Deliverable D2.1

Continuously certifiable technical and organizational measures and Catalogue of cloud security metrics-v1

Editor(s):	Leire Orue-Echevarria
Responsible Partner:	TECNALIA
Status-Version:	Final – V1.0
Date:	31.10.2021
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-v1
Due Date of Delivery to the EC	31.10.2021

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

Abstract:	This set of deliverables will present 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. These deliverables are the result of Task 2.2 and part of 2.1.
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	09.12.2020	TOC	Leire Orue-Echevarria (TECNALIA)
v0.2	20.10.2021	Sent for internal review	Leire Orue-Echevarria (TECNALIA)
V0.3	27.10.2021	Addressed all comments received in the internal QA review	Leire Orue-Echevarria (TECNALIA)
V1.0	27.10.2021	Ready for submission	Leire Orue-Echevarria (TECNALIA)

Table of contents

List of tables

List of figures

Terms and abbreviations

CSA or EU CSA	Cybersecurity Act
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CVE	Common Vulnerabilities and Exposures
DoA	Description of Action
EC	European Commission
EUCS	European Cloud services
GA	Grant Agreement to the project
ISMS	Information Security Management Systems
KPI	Key Performance Indicator
TOM	Technical and Organizational Measure

Executive Summary

This deliverable presents the initial version of the catalogue of TOMs and security metrics.

The document starts with a comparative analysis of four schemes, namely EUCS, ISO/IEC 27000 family (27002, 27017), BSI C5 and SecNumCloud, in different dimensions such as the categories, the structure, the levels and the conformity assessment method, as well as the mapping of the controls. The goal of this mapping is to allow an easier transition from one scheme to another and facilitate the reuse of evidence whenever possible.

The second goal of this document is to present a set of reference technical and organizational measures for the 33 requirements identified with the assurance level high in the version of December 2020 of the European draft candidate EUCS. A reference TOM is a sort of implementation guidance that is vendor and technology agnostic. This is another novelty brought in by MEDINA and they are aimed at small and medium CSPs aiming at the assurance level high. This reference TOMs are used as input by the certification language for the creation of their corpus of data.

The third goal is the definition of the MEDINA catalogue of security metrics, which lie at the core of the project as most of the tools rely heavily on them. More than 250 metrics have been elicited at this stage, coming from literature and other European projects but also from MEDINA partners themselves. 70% of the elicited metrics come from the MEDINA partners to be compliant with the draft EUCS, which is also a novelty. All metrics have been described following the same structure; whose details can be seen in Appendix 3. They all have a defined data type, data range, interval, and formula. While most metrics are directly linked to a requirement of assurance level "high", there are some that are either of a more general purpose or compliant with a requirement of a lower level of assurance. They are however still relevant at this stage because they are needed to measure the operational effectiveness required in the substantial level of assurance.

Finally, the document includes the functional and technical design of the first version of the software implementation of the catalogue. The current version includes the implementation of three core requirements, which will be extended in future versions.

The deliverable includes four appendices complementing the previous sections.

The next version of this document (M27) will contain updated versions of the mapping as it is expected that the EUCS will evolve (it is currently under revision), new and updated TOMs as well as new and updated metrics. It will also include the final version of the software component of the catalogue.

This document is tightly related with other activities that are currently on-going in MEDINA such as the certification language (e.g., CNL editor), 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 first iteration of two and aims at presenting a catalogue of technical and organizational measures and security metrics that can be later on used by the rest of the components of the MEDINA framework.

1.2 Document structure

This document is structured as follows. Section 2 has a twofold goal. Firstly, it starts with an overview of four schemes, namely the European draft candidate EU Cloud Services certification scheme (EUCS) in the public version released in December 2020, ISO/IEC 27000, BSI C5 and SecNumCloud. This subsection finishes with a comparative analysis in terms of control categories, structure, and conformity assessment method of said schemes. Secondly, it maps the security controls from the schemes previously mentioned.

Section 3 presents an initial version of reference Technical and Organizational Measure (TOM) implementations for the 33 requirements of assurance level high of the European draft candidate EU Cloud Services certification scheme (EUCS) in the public version released in December 2020. A reference TOM implementation 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 with what the scheme says. This is to serve as guidance but also as input to the certification language, through Natural Language Processing (NLP) Techniques. The section includes not only the initial version of the TOMs but also the motivation and the methodology followed. The details of the 33 requirements covered by said TOMs can be found in Appendix 2 for understandability reasons.

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 gathered the metrics and the structure of the metrics. While the goal initially was to elicit metrics for the 33 requirements of assurance level high of the European draft candidate EU Cloud Services certification scheme (EUCS) in the public version released in December 2020, MEDINA partners have also defined additional relevant metrics for other requirements deemed relevant for the continuous monitoring or operational effectiveness, as described in EUCS. The complete description of metrics can be found in Appendix 3.

Section 5 describes the technical implementation of the catalogue of security controls and metrics, which is the software implementation of all the elements described in the previous sections. This is the first version of the prototype and the section describes the architecture, the data model and the sequence diagram, extending the information provided in D5.1 [1].

Section 6 concludes this deliverable.

Appendix 4 presents the MEDINA Glossary with the most common terms used in the project for clarification purposes. It extends and corrects the previous edition of the glossary presented in Deliverable D1.1, which is confidential.

2 Mapping of security controls

This section presents a brief overview of the security schemes analysed for this version, which are BSI C5 in the versions of 2016 and 2020, as both are still active at the time of writing this deliverable, ISO/IEC 27000 family, SecNumCloud and the European draft candidate EU Cloud Services certification scheme (EUCS) in its version from December 2020.

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

- Categories, that is, the domains that the scheme covers
- Structure of the scheme
- Conformity assessment method

The section includes also a table summarizing and comparing them on various dimensions.

Finally, the section finishes with a mapping of the controls of the schemes and standards previously analysed. The goal of this mapping is to provide a guidance in the transitioning towards the EUCS.

2.1 Compared Schemes and standards

2.1.1 European draft candidate EU Cloud Services certification scheme (EUCS)

The European draft candidate EU Cloud Services certification scheme (EUCS) [2] looks into the certification of cloud services and was published for public review on December 2020. While this version is still under revision, this is the version that has been analysed for this deliverable. For upcoming versions of this deliverable, relevant updates of the EUCS will reported hereby.

The EUCS is the second certification scheme that is being created under the scope of the Cybersecurity Act (EU CSA) [3][1]. Following the request of the European Commission on November 2020 and in accordance to Article 48.2 of the EU CSA [3], ENISA created an ad-hoc working group consisting of 20 members [4] 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 [5], BSI C5 [6], SecNumCloud [7], ISO standards [8] [9] [10], and ISAE [9] [11], among others.

EUCS follows the three levels proposed in the Article 52(6) of the EU CSA) [3], 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 scheme EUCS states [2] (p.5) that “*the requirements at level ‘high’ are demanding and close to the state-of-the-art, whereas the requirements at level ‘basic’ define a minimum acceptable baseline for cloud cybersecurity*” [2].

The draft EUCS candidate version of December 2020 has the following categories and objectives [2]:

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

Table 1. Categories and objectives of the controls from the draft EUCS candidate version of December 2020

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

EUCS Category [2]	EUCS Objective [2]
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 conformity assessment methodologies:

- For basic: 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 [2, p. 6]
- For substantial and high: EUCS has defined an assessment approach that is compatible with both ISO27000 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/IEC27000 family

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

For the scope of MEDINA, the following standards out of the ISO/IEC 27000 family are relevant. These are:

- ISO/IEC 27001 [9]: it specifies the requirements to set up, implement and maintain an ISMS of an organization. Annex A contains the controls.
- ISO/IEC 27002 [8]: it provides the guidelines and best practices for the implementation of the ISMS. It actually presents the controls to implement ISMS of ISO/IEC 27001. The controls are the same as in annex A of ISO/IEC 27001, but it also includes some implementation guidance.
- ISO/IEC 27017 [10]: it extends the controls of ISO/IEC 27002 with controls applicable to cloud services.

