	1460, 1605, 1606, 1143, 1643, 0298, 0303, 1498, 1499, 1544, 1467, 1483, 1497, 1500
IAM-03	IDM-03	9.3	5.18		CCF 148									9.2.1				IDM-03	AC-2, AC-3, AC-7	op.acc.5, op.acc.6			9.4.2.9, 9.4.3	8.1.4, 8.1.6.a, 8.1.6.b, 8.1.7, 10.2, 10.2.4, 10.6	2-2-P-1-2, 2-2-P-1-4, 2-2-T-1-3		X	X	X	X	1404, 1403, 0431, 0976
CCM-04	DEV-09		8.31 8.32		CCF 30	CC2.1, CC6.1, CC6.8, CC7.1, CC8.1					A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5, A.12.1.2, A.12.1.4, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6							OIS-04, OPS-16, IDM-06, DEV-01, DEV-03, DEV-09	CM-10, IA-5, SA-3	org.2, op.pl.3, op.acc.2, op.acc.4	op.acc.3, op.exp.5, mp.sw.1	op.acc.3, op.exp.5, mp.sw.1	6.1.2, 9.1.2, 9.2.3, 9.4.4, 9.4.5, 12.1.2, 12.1.5.P, 12.4.1.7, 12.4.3, 12.5.1.18, 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 4.5.4.4	6.4.2, 6.4.6, 11.5.a, 11.5.b, 11.5.1	1-5-P-3-1, 1-5-P-3-2, 2-3-P-1-5, 2-3-P-1-7, 2-16-P-3-1, 2-16-P-3-2	6.2.B, 6.2.F, 6.2.K, 6.2.M	X	X	X	X	1211, 1422, 1255

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
CCM-05	DEV-07	12.2 14.2	8.33		CCF 25	CC2.1, CC6.8, CC7.1, CC8.1				Clause 8.1	A.6.1.2, A.9.4.4, A.9.4.5, A.12.1.2, A.12.4.3, A.12.5.1, A.12.6.2, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9							OIS-04, OPS-16, DEV-01, DEV-02, DEV-03, DEV-06, DEV-07, DEV-08, PSS-02	CM-1, CM-4, CM-6, SI-2	org.4, op.pl.3, mp.sw.2	op.acc.3, op.exp.5, mp.sw.1	op.acc.3, op.exp.5, mp.sw.1	6.1.2, 9.4.4, 9.4.5, 12.1.2, 12.1.5.P, 12.4.3, 12.5.1, 12.5.1.2, 12.6.2, 14.2.1, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 4.5.4.1, 4.5.4.2, 4.5.4.3, 4.5.4.4, 4.5.4.5	1.1.1.a, 1.1.1.b, 1.1.1.c, 6.3.a, 6.3.b, 6.3.c, 6.3.d, 6.3.2.a, 6.3.2.b, 6.4, 6.4.5.1, 6.4.5.2, 6.4.5.3.a, 6.4.5.3.b, 6.4.6, 10.4.2.a, 10.4.2.b	1-5-P-1, 1-5-P-2, 1-5-P-3-1, 1-5-P-3-2, 2-3-P-1-5, 2-16-P-2, 1-5-3-2, 1-6-1, 1-6-2-1, 1-6-2-2, 1-6-3-1, 1-6-3-2, 1-6-3-3, 1-6-3-4, 1-6-3-5	6.2.B, 6.2.F, 6.2.K, 6.2.M	X	X	X	X	1211, 1239, 1419
PM-04	SSO-04	15.5	5.22		CCF 247	CC1.3, CC2.3, CC3.4, CC6.1, CC6.4, CC6.5, CC9.2	A1.2, A1.3	C1.1, C1.2		Clause 6.1.2, Clause 6.1.3, Clause 7.4, Clause 8.1	A.6.1.3, A.7.2.1, A.9.2.6, A.13.2.1, A.13.2.2, A.13.2.3, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.18.1.2							OIS-07, OPS-21, COS-01, COS-03, DEV-02, SSO-01, SSO-02, SSO-03, SSO-04, SSO-05, SIM-04	CA-3, PS-7, SA-1, SA-4, SA-9	org.4, op.pl.1	op.ext.1	op.ext.1	7.2.1, 12.1.2, 13.1.2.1, 13.2.1, 13.2.2, 13.2.3, 14.2.5.7, 14.2.7, 15.1.1, 15.1.2, 15.1.3, 15.1.3.10.P, 15.1.3.11.P, 15.2.1, 15.2.2, 18.1.2, 4.4.7.1, 4.4.7.2, 4.4.7.3, 4.4.7.4, 4.4.8.1, 4.4.8.2, 4.4.8.3, 4.4.8.4, 4.4.8.5, 4.5.1.1, 4.5.3.1, 4.5.4.1, 4.5.4.2, 4.5.4.3, 4.5.4.4, 4.5.4.5	2.5, 2.6, 9.5, 9.5.1, 12.8, 12.8.2, 12.8.3, 12.8.4, 12.8.5	2-9-T-1-2, 4-1-P-1-2, 4-1-P-1-3, 4-1-P-1-4, 1-5-3-3, 4-1-2-2, 4-1-3-1, 4-1-4, 4-2-1, 4-2-2	6.2.C, 6.2.F, 6.2.G, 6.2.L, 6.2.M, 6.2.N, 6.2.Q	X	X	X	X	1631, 1637, 0938, 1322, 0141, 1568, 1632
IM-02	SIM-02	16.3 16.5	5.25 8.8		CCF 236	CC2.2, CC3.2, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1				Clause 7.4, Clause 7.5.3	A.6.1.3, A.6.1.5, A.14.1.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.6							OIS-03, SP-01, OPS-13, SIM-01, SIM-02, SIM-03, SIM-05	IR-1, IR-2, IR-4, IR-6, IR-7, IR-8	org.2, org.3, op.mon.2, mp.per.3, mp.eq.3	op.exp.3, op.exp.7, op.ext.2, op.mon.2	op.exp.3, op.exp.7, op.ext.2, op.mon.2, mp.s.8	6.1.3, 6.1.5, 12.1.5.1.PB, 14.1.3, 16.1.1, 16.1.2, 16.1.3, 16.1.6, 3.1.5.2, 3.1.5.4, 3.1.5.5, 4.4.1.2, 4.5.3.1, 4.8.2.2, 4.9.2.2	6.1.a, 6.1.b, 11.2.a, 11.2.b, 11.5.1, 12.10, 12.10.1.a, 12.10.1.b, 12.10.4, 12.10.5, 12.10.6	2-3-P-1-12, 2-9-T-1-2 , 2-12-3-1, 2-12-3-2, 2-13-3-3, 2-12-3-4, 2-13-3-1, 2-13-3-2, 2-12-1, 2-12-2, 2-13-1, 2-13-2, 2-13-4	6.2.B, 6.2.M, 6.2.O, 6.2.P	X	X	X	X	1213, 1631, 0123, 0043, 0817, 1626