ISO/IEC 27002 defines the following categories [8]:

Table 2. ISO/IEC 27002 control categories and objectives

ISO/IEC 27002 category [8]	ISO/IEC 27002 objective [8]
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	It defines all aspects related to the policies and procedures related to human resources prior, during and after employment.
Asset management	To 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	To manage the access, rights, controls and authentication of users
Cryptography	Cryptographic controls and key management.
Physical and environmental security	To 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	To 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 [8] are structured as follows:

- Control name
- Control objective: it defines the statement that needs to be satisfied
- Implementation guidance: it provides some support on how the control should be implemented to meet the control objective.
- Other information: this is for instance other 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 [12].

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[2] for cloud computing, often referred as C5 [13]. 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 the known standards and schemes [14], 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, BSI IT-Grundschutz-Kompendium - Edition 2019. Moreover, C5:2016 states [13] that for the definition of the requirements they used as baseline content coming from requirements coming 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.

BSI has aimed to document the requirements in a transparent manner so the CSP could perform a comparative analysis with their own security level.

C5 is audited following the ISAE methodology [11] [15] by a public accountant where the result is a report.

C5 has released two version of the Catalogue of controls, one in 2016 and a second one in 2020, in preparation and response to the EU CSA. Both are included because at the time of writing this deliverable both are still active. The following table presents the categories in C5, as well as their scope and their prevalence in their versions of 2016 and 2020. Their differences in their wording are highlighted in cursive.

Table 3. Categories description of C5:2020 vs. C52016

C5: 2016 [13]	**C5:2020** [6]
Organisation of information security: Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.	Organisation of Information Security: *Plan, implement, maintain and continuously improve* the information security framework within the organisation.
Security policies and work instructions: Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.	Security Policies and Instructions: *Provide policies and instructions regarding security requirements and to support business requirements.*
Personnel: Making sure that employees, service providers and suppliers understand their tasks, are aware of their responsibility with regard to information security and that the assets of the organisation are protected if the tasks are modified or completed.	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.*

[2] 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".

C5: 2016 [13]	**C5:2020** [6]
Asset management: Identifying the organisation's own assets and responsible persons as well as ensuring an appropriate level of protection.	Asset Management: Identify the organisation’s own assets *and ensure* an appropriate level of protection *throughout their lifecycle*.
Physical security: Preventing unauthorised physical access and protection against theft, damage, loss and failure of operations.	Physical Security: *Prevent* unauthorised physical access and *protect* against theft, damage, loss and *outage* of operations.
Safeguards for regular operations: Assuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.	*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: Providing the ability to securely operate the service on different IT platforms as well as the possibility of secure connections to different IT platforms and termination of the service	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: Securing the authorisation and authentication of users of the cloud provider (usually privileged user) and the cloud customer in order to prevent unauthorised access.	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: Using appropriate and effective cryptography in order to safeguard information security.	Cryptography and Key Management: *Ensure* appropriate and effective use of cryptography *to protect the confidentiality, authenticity or integrity of information.*
Communication security: Protecting information in networks and the corresponding information-processing systems.	Communication Security: *Ensure* the protection of information in networks and the corresponding information processing systems.
Procurement, development and maintenance of information systems: Complying with the security targets in case of new developments and procurement of information systems as well as changes.	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: Protecting information that can be accessed by service providers and/or suppliers of the cloud provider (subcontractors) and monitoring the	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.*

C5: 2016 [13]	**C5:2020** [6]
services and security requirements agreed upon.	
Security incident management: Assuring a consistent and comprehensive approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.	Security Incident Management: *Ensure* a consistent and comprehensive approach to the *capturing, evaluation, communication and handling of* security incidents.
Business continuity management: Strategic establishment and governance of a business continuity management (BCM). Planning, implementing and testing business continuity concepts as well as incorporating safeguards in order to ensure and maintain continuous operations	Business Continuity Management: *Plan, implement, maintain and test procedures and measures for business continuity and emergency management.*
Security check and verification: Checking and verifying that the information security safeguards are implemented and carried out in accordance with the organisation-wide policies and instructions.	
Compliance and data protection: Preventing violations against statutory or contractual duties with respect to information security.	Compliance: *Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.*
Mobile device management: Guaranteeing secure access to IT systems via mobile devices in the cloud provider's responsibility to develop and operate the cloud service.	
	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, appropriate mechanisms for troubleshooting and logging, as well as authentication

The controls that have changed between the versions of C5:2016 and C5:2020 are mapped in Appendix 1.

The controls in C5:2020 are structured as follows:

- Basic Criteria: the 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 decide that they need a higher level of protection, this additional criterion is therefore for them and shall be included in an 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 controls of C5 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.

In contrast with C5:2020, C5:2016 states that a requirement specifies general principles, procedures and measures for fulfilling an objective. C5:2016 was structured as follows:

- Basic requirement: which is considered essential and the CSP must meet and comply with in an audit.
- Additional requirement: it is an optional requirement and is classified as to whether it addresses confidentiality, availability or both. According to BSI "*It turned out that there are no effective higher-level requirements for integrity (I) in addition to the basic requirements, which is why this category is missing here*".

2.1.4 SecNumCloud

SecNumCloud [7] 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 [7]:

- 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, it contains additional requirements focused on:

Table 4. SecNumCloud additional requirements

SecNumCloud Additional requirements [7]	SecNumCloud Additional requirements description [7]
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 processes, which it 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	This means that the CSP shall ensure a secure erase of all the data of the customer.

In SecNumCloud, the scheme is structured as follows:

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

2.1.5 Summary – comparative analysis

The following table summarizes the information of the previous sections:

Table 5. Summary – comparative analysis (source: MEDINA's own contribution)

	EUCS	C5:2016	C5:2020	SecNumCloud	ISO/IEC27002 – ISO/IEC 27017
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	1. Organisation of information security (OIS) 2. Security policies and work instructions 3. Personnel (HR) 4. Asset management (AM) 5. Physical security (PS) 6. Operations (RB) 7. Identity and access management (IDM) 8. Cryptography and key management (KRY) 9. Communication security (KOS) 10. Portability and interoperability (PI) 11. Procurement, development, and maintenance	1. Organisation of Information Security (OIS) 2. Security Policies and Instructions (SP) 3. Personnel (HR) 4. Asset Management (AM) 5. Physical Security (PS) 6. Operations (OPS) 7. Identity and Access Management (IDM) 8. Cryptography and Key Management (CRY) 9. Communication Security (COS) 10. Portability and Interoperability (PI) 11. Procurement, Development and Modification of Information Systems (DEV) 12. Control and Monitoring of Service Providers and Suppliers (SSO)	• 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.

	EUCS	C5:2016	C5:2020	SecNumCloud	ISO/IEC27002 – ISO/IEC 27017
	• Dealing with investigation requests from government agencies • Product safety and security	of information systems (BEI) 12. Control and monitoring of service providers and suppliers (DLL) 13. Security incident management (SIM) 14. Business continuity management (BCM) 15. Security check and verification (SPN) 16. Compliance and data protection (COM) 17. Mobile device management (MDM)	13. Security Incident Management (SIM) 14. Business Continuity Management (BCM) 15. Compliance (COM) 16. Dealing with investigation requests from government agencies (INQ) 17. Product Safety and Security (PSS)		
Structure of the controls	• Category title • Category objective: statement of that category • Control id and name • Control objective: goal of that control	• Basic requirement • Additional requirement	• Basic Criteria • Additional Criteria: • Supplementary information: • Notes on Continuous Auditing	• Category title • Control title • Requirements	• Category title • Control name • Control objective • Implementation guidance • Other information

	EUCS	C5:2016	C5:2020	SecNumCloud	ISO/IEC27002 – ISO/IEC 27017
	• Requirement id, description and assurance level • Implementation guidance		• Complementary Customer Criteria:		
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 [2] (p.6). • For substantial and high: EUCS has defined an assessment approach compatible ISO/IEC 17065 ISAE 3402	ISAE 3402	ISAE 3402	Qualification	ISO based (ISO 17065)
Scope	Service	Service	Service	Provider (*Prestataire*)	ISMS

2.2 Mapping of the controls of the previously analysed schemes

In this version, a mapping between EUCS, C5:2020, SecNumCloud, ISO/IEC 27002 and ISO/IEC 27017 has been performed.

The goal of this mapping is to identify similar controls in scope other schemes to facilitate, as much as possible, the transition from other standards and schemes towards EUCS as well as the reuse of evidence, whenever possible.

The mapping has been performed in a manual and empirical way, by reading the controls one by one and matching them. While the analysis before has shown the different granularity level in which the different schemes are structured, it can be seen that the minimum common level of comparability is the control.

The EUCS controls are considered the baseline controls. Whenever a similar control in scope or meaning was found in the other schemes or standards, they were noted down, even if the matching was not 1:1 or 100%, hence the multiple matching. This has been done so purposely not to leave any requirement out.

Table 6. Mapping of security controls (EUCS version December 2020, C5:2020, SecNumCloud, ISO/IEC 27002, ISO/IEC 27017) (source: MEDINA's own contribution)

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
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
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			
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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
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	
HR-04 - SECURITY AWARENESS AND TRAINING	HR-03		7.2.2	
HR-05 - TERMINATION OR CHANGE IN EMPLOYMENT	HR-05	7.5	7.3.1	
HR-06 - CONFIDENTIALITY AGREEMENTS	HR-06		7.1.2 13.2.4	
AM-01 - ASSET INVENTORY	AM-01	8.1.1. 8.1.2	8.1.1	
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	
AM-04 - ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS	AM-05		8.1.4 8.2.1	CLD 8.1.5
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	
PS-03 - WORKING IN NON-PUBLIC AREAS		11.4		
PS-04 - EQUIPMENT PROTECTION		11.6 11.7 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	
OPS-03 - CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES	OPS-03			CLD.12.4.5

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
OPS-04 - PROTECTION AGAINST MALWARE – POLICIES	OPS-04	12.4		
OPS-05 - PROTECTION AGAINST MALWARE – IMPLEMENTATION	OPS-05	12.4	12.2.1	
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		
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		
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		
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	
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			
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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
OPS-20 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS OF PROCEDURES	OPS-20	12.9	12.6.1	
OPS-21 - MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	OPS-23	12.9		
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	
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 ENCRYPTION MECHANISMS 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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
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	
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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
CCM-04 - APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT	DEV-09			
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	
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	
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	
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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
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		
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	
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	

EUCS Control	C5.2020 GERMANY	SecNumCloud FRANCE	ISO/IEC 27002	ISO/IEC 27017
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-06 - 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			
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			
PSS-05 - LOCATIONS OF DATA PROCESSING AND STORAGE	PSS-12			

3 Reference Technical and organizational measures (TOMs) for continuous assessment

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 released on December 2020 [2].

The draft version of the candidate EUCS scheme released on December 2020 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.

The ones that comply with both prerequisites are shown in the next table:

Table 2. Requirements considered in MEDINA that are of assurance level high and have the wording "automatically monitor" (source: EUCS [2])*

EUCS Category [2]	EUCS Security Control [2]	EUCS Security Requirement [2]
Organisation of Information Security	OIS-02 Segregation of duties	OIS-02.4 The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
Security Policies and Procedures	ISP-03 Exceptions	ISP-03.7 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	N/A
Human Resources	HR-03 Employee terms and Conditions	HR-03.5 The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.
Human Resources	HR04 Security awareness and training	HR-04.7 The CSP shall automatically monitor the completion of the security awareness and training program.
Human Resources	HR05 Termination or change in employment	HR-05.4 The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2
Human Resources	HR06 Confidentiality Agreements	HR06.7 The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers
Asset Management	AM01 Asset Inventory	AM01.06 The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date
Asset Management	AM-03 Commissioning and decommissioning of hardware	AM03.06 The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.

EUCS Category [2]	EUCS Security Control [2]	EUCS Security Requirement [2]
Asset Management	AM-04 Acceptable use, safe handling and return of assets	AM04.04 The verification of the commitment defined in AM-04.1 shall be automatically monitored
Physical Security	PS02 Physical Site Access control	PS02.10 The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9
Operational security	OPS2 – Capacity management - monitoring	OPS02.3 The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1
Operational security	OPS-05 - Protection against malware - implementation	OPS.05.3 The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1
Operational security	OPS-05 - Protection against malware - implementation	OPS.05.4 The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities
Operational security	OPS-07 Data backup and recovery - monitoring	OPS.07.2 The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1
Operational security	OPS-07 Data backup and recovery - monitoring	OPS.07.3 The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1
Operational security	Ops-09 data backup and recovery – storage	OPS-09.5 When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1
Operational security	Ops-12 logging and monitoring – identification of events	OPS-12.4 Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.
Operational security	Ops-13 logging and monitoring – access, storage and deletion	OPS-13.7 The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1
Operational security	Ops-18 managing vulnerabilities, malfunctions and errors – online registers	OPS-18.6 The CSP shall equip with automatic update mechanisms 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

EUCS Category [2]	EUCS Security Control [2]	EUCS Security Requirement [2]
Operational security	Ops-21 managing vulnerabilities, malfunctions and errors – system hardening	OPS-21.3 The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications
Identity, authentication and access control management	IAM-03 locking, unlocking and revocation of user accounts	IAM-03.11 The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03
Identity, authentication and access control management		IAM-03.12 The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons
Cryptography and key management	N/A	N/A
Communication security	CS-04 cross-network access	CS-04.5 The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1
Portability and interoperability	N/A	N/A
Change and configuration management	CCM-03 TESTING CHANGES	CCM-03.10 The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues
Change and configuration management	CCM-04 approvals for provision in the production environment	CCM-04.3The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1
Change and configuration management	CCM-05 performing and logging changes	CCM-05.3 The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1
Development of information systems	N/A	N/A
Procurement management	PM-04 Monitoring of compliance with requirements	PM-04.7 The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: •Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).

EUCS Category [2]	EUCS Security Control [2]	EUCS Security Requirement [2]
Procurement management	PM-04 Monitoring of compliance with requirements	PM-04.8 The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action
Incident management	IM-03 Documentation and reporting of security incidents	IM-03.4The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period
Business continuity	N/A	N/A
Compliance	CO-03 Internal audits of the internal control system	CO-O3.4 Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions
Compliance	CO-03 Internal audits of the internal control system	CO-O3.5 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	N/A
Dealing with investigation requests from government agencies	INQ-03 Conditions for access to or disclosure of data in investigation requests	INQ-03.4 The CSP shall automatically monitor the accesses performed by or on behalf of investigators to ensure that they correspond to the determined legal basis
Product safety and security	PSS-04 Images for virtual machines and containers	PSS-04.3 An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images

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

The objective of this section is to facilitate, especially small and medium CSPs with some reference technical and organizational implementations of requirements of assurance level high. A reference TOM implementation can be considered an explanation of how a specific security requirement can be implemented, in a vendor – and technology-agnostic way. This reference TOMs can then be enriched with examples coming from larger CSPs such as Amazon or Azure and that can be used as inspiration. These reference implementations are used as input in the certification language for the associations between the TOMs and metrics using Natural language processing (NLP). TOMs are used in this case as obligations (see D2.3 [16]).

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 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.

3.3 Technical and organizational measures reference implementations per security requirement

The following section describes the initial versions of the elicited reference implementations of the technical and organizational measures per security requirement. Depending on the complexity of the requirements, different levels of detail are provided.

3.3.1 Asset Management :: Asset Inventory :: AM-01.06

The EUCS requirement states [2]:

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

Usually, the CSP sets a suitable framework for identifying, classifying and implementing an inventory of IT-processes, systems and components (assets).

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.

Monitoring 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 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 assets that have the potential to store or process information.

To perform automated monitoring of 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[3] 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.
- Review the inventory on a regular basis to ensure that unauthorized resources are deleted.
- 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, and Refresh time, install date and other information.

3.3.2 Asset Management :: Commissioning and Decommissioning of hardware :: AM-03.6

The EUCS requirement states [2]:

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

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 decommissioning process may differ from every hardware type or technology, but some basics steps include [23]:

- 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

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

- Terminate the Contracts
- Create Backups
- Wipe Data
- Unplug
- Cut Power and Remove
- Destroy Server

3.3.3 Asset Management :: Acceptable use, safe handling and return of assets :: AM-04.4

The EUCS requirement states [2]:

> *The verification of the commitment defined in AM-04.1 shall be automatically monitored*

The requirement's description refers to the following related requirement:

AM-04.1	The CSP shall ensure and document that all internal and external employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-03

This requirement requires that all the CSP needs to monitor is the assurance that internal and external employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-03 [2], which is the commissioning and decommissioning of hardware.