EUCS	C5	SecNumCloud	ISO 27002	ISO 27017	Cisco CCF	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*	13*	14*	15*	16*	17*	18*	19*	20*	21*	22*	23*	24*	25*	26*
CO-03	COM-03		5.35		CCF 1	CC1.5, CC2.1, CC2.2, CC2.3, CC3.1, CC3.2, CC4.1, CC5.1, CC5.2, CC5.3				Clause 6.1.1(e), Clause 6.1.2, Clause 6.1.3, Clause 7.1, Clause 8.3, Clause 9.1, Clause 9.2, Clause 9.3(c), Clause 10.1, Clause 10.2	A.12.7.1, A.18.1.1, A.18.2.1, A.18.2.2, A.18.2.3							OIS-01, SP-01, SP-02, SP-03, SSO-04, COM-02, COM-03	AU-1, CA-2, CA-2 (1), CA-5, CA-7	org.2, org.3, op.mon.2		op.pl.5	13.1.1.7, 17.1.3, 18.1.1, 18.2.1, 18.2.1.9.P , 18.2.1.12.P, 18.2.1.13.P, 18.2.2, 18.2.3, 3.1.4.1, 3.1.4.2, 3.1.4.3, 3.1.4.4, 3.1.5.2, 3.1.5.5, 3.1.6.1, 3.1.6.2, 4.4.1.1, 4.4.1.2, 4.4.6.1, 4.4.7.1, 4.4.7.2, 4.4.7.3, 4.4.7.4, 4.4.8.1, 4.4.8.2, 4.4.8.3, 4.4.8.4, 4.4.8.5,	6.4.6, 10.1	2-16-P-4, 1-3-T-1-1, 1-9-4-2, 2-1-2, 2-1-4, 1-1-3, 1-3-2, 1-8-1, 1-8-2, 1-8-3, 2-2-2, 2-2-4, 2-3-4, 2-4-4, 2-5-4, 2-6-4, 2-7-4, 2-8-4, 2-9-4, 2-10-4, 2-11-4, 2-12-4, 2-13-4, 2-14-4, 2-15-4, 3-1-4, 4-1-4, 4-2-4, 5-1-4	5.5.A, 5.5.B, 6.2.K, 6.3.A	X	X	X	X	1163, 1563, 1564, 0810, 0336, 1493
INQ-03	INQ-03 INQ-04				CCF 279													INQ-01, INQ-03, INQ-04							2-12-P-1-5	5.11.B					
PSS-04	PSS-11				CCF 173													PSS-11					, 5.1.1.28.P , 9.5.1.P, 9.5.2.P, 9.5.2.1.PB , 13.1.4.P, 13.1.4.1.P		5-1-2, 5-1-3-1, 5-1-3-2		X	X	X	X	1605