This includes, the automatically 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 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.

3.3.4 Change and configuration management :: Testing changes :: CCM-03.10

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues*

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 [24].

Even though the configuration of the service is in continuous change, the service should not be deployed without being constantly tested in order the minimize the risks of failure upon deployment. These modifications in the configuration of the architecture and the code are usually very frequently so it is recommendable to monitor the definition and execution of the tests related to a change in an automatic way, as well as the mitigation strategies to follow in each case. This automation can reduce delivery time, improve quality and security, and eliminate human errors [25]. It consists of using special software tools to control the definition and execution of the tests and then comparing the actual results with the predicted and expected ones [26], without, or almost, intervention of the CSP developer or operator. This way, a configuration shall only be deployed if all the automated tests are passed, that is, they result in "positive". Accordingly, specific automated test tools should be planned, budgeted, and integrated them into the enterprise architectures and tools used in the CSP for the development of the service / system.

Every time a change in the configuration takes place the following process should be carried out:

- Automatically launch the tests in accordance with their definition
- After the tests have been executed, analyse the results. If is satisfactorily passed, then the service with the new configuration can be deployed, but if not, mitigation issues should be applied (e.g., correct errors and relaunch the tests).
- Store a report with the result and the date

Finally, the CSPs should continuously thoroughly test the service and execute the contingency plan regularly.

3.3.5 Change and configuration management :: Approvals for provision in the production environment :: CCM-04.3

The EUCS requirement states [2]:

The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1*

The requirement's description refers to the following related requirement:

CCM-04.1	The CSP shall approve any change to the cloud service, based on defined criteria, before they are made available to CSCs in the production environment

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 [24]. 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 in the configuration of the architecture usually are very frequently so that it is recommendable to automatically monitor the approvals of these changes deployed in the production environment to guarantee it is done before they are made available to CSCs in the production environment.

Tools can be used in order to give to the administrator a view of all the approvals[4]. A checking process could carry out with the aim of matching the current results with the estimated ones. If this process is satisfactory passed, an approval could be maintained. In the case of approvals, the cloud service could made available to CSCs in the production environment.

3.3.6 Change and configuration management :: Performing and logging changes :: CCM-05.3

The EUCS requirement states [2]:

> *The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1*

The requirement's description refers to the following related requirement:

CCM-05.1	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.

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. Although the configuration of the service is in constant change, the modifications in the configuration of the architecture needs to be authorised and traceable.

Once a change in the production environment will be carried out, its identifier must be stored and matched with the responsible of the modification for a late consultation if necessary (specifically for checking permissions, authorisations, later on). These data could be stored in a stack[5], in a queue, or in other means.

3.3.7 Compliance :: Internal audits of the internal control system :: CO-03.4

The EUCS requirement states [2]:

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

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 two-fold: The overall compliance is evaluated as a percentage of automatically monitored requirements where the target value is 100 %. Secondly, fulfilment of this requirement needs an evaluation 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

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

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

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 the following table imaginary assets and requirements are used for illustration purposes.

Table 8. 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-02.4	100 % (1/1)	<link to measurement>	OK	N/A
HR-04.7	0% (0/0)	<asset_X_measurement not defined>	N/A	N/A
OPS-07.3	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>

3.3.8 Compliance :: Internal audits of the internal control system :: CO-03.5

The 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.*

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. Examples of these pieces of information are version number and identified vulnerability. The provided information may vary depending on the measurement tool’s capabilities.

Table 9. 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. The simplified output with two measurements can be presented like this:

Table 10. 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.

3.3.9 Communication Security :: Cross-network access is restricted and only authorised based on specific security assessments.:: CS-04.5

The EUCS requirement states [2]:

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

And CS-04.1*:*

References as “measures” the following requirements also from CS-04 Cross-network access:

CS-04.1	*Each network perimeter shall be controlled by security gateways*

The usage of security gateways to protect the perimeter of a (cloud-based virtual) network is a decision to be taken at the architectural-level. From a cloud-platform perspective the usage of security gateways (proxy’s or reverse proxy’s) is a useful measure to enable access control to/from the internet, more specific for services which would be otherwise publicly reachable. Automated monitoring in these circumstances (i.e., cloud platform-level) might be implemented by relying on assess management systems which per-se bring their own technical complexities, in particular for hyper-scalers with global footprint.

A second typical scenario for the deployment of security gateways refers to virtual networks, which are typically used both in IaaS and some PaaS integrations[6]. Virtual networks allow cloud architects to better manage the security of associated network perimeters, in particular for internet-facing services. In these deployments it is common to find virtual network appliances[7] (e.g., security gateways) for implementing requirements like CS-04.5.

Because most virtual network appliances will rely on a pre-existing virtual network, it is possible to implement the continuous monitoring by assessing if the cloud services (IaaS or supported PaaS) is actually part of a virtual network. Despite such assessment only partially implements CS-04.5, it provides the basis to perform more complex assessments like checking for the existing of a particular virtual network appliance into the virtual network.

3.3.10 Human Resources :: Employee terms and conditions:: HR-03.5

The EUCS requirement states [2]:

> *The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.*

The requirement's description refers to the following related requirement:

HR-03.4	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof.

Typically, a CSP defines information security policies and procedures to determine an 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 [8].

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

[6] In particular when the PaaS service supports integration into a virtual network, along with traditional IaaS like virtual machines.

[7] Take for example https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices?bc=/azure/cloud-adoption-framework/_bread/toc.json&toc=/azure/cloud-adoption-framework/toc.json

the party regarding the implementation of the policy, the date when the form is signed and the signature [27].

In addition to the digital signature, the process of collection 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.

3.3.11 Human Resources :: Security awareness and training:: HR-04.7

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the completion of the security awareness and training program*

Upstream of this requirement is the fact that the employee of the CSP 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 employee has taken these courses.

Thus, a possible way to implement this requirement would be: the employee can attend a refresher course organized by the CSP online, and digitally sign an exam taken after the course.

3.3.12 Human Resources :: Termination or change in employment:: HR-05.4

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2*

The requirement's description refers to the following related requirement:

HR-05.2	The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed

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. 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 [8]. 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 [28].

For internal employees, human resources's function is typically responsible for 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 to the contract between this party and the organisation.

3.3.13 Human Resources :: Confidentiality agreements :: HR-06.7

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers*

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. It is required to ensure that 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 [8]. This is typically done before employment [29].

An NDA can be digitally signed and, in this way, 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 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 [30].

3.3.14 Identity, authentication, and access control management :: locking, unlocking and revocation of user accounts :: IAM-03.11

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03*

This requirement refers to IAM-03, which is the control:

IAM-03	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.

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[8].

Hence, compliant with IAM-03 first it is important to set up a period of time (e.g., 3 months) in which 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 (e.g., 3 months). For this, the logs of the events produced by the automated mechanisms could be monitored.

3.3.15 Identity, authentication, and access control management :: locking, unlocking and revocation of user accounts :: IAM-03.12

The EUCS requirement states [2]:

> *The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons*

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

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 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.

For the automated monitoring at least the following aspects should be considered:

- Number of authentication attempts, which can be seen from 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.

3.3.16 Incident Management :: Documentation and reporting of security incidents:: IM-03.4

The EUCS requirement states [2]:

> *The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period*

To implement this requirement, first the customers shall have the ability to review security incident solutions in a "digital" way and be able to provide feedback / approval also in a kind of a digital way.

In addition to that, the requirement states that the customer must prove the solution for a certain period of time before approving it. This proving period is not defined and shall therefore defined in the policies and procedures. The monitoring tool to be implemented shall monitor that whenever an approval process is launched for a specific customer, this customer does not approve the proposed solution until the period of time has elapsed.

For that, the CSP shall implement 1) an approval process 2) supported by an IT tool that digitally audits such approval process, and 3) that is able to monitor whenever an approval process is launched for a customer, the customer does not approve the solution until the period of time has elapsed.

3.3.17 Information security policy :: Exceptions:: ISP-03.7

The EUCS requirement states [2]:

> *An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images*

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.