1	SOC TSC Common Criteria
2	SOC TSC Availability
3	SOC TSC Confidentiality
4	SOC TSC Privacy
5	ISO 27001 ISMS
6	ISO 27002 Annex A
7	Service Customers ISO 27017

8	Cloud Service Providers ISO 27017
9	ISO 27018
10	PII Controller ISO 27701
11	PII Processor ISO 27701
12	ISO 22301
13	BSI C5
14	FedRAMP Tailored Control

15	Spanish ENS BASIC Control
16	Spanish ENS Medium Control
17	Spanish ENS High Control
18	ISMAP
19	PCI
20	Saudi CCC
21	EU Code of Conduct

22	IRAP Official
23	IRAP Protected
24	IRAP Secret
25	IRAP Top Secret
26	IRAP Control

Appendix 4: MEDINA Glossary

This appendix provides a glossary of the terms that are often used in MEDINA. It is an update of the glossary presented in D2.1 [1].

- **Assurance Level:** a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned. The EU Cybersecurity Act defines the following assurance levels:
    - Basic
    - Substantial
    - High

  Source: EU Cybersecurity Act [6]

- **Certification**: third-party attestation related to an object of conformity assessment, with the exception of accreditation

  Source: EUCS1 [47]

- **Certification scheme**: conformity assessment scheme that includes a certification activity.

  Source: EUCS1 [47]

- **Certified cloud service:** a cloud service that that has been awarded an EUCS certificate that is still valid, and whose CSP continues to fulfil the EUCS requirements.

  Note 1 to entry: This is a restrictive definition in use solely in the EUCS scheme.
  Source: EUCS1 [47]

- **Cloud capabilities type**: Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used.

  Source: ISO/IEC 17888 [48]

- **Cloud Service:** One or more capabilities offered via cloud computing invoked using a defined interface.

  Source: ISO/IEC 17888 [48]

- **Cloud Service Provider (CSP):** Party which makes cloud services available

  Source: ISO/IEC 17888 [48]

- **Compliance:** conformity in the context of the rules and requirements defined in a certification scheme that apply to the provider of the certified product, service or process.

  Note 1 to entry: This is a refinement of ISO19011, which defines compliance as conformity in the context of a statutory requirement or regulatory requirement. In this case, compliance is conformity in the context of a given scheme.

Note 2 to entry: The term is used to differentiate between compliance of a cloud service provider to the requirements defined in the scheme and conformity of a cloud service to the requirements on controls defined in the scheme.

Source: EUCS1 [47]

- **Composition**: reuse of the results of certification activities of a certified cloud service in the evaluation of a primary cloud service using that certified cloud service as secondary cloud service.

  Source: EUCS1 [47]

- **Conformity:** fulfilment of a requirement.

  Note 1 to entry: when used in opposition with compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme.

  Source: EUCS1 [47]

- **Conformity assessment body (CAB):** body that performs conformity assessment services.

  Source: EUCS1 [47]

- **European cybersecurity certification scheme (EUCS):** a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.

  Note 1 to entry: This definition is a refinement of the definition of a certification scheme.
  Source: EUCS1 [47]

- **Evidence:** 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

  Source: ISO9000:3.8.3

- **Measurement Result:** the outcome of applying a Metric.

  Example: TLS Version = 1.0, Maximum Password Age = 20 days, Password Length = 6 characters, Encryption at rest = Enabled

- **Monitoring:** determining the status of a system, a process or an activity.

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

Source: EUCS1 [47]

- **Monitor automatically:** Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency by non-human means.