3.3.18 Procurement Management :: Monitoring of compliance with requirements :: PM-04.7

The EUCS requirement PM-04.7 states [2]:

> *The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects:*
>
> - *Configuration of system components;*
> - *Performance and availability of system components;*
> - *Response time to malfunctions and security incidents; and*
> - *Recovery time (time until completion of error handling).*

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) CSPM 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, 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 [31] 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).

Also, current CSPM 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.

3.3.19 Procurement Management :: Monitoring of compliance with requirements :: PM-04.8

The requirement PM-04.8:

> *The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action.*

As in the case of PM-04.7, the deployment of a CSPM service can implement (at least partially) this PM-04.8 requirement. The vast majority of CSPM 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.

Challenges related to the implementation of PM-04.8 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-04.7, 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 to EUCS.

3.3.20 Organisation of information security :: Segregation of duties:: OIS-02.4

The EUCS requirement states [2]:

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

Usually the Access management for cloud resources is a critical function and realized by the CSP implementing a Cloud role-based access control (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 Cloud RBAC 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. The role assignment is the process (grant, change, revoke) of attaching a role definition to a security principal at a particular scope.

The role assignment is monitored by the CSP.

3.3.21 Operational security :: capacity management – monitoring:: OPS-02.3

The EUCS requirement states [2]:

> *The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1*

References as "measures" the following requirements also from OPS-02 CAPACITY MANAGEMENT – MONITORING:

OPS-02.1	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

Usually the CSP provides a Cloud Resource Manager which enables the Cloud Service Customer to view the deployment history of all cloud services which he is responsible for. The Cloud Service Customer can examine specific operations in past deployments and see which resources were provisioned and un-provisioned.

3.3.22 Operational security :: Protection against malware – implementation:: OPS-05.3

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 OPS-05.1*

References as "measures" the following requirements also from OPS-05 PROTECTION AGAINST MALWARE – IMPLEMENTATION:

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

Usually 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.

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

3.3.23 Operational security :: Protection against malware – implementation:: OPS-05.4

The EUCS requirement states [2]:

The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities

Usually the CSP shall implement an antimalware solution to identify and remove viruses, spyware, and other malicious software[9]. It shall periodically scan and monitor the activity in Cloud Services and on Virtual Machines to detect and block malware execution.

It shall automatically take action on detected malware, such as deleting or quarantining malicious files and generates alerts. This enables the Cloud Service Customer to refine the service and enable troubleshooting.

3.3.24 Operational security :: Data backup and recovery – monitoring:: OPS-07.2

The EUCS requirement states [2]:

The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1

[9] https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

References as "measures" the following requirements also from OPS-07.2 Operational Security[2]:

OPS-07.1	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-06.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery
OPS-06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08).
OPS-08.1	The CSP shall test the restore procedures at least annually
OPS-08.2	The restore tests shall assess if the specifications for the RTO and RPO agreed with the customers are met
OPS-08.3	Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation
OPS-08.4	The CSP shall inform CSCs, at their request, of the results of the recovery tests
OPS-08.5	Recovery tests shall be included in the CSP's business continuity management

Native cloud backup services offered by most CSPs (e.g., Azure backup[10] or AWS backup[11] will offer out of the box the "portal" or API functionalities which implement OPS-06 and OPS-08 (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). Therefore, a more complete implementation considers both OPS-07.2 and OPS-07.3 as complementary.

3.3.25 Operational security :: Data backup and recovery – monitoring:: OPS-07.3

The EUCS requirement states [2]:

> *The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1*

References as "measures" the following requirements also from OPS-07.2 Operational Security [2]:

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

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

OPS-07.1	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-06.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery
OPS-06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08).
OPS-08.1	The CSP shall test the restore procedures at least annually
OPS-08.2	The restore tests shall assess if the specifications for the RTO and RPO agreed with the customers are met
OPS-08.3	Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation
OPS-08.4	The CSP shall inform CSCs, at their request, of the results of the recovery tests
OPS-08.5	Recovery tests shall be included in the CSP’s business continuity management

Continuous monitoring of the data backup service offered by the CSP will assess the existence of technical configuration properties like those mentioned on OPS-06.2, 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[12]. 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-08.2), which cannot be expected to be automatically monitored at the state of practice.

3.3.26 Operational security :: Data backup and recovery – storage:: OPS-09.5

The EUCS requirement states [2]:

> *When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1*

references as “measures” the following requirements [2]:

[12] 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-09.1]	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location.
[OPS-09.2]	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).
[OPS-09.3]	The CSP shall select a remote location to store its backups concerning the distance, recovery times and the impact of disasters of both sites.
[OPS-09.4]	The physical and environmental security measures at the remote site shall have the same level as at the main site.
[CKM-02.1]	The CSP shall define and implement strong encryption mechanisms for the transmission of cloud customer data over public networks.
[CKM-02.2]	The CSP shall define and implement strong encryption mechanisms for the transmission of all data over public networks.
[OPS-08.1]	The CSP shall test the restore procedures at least annually.
[OPS-08.2]	The restore tests shall assess if the specifications for the RTO and RPO agreed with the customers are met.

Requirement OPS-09.5 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.

3.3.27 Operational security :: Logging and monitoring – identification of events :: OPS-12.4

The EUCS requirement states [2]:

> *The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1.*

references as "measures" the following requirements [2]:

[OPS-12.1]	The CSP shall monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements.

[OPS-12.3]	The monitoring of events mentioned in OPS-12.1 shall be automated.
[AM-05.1]	The CSP shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits.
[AM-05.2]	The asset classification schema shall provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.
[AM-05.3]	When applicable, the CSP shall label all assets according to their classification in the asset classification schema.

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 analyze log data on the resource, for instance on a virtual machine. The logs can then be centrally collected and analyzed.

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 analyzed 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.

3.3.28 Operational security:: Logging and monitoring – access, storage and deletion:: OPS-13.7

The EUCS requirement states [2]:

The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2

references as "measures" the following requirements:

[OPS-13.2]	Log data shall be deleted when it is no longer required for the purpose for which they were collected.
[OPS-13.5]	The CSP shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: - Access only to authorised users and systems; - Retention for the specified period; - Deletion when further retention is no longer necessary for the purpose of collection.
[OPS-10.2]	The policies and procedures shall cover at least the following aspects: - Definition of events that could lead to a violation of the protection goals; - Specifications for activating, stopping and pausing the various logs; - Information regarding the purpose and retention period of the logs;

	- Define roles and responsibilities for setting up and monitoring logging; - Time synchronisation of system components; and - Compliance with legal and regulatory frameworks.
[OPS-15.2]	Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01)

OPS-13.2 targets the management of logging and monitoring data. To fulfil this requirement, the CSP should therefore automatically monitor the effectiveness of the respective logging and monitoring mechanisms as well as incorporate changes in the monitoring configuration based on applicable policies.

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 fulfill the requirement.

For self-created logs, the agents or framework needs 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.

3.3.29 Operational security :: Managing vulnerabilities, malfunctions and errors – online registers :: OPS-18.6

The EUCS requirement states [2]:

The CSP shall equip with automatic update mechanisms 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

references as “measures” the following requirements [2]:

[OPS-18.2]	The online register shall indicate at least the following information for every vulnerability: • A presentation of the vulnerability following an industry-accepted scoring system; • A description of the remediation options for that vulnerability; • Information on the availability of updates or patches for that vulnerability; • Information about the remediation or deployment of patches or updates by the CSP or CSC, including detailed instructions for operations to be performed by the CSC.
[OPS-18.1]	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-18.3]	The CSP shall publish and maintain a list of pointers to online registers published by its subservice providers and suppliers, or integrate regularly the content of these online registers relevant to the cloud service into its own online register (cf. OPS-18.1)

[OPS-18.5]	The CSP shall consult the online registers published by its subservice providers and suppliers at least daily and update accordingly its own online register.

Unpatched assets are a major security issue in many cloud systems. OPS 18.6 therefore moves the responsibility of providing a mechanism to automate patching to the CSP.

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)[13]. In this case, a monitoring can simply check whether the respective configuration is enabled.

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 [14].

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

3.3.30 Operational security :: Managing vulnerabilities, malfunctions and errors – system hardening:: OPS-21.3

The EUCS requirement states [2]:

The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications

references as "measures" the following requirements [2]:

[OPS-21.1]	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards.
[OPS-21.2]	The hardening requirements for each system component shall be documented.