  Source: EUCS1 [47]

- **Questionnaire**: Is the checklist elaborated in MEDINA to develop an assessment model for requirements in the basic/substantial/high level of assurance that can be understood by less experienced compliance managers and CSPs in general. However, CABs and auditors could also adopt it as guidance.

- **Assurance_level**: the level of assurance for which the user wants to assess the cloud service. Each question has also an assurance level assigned. The possible values are:

  - Basic
  - Substantial
  - High

- **Question**: The questionnaire is composed by a series of questions, based on the experience of the auditors, consultants and CSPs that participated in MEDINA, as well as from literature. Multiple questions have been created for each of the requirements in the EUCS framework, hence, more than 900 questions are included in the questionnaire. The questions identify some examples of evidence that the CSP shall submit to the CAB for the evaluation assessment.

  Example: Does the CSP have an information security management system (ISMS) documented?

- **Question_answer**: The answer to each question. It is a closed group that can take one of these values:

  - Fully supported
  - Partially supported
  - Not supported
  - Not applicable

- **Questionnaire non-conformities**: The non-conformities are deviations from the requirement. In the MEDINA questionnaire, they are textual sentences that can be introduced by an auditor in each requirement.

- **Questionnaire purpose**: we distinguish two different possible purposes for a questionnaire:

  - Self-evaluation
  - External audit

- **Jhi_user**: Is the user that creates and answers the questionnaire. Users in MEDINA are centralized by the Keycloak identity manager, where they are and created and managed. The user is linked to a cloud service provider, and has a list of cloud services list associated to him.

- **Requirement:** need or expectation that is stated, generally implied or obligatory.

  Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

  Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

  Note 3 to entry: A qualifier can be used to denote a specific type of requirement, e.g. product requirement, service requirement, customer requirement.

  Source: EUCS1 [47]

- **Resource:** component of the Cloud Service, which offers a specific capability to the cloud customer.

  Examples:

  - Virtual Machines.
  - Kubernetes clusters.
  - Databases.

  Source: leverages ISO17788:3.2.4

- **Scope of certification:** identification of:
  - the product(s), process(es) or service(s) for which the certification is granted,
  - the applicable certification scheme,
  - and the standard(s) and other normative document(s), including their date of publication, to which it is judged that the product(s), process(es) or service(s) comply.

  Source: EUCS1 [47]

  - **Target of Evaluation (Target of Certification):** in the context of MEDINA, it refers to the Cloud Service which is in the scope of certification.

    Source: MEDINA project

- **Security Metric:** An abstract definition that describes the conditions and process for assessing a specific Security Requirement as part of a Security Assessment Rule. The metric does not define the Target Value for the Security Assessment Rule.

  Example: TLS Version, Maximum Password Age, Password Length, Retention Time

  Source: NIST SP500-307

- **Technical and Organizational Measure Reference:** documented good practice that provides the basis for a compliant implementation of a Technical and Organizational Measure. The Reference Technical and Organizational Measure should be technology-/CSP-agnostic.

  Example: The retention time for data backups is configured individually for each resource provisioned from the CSP, by accessing the corresponding user interface. The retention period is then configured according to the documented security policy of the CSP.

  Source: MEDINA project

- **Security Assessment Result:** the outcome of a performed Security Assessment Rule.

  Example: Compliant, Non-compliant

- **Security Assessment Rule:** is the process that applies a specific Metric to assess if the Security Configuration is compliant with a specific Target Value. The Security Assessment Rule compares a Measurement Result with the specific Target Value to obtain a Security Assessment Result. The security assessment rule is instantiated from a template which references the Metric to apply, but not the specific Target Value to use for the assessment of the Security Configuration. This is the DSL. The rules are translated from Security obligations (CNL) to rego-code.

  Example:

  - Requirement text: Check that the retention time configured for a cloud-based SQL database is set to 35 days.

    Rego code (comments are marked with #):

    ```
    {
          tv := 35 # Retention-time-target-value
          mv := 30 # Retention-time-measured-value
          tv >= mv
    }
    ```
  - Check that the configured TLS Version of an Application Service is at least 1.2
  - Check that the maximum password age on a cloud-based Linux VM is set to 30 days.

  Source: MEDINA project

- **Security Configuration:** the Cloud Service's implementation of a specific Technical and Organizational Measure. Ideally, the Security Configuration of a Cloud Service must be fully compliant with the TOM.

  Example: backup retention time on a cloud-based SQL database is set to 30 days

- **Security Control:** a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (cf. Technical and Organizational Measures).

  Example: CKM-01 POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT (from EU Cloud Services Certification Scheme)

  Source: Security and Privacy Controls for Federal Information Systems and Organizations - NIST Special Publication 800-53. rev 4 [49]

- **Security Control Category:** set of security controls, obtained by grouping together related security controls.

  Examples:

  - Information Security Policies
  - Personnel & Training
  - Identity and Access Management
  - Cryptography and Key Management

- **Security Control Effectiveness:** the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

  Source: NIST, "Security and Privacy Controls for Federal Information Systems and Organizations - NIST Special Publication 800-53. rev 4," 2014 [49].

- **Security Control Framework:** Set of security control categories, namely a scheme.

  Examples:

  - ISO/IEC 27001 [50]
  - NIST SP 800-53 [49]
  - BSI C5

- **Security Control Objective:** statement describing what it is to be achieved as a result of implementing a control.

  Example:

  CKM-01 POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT

  Objective

  Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.

  Source: ISO/IEC 27000:2018 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary [51]

  - **Security obligation:** This is the CNL. It is the formal definition of a set of metrics mapped to a requirement.

  The **Medina CNL** is based on the notion of Simple Obligation ***obl***:

  $$\mathbf{obl} = \mathrm{op}(M(A), TV)$$

  Recursive definition of the Composed Obligation *OBL*

  $$OBL = obl \mid OBL \textbf{ and } OBL$$

  M metric; **A** asset; **TV** target value; **M(A)** returns the value of the metric measured on the asset

  op(*,*) is a binary operator, returns a **Boolean** value, range over {**=, >, <** …}

  Source: MEDINA project

- **Security requirement:** see Technical and Organizational Measure.

- **Similar Control**: a control that has been mapped by MEDINA as "equivalent" to an EUCS control in other schemes or standards. The objective is to facilitate the transition from other schemes towards EUCS and vice versa, as well as the reuse of evidence, whenever possible. In the catalogue, we have defined a list of equivalences among EUCS controls and controls in these other schemas: ISO/IEC 27000, BSI C5:2020, SecNumCloud and Cisco CCF,

- **Tamper proof:** feature of the Digital Audit Trail (DAT) system guaranteeing information cannot be modified (it is impossible to change).

- **Target Value:** property of a Security Assessment Rule, defining the value for a specific Metric so the Security Configuration of the Cloud Service is compliant with the TOM. The target value is defined by the CSP.

  Example: Max Password Age <= 90 days, TLS Version In Use >= 1.2, Encryption Key Length >= 1024 bits, Retention Time > 35 days

- **Technical and Organizational Measure (TOM):** a security requirement that modifies the likelihood or the severity of a risk. It includes the policy, procedures, guidelines, and the organizational practices or structures, and can be of an administrative, technical, managerial or legal nature.

  Example: (from the EU Cloud Services Certification Scheme)

  CKM-01.1: The CSP shall define, communicate and make available policies with technical and organizational safeguards for encryption and key management, according to ISP-02, in which at least the following aspects are described:

  - Usage of strong encryption procedures and secure network protocols
  - Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys
  - Consideration of relevant legal and regulatory obligations and requirements

  Source: *EU Cloud Services Certification Scheme*

Terms coming from the Cybersecurity Act Article 2

The following terms are defined in Article 2 of the Cybersecurity Act [6]. Their meaning in this document is aligned with the definition of this regulation. They are copied in this document for readability issues but are publicly available in [6]:

(1)

‘**cybersecurity’** means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(2)

‘**network and information system’** means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;

(3)

‘national strategy on the security of network and information systems’ means a national strategy on the security of network and information systems as defined in point (3) of Article 4 of Directive (EU) 2016/1148;

(4)

‘operator of essential services’ means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5)

‘**digital service provider’** means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;

(6)

‘**incident’** means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7)

‘incident handling’ means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8)

‘cyber threat’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(9)

‘**European cybersecurity certification scheme’** means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(10)

‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme;

(11)

‘European cybersecurity certificate’ means a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

(12)

‘ICT product’ **means an element or a group of elements of a network or information system;**

(13)

‘ICT service’ means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(14)

‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(15)

‘accreditation’ means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;

(16)

‘national accreditation body’ means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;

(17)

‘conformity assessment’ means a conformity assessment as defined in point (12) of Article 2 of Regulation (EC) No 765/2008;

(18)

‘conformity assessment body’ means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008;

(19)

‘standard’ means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012;

(20)

‘technical specification’ means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process;

(21)

‘assurance level’ means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned;

(22)

‘conformity self-assessment’ means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.