To fulfill OPS-21.3, first, a set of hardening specifications (and assets that should be hardened) needs to be defined and documented (OPS-21-2). The CSP then needs to monitor the fulfillment according to these specifications. 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.

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.

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

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

3.3.31 Physical security :: Physical site access control:: PS.02.10

The EUCS requirement states [2]:

> *The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9*

is related to another requirement [2]:

PS-02.9	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 zones
PS-02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9

Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.

In order to perform the automated monitoring of access to non-public areas by unauthorized personnel the following practices shall be considered [32]:

- 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

3.3.32 Product safety and security :: Images for virtual machines and containers:: PSS-04.3

The EUCS requirement states [2]:

> *An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images*

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 [33]. NIST 800-55 [34] standardizes the term measures for metrics to "*mean the collection, analysis, and reporting*".

Information security measures state desired performance objectives, whose goal is to be monitored in order to evaluate their accomplishment to facilitate decision-making and improve the process by applying corrective actions based on the collected and observed measurements.

Metrics can be obtained at different levels, at organizational level, at service level, at 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 by identifying principles and practices defined by policies and procedures which should be consistently implemented through the different security requirements across the organization, in spite of being the scope of being the cloud service the scope of the EUCS. Examples of this are security awareness and training, information security policies, or access control.

Metrics must be quantifiable, and they shall measure the efficiency and effectiveness of the technical and organizational measures put in place so that improvement actions can be taken in case the goals are not reached.

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 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, reals) being the most common values but also Booleans or reference values within interval (scales) are frequent. For continuous monitoring approaches such as the one in MEDINA, it is also very 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 [34]:

- **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 contributing quantifiable information to the risk management process. It can also support organizations in their decision-making since through this data they can measure success, failures, justify investments, and so on.

The definition of good metrics is of paramount importance in MEDINA as several tools depend heavily on them. Some of them include:

- The metric recommender (see D2.3 [16]): 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 D2.3 [16]): Some of the metrics defined such as M201, M203, M204, M205, M206, M207 can be mapped ontology that MEDINA has defined . This ontology offers a vendor-independent way to describe technical evidence, such as the configuration of a Cloud resource. A metric can then be applied to an evidence which then produces a measurement result. The security assessment is then putting constraints on the measurement result, e.g. assessing whether a certain measured value is compliant or not
-
- Evidence Management Tools (e.g., Clouditor, Wazuh, VAT, Codyze, NLP and organizational measures) (see D3.1 [35] and D3.4 [36]) which take this information as input to extend or develop the functionalities of the different components.

4.2 Security metrics in MEDINA

In this current version, MEDINA partners have defined more than 250 metrics covering the 33 requirements of assurance level high from the draft version of December 2020 of the candidate EUCS scheme [2]. However, some of the elicited metrics are not associated to any of said requirements but are of more generic purpose, while other metrics are associated to other requirements of lower levels, that will be of need in later stages of the project, when the operational effectiveness that is required for the requirements of the substantial level will have to be implemented.

For the elicitation of the security metrics, MEDINA consortium partners have used the following sources:

- NIST 800-55 r1 [34]
- EU funded projects such as EU FP7 CUMULUS [37], A4Cloud [38], SPECS [39]
- Literature [40], [41], [42], [43], [44]

Other metrics have been created and elicited by the MEDINA partners for the purpose of the MEDINA project, the MEDINA tools and compliant with the draft candidate scheme EUCS. It is expected that in upcoming versions of this deliverable new metrics will be defined or these ones will be updated as the result of the validation in the use cases.

The following table shows the matching between the sources and the numbers of metrics elicited from each of the sources. The metrics developed and designed in the context in MEDINA have been labelled as “EUCS”. 70% out of the MEDINA metrics have originated within the project and are specific for EUCS, which demonstrate the project’s novelty.

Table 11. Summary of metrics elicited in MEDINA per source (source: MEDINA’s own contribution)

Source of the metrics	Number of metrics
NIST 800-55 r1 [34]	19
Literature [33, [38], [39], [40], [41], [42], [43], [44]	135
EUCS (new from MEDINA)	108

The current version of the metrics can be seen in Appendix 3. The structure of the metrics as seen in the appendix is as follows:

Table 12. 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 category.
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 project has written "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. This can be: =, >, >=, …
Target Value	This is the expected value that the metric should have. This is the value to which the different medina tools (e.g. Clouditor, vat, wazuh, codyze) 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)	The interval indicates the frequency indicates how often a metric shall be collected. It can be daily, annual or event driven
Target/Asset	It states which asset of the cloud service is affected by said metric. It can be a software, a person, a resource, or the organization itself.

The following table shows the number of metrics identified per security requirement. The complete list and details can be found in Appendix 3.

Table 13. Number of identified metrics per EUCS security requirement (source: MEDINA's own contribution)

EUCS Req ID [2]	**EUCS Security Requirement** [2]	**Number of metrics**
AM01.06	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date	6
AM03.06	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.	2
AM04.04	The verification of the commitment defined in AM-04.1 shall be automatically monitored	7
CCM-03.10	The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues	1
CCM-04.3	The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1	2

EUCS Req ID [2]	**EUCS Security Requirement** [2]	**Number of metrics**
CCM-05.3	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1	5
CO-O3.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions	8
CO-O3.5	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	4
CS-04.5	The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1	8
CS-05.4	When the administration networks are not physically segregated from other networks, the administration flows must be conveyed in a strongly encrypted tunnel **(extra)**	1
HR-03.5	The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.	4
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program.	5
HR-05.4	The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2	5
HR06.7	The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers	4
IAM-03.11	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03	4
IAM-03.12	The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons	4
IAM-07.2	The access to all environments of the CSP shall be authenticated, including non-production environments **(extra)**	1
IAM-08.4	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01) **(extra)**	1
IM-03.4	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period	5
INQ-03.4	The CSP shall automatically monitor the accesses performed by or on behalf of investigators to ensure that they correspond to the determined legal basis	1
ISP-03.7	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	3

EUCS Req ID [2]	EUCS Security Requirement [2]	Number of metrics
N/A	Not in scope of EUCS for automated monitoring	91
OIS-02.4	The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.	1
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1	1
OPS.05.3	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1	2
OPS.05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	2
OPS-06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08). **(extra)**	1
OPS.07.2	The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1	1
OPS-09.2	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 sate-of-the-art (cf. CKM- 02). **(extra)**	1
OPS.07.3	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1	5
OPS-09.5	When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1	1
OPS-11.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 that govern the secure handling of derived data **(extra)**	1
OPS-12.4	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.	3

EUCS Req ID [2]	**EUCS Security Requirement** [2]	**Number of metrics**
OPS-13.3	The communication between the assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality **(extra)**	3
OPS-13.7	The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1	2
OPS-18.6	The CSP shall equip with automatic update mechanisms 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	2
OPS-21.3	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications	41
PM-04.7	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: •Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).	6
PM-04.8	The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action	4
PS02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9	3
PSS-02.1	A suitable session management system shall be used that at least corresponds to the state- of-the-art and is protected against known attacks **(extra)**	1
PSS-02.2	The session management system shall include mechanisms that invalidate a session after it has been detected as inactive. **(extra)**	1
PSS-02.3	If inactivity is detected by time measurement, the time interval shall be configurable by the CSP or – if technically possible – by the CSC **(extra)**	1
PSS-04.3	An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images	3

5 Catalogue of controls and security metrics

5.1 Functional description

The Catalogue is the software implementation of the information provided in the previous section of this deliverable. The catalogue is one of the main entry points of the MEDINA framework. Target users are mainly CSP compliance managers and auditors.

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 he can obtain all the information and guidance related to that security scheme, namely the controls, the security requirements, and the levels, that is, all what can be considered “static” information that appears in the norm. This information has been extended with all the research and implementation work performed in MEDINA such as the reference implementation TOMs, the metrics, the controls similar in other schemes, the self-assessment questionnaires or the tools that would aid in the automated monitoring and collection of evidences.

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, evidences, and assurance levels. Furthermore, it will have to provision guidance for the implementation and 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, selection of requirements from a certain framework or selection of metrics related to reference TOM.

The homogenization of the certification schemes, provision of information about related requirements from different frameworks especially referenced to the EUCS, must be provided by the Catalogue too.

The requirements satisfied by this version are described in the Table 14, and are the same requirements that can be found in D5.1 [1]. These requirements will be further polished and adapted in future stages of the project. For this reason, they can be considered as the vision of the Catalogue at this stage of the project. The table below show the status of the current prototype at M12.

Table 14. Requirements of the Catalogue (source: D5.1 [1])

Req. ID	Description	Status[15]
RCME.01	The repository shall contain a Catalogue of elements (categories, TOMs and reference implementations, controls and controls objectives, assurance levels) associated to the security control frameworks.	Satisfied
RCME.02	The repository should include realizable metrics for at least for the 70% of the TOMs referenced in major security control frameworks related to system security and	Satisfied

[15] Given the evolving nature of EUCS, which is still in a draft status, the elicitation of new metrics as well as the update of already elicited ones, as well as the update of reference TOMs, the mapping of the controls with other schemes or the new version of EUCS, etc., and, while the functionality of these requirements (RCME.01 – RCME.03) in principle has been fully satisfied the content related part will be continuously on-going.

Req. ID	Description	Status[15]
	integrity, operational security, business continuity and incident management. These include: EUCS, ISO/IEC 27002. ISO/IEC 27017, ISO/IEC 27018, ANSII SecNumCloud, BSI C5 and the ENISA Metaframework	
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.	Partially satisfied
RCME.05	The repository should be accessible by the continuous evaluation tools.	Partially 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.	Partially satisfied

5.2 Fitting into overall MEDINA Architecture

The Catalogue is one of the components of the MEDINA architecture. It interacts with other tools in the MEDINA ecosystem, as can be seen in the Figure 1 :

- **CSP Compliance manager**. It endorses new security schemes through the Catalogue (SFC) frontend.
- **Auditor.** It discovers information contained in the Catalogue based on a set of filters through the Catalogue (SFC) frontend.
- **NLCS editor**. It requests to the Catalogue the requirements and related information for a certain user.

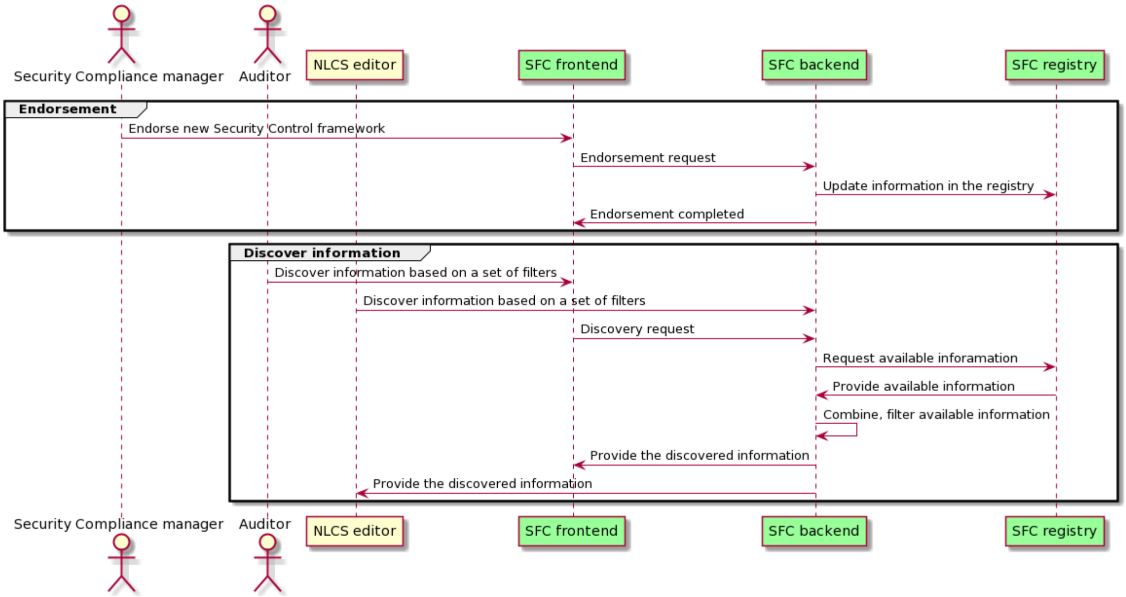
Security Compliance manager
Auditor
NLCS editor
SFC frontend
SFC backend
SFC registry
Endorsement
Endorse new Security Control framework
Endorsement request
Update information in the registry
Endorsement completed
Discover information
Discover information based on a set of filters
Discover information based on a set of filters
Discovery request
Request available inforamation
Provide available information
Combine, filter available information
Provide the discovered information
Provide the discovered information

Figure 1. Interaction of the Catalogue with other components in MEDINA.

5.3 Technical description

This subsection is devoted to describing the technical specification of this first prototype. First, the main architecture of the prototype is shown and described, including all sub-components of the prototype. Next, the data Model used by the Catalogue is presented, describing the different entities employed and its attributes. The subsection finishes with the technical specifications of the developed system.

5.3.1 Prototype architecture

The SFC architecture is based on a micro-services style which splits the front-end and the back end, so that it is easier to scale for an increasing number of users and also to survive infrastructure issues. This is also in preparation for the exploitation and sustainability. The architecture diagram is shown in Figure 2:

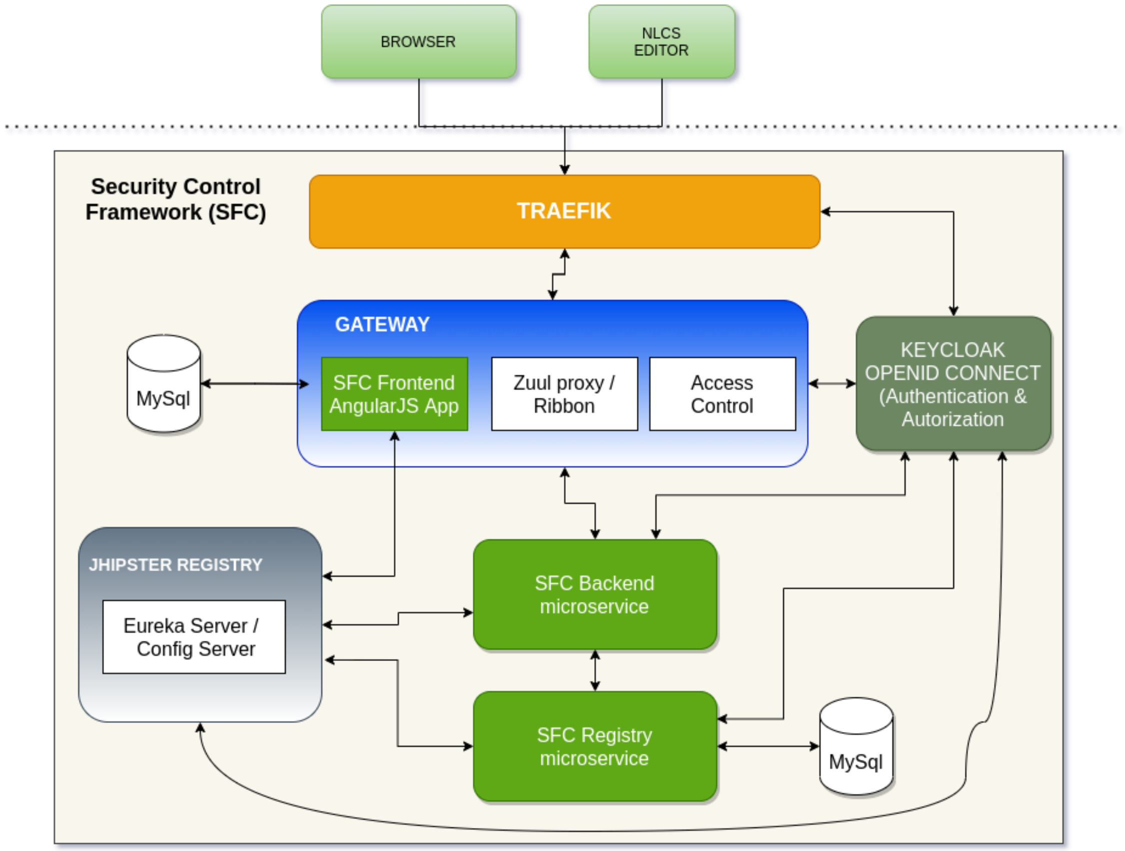
BROWSER
NLCS EDITOR
Security Control Framework (SFC)
TRAEFIK
GATEWAY
MySql
SFC Frontend AngularJS App
Zuul proxy / Ribbon
Access Control
KEYCLOAK OPENID CONNECT (Authentication & Autorization
JHIPSTER REGISTRY
Eureka Server / Config Server
SFC Backend microservice
SFC Registry microservice
MySql

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

5.3.1.1 Components description

The Catalogue is composed by three principal components, which main purpose are briefly described as follows.

- **SFC-Frontend**: This sub-component is the graphical user interface of the SFC. This SFC front-end will allow the user to indicate his 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 reference TOM, references TOMs, guidance, etc.

- **SFC-Backend**: It is the core sub-component of the Catalogue. It will perform the actual discovery of the requirements, evidences, etc. from the Security Control Frameworks registry, considering the set of filters established by the user through the UI/ API.

- **SFC-Registry**: The Security Control Frameworks registry will store the available list of Frameworks and the related info for a specific CSP. This component will also include corresponding databases.

In addition, some considerations about the other components of the SFC infrastructure:

- **Access control**. In this version, Keycloak identity and access management is used. The Keycloak instance should be deployed outside the SFC Framework in futures versions.
- **Data persistence** in MySQL database.
- **JHipster Registry**. Service discovery that uses Netflix Eureka.

5.3.2 Data Model

This data model describes the different entities (and their attributes) that will be used by the component “Catalogue of controls and security schemes". A diagram of the entities can be seen in the next figure (Figure 3his model matches the one shown in D5.1 [1]:

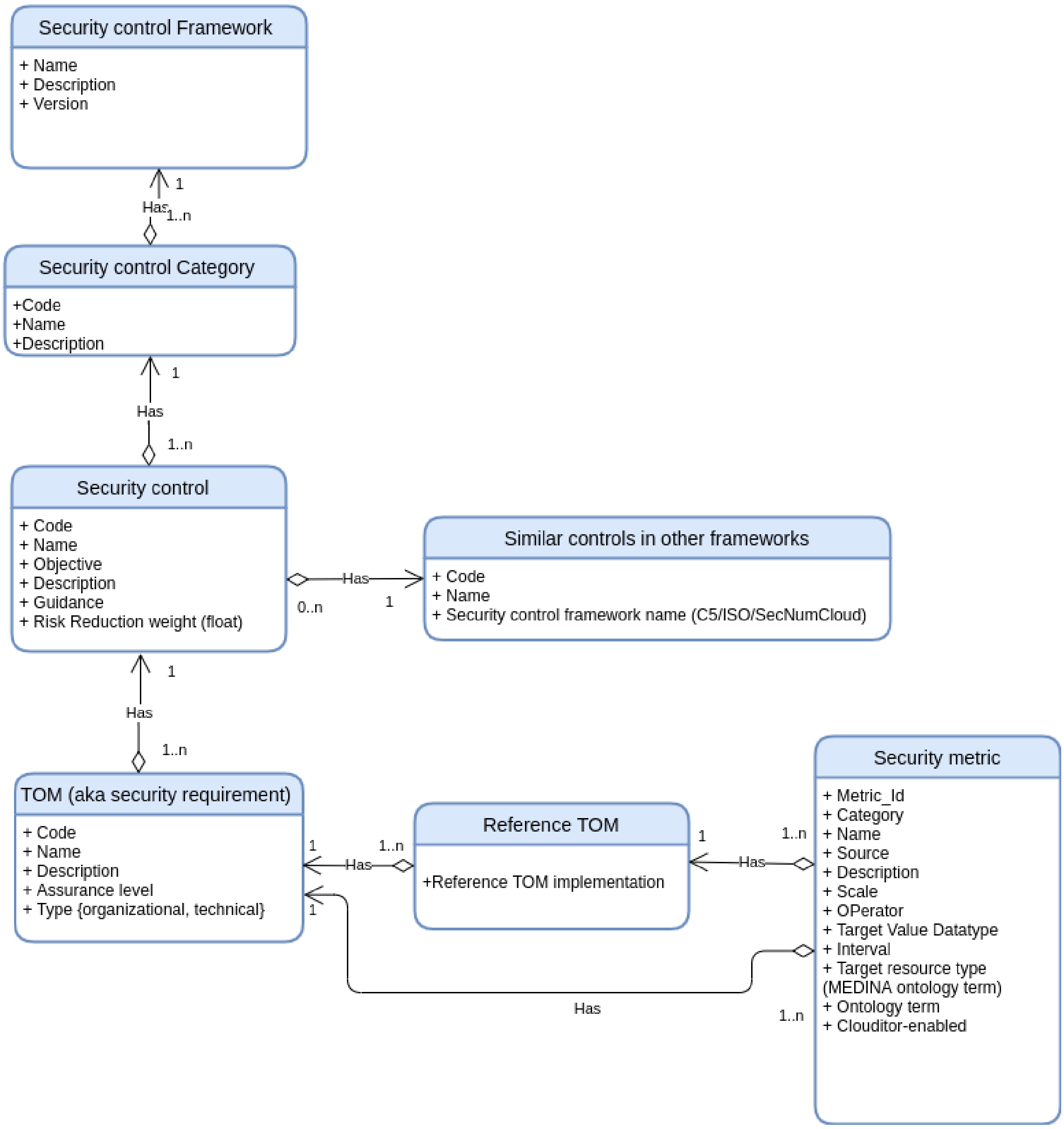

Figure 3. Data Model of the catalogue. (source D5.1 [1])

In the following, the elements that appear in the entity-relation diagram above are described. These descriptions are taken from the MEDINA glossary (see Appendix 4):

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. Examples are:

- Information Security Policies
- Personnel & Training
- Identity and Access Management
- Cryptography and Key Management

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). A security control is composed of a control ID, a control name and a control objective.

Example:

- CKM-01 POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT (from EU Cloud Services Certification Scheme)

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. In MEDINA TOM is the equivalent of a security requirement and is represented as a requirement ID, requirement objective and the associated assurance level.

Example: (from the EU Cloud Services Certification Scheme) [2]:

- 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 [2]

Reference TOM: It is a 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.

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 SP 500-307 [45]

5.3.3 Technical specifications

This prototype has been developed using the JHipster Framework.[16]

The framework provides all the needed mechanisms for a modern web application and microservice architecture.[17]

JHipster uses Spring boot for application configuration.

On the client side, SFC-Frontend gateway uses Yeoman, Webpack, Angular and Bootstrap technologies.

In the server side, SFC-Backend and SFC-Registry microservices, use Maven, Spring, Spring MVC REST, Spring Data JPA and Netflix OSS.[18]

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

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

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

6 Conclusions

This deliverable has presented the initial version of the catalogue of TOMs and security metrics.

The document starts with a comparative analysis of four schemes, namely EUCS, ISO/IEC 27000 family (27002, 27017), BSI C5 and SecNumCloud, in different dimensions such as the categories, the structure, the levels and the conformity assessment method, as well as the mapping of the controls among the different schemes.

The second goal this document is to present a set of reference technical and organizational measures for the 33 requirements identified with the assurance level high in the version of December 2020 of the European draft candidate EUCS. A reference TOM is a sort of implementation guidance that is vendor and technology agnostic.

The third goal of this document is the definition of the MEDINA catalogue of security metrics, which lie at the core of the project as most of the tools rely heavily on them. More than 250 metrics have been elicited at this stage, coming from literature and other European projects but also from MEDINA partners themselves. All metrics have been described following the same structure; whose details can be seen in Appendix 3. They all have a defined data type, data range, interval, and formula. While most metrics are linked to a requirement of assurance level high, there are some that are either of a more general purpose or compliant with a requirement of a lower level of assurance, that however are relevant at this stage because they are needed to measure the operational effectiveness required in the substantial level of assurance.

The document includes the functional and technical design of the first version of the software implementation of the MEDINA catalogue. The current version includes the implementation of three core requirements, which will be extended in future versions.

The deliverable includes five appendices complementing the previous sections.

The next version of this document (M27) will contain updated versions of the mapping as it is expected that the EUCS will evolve (it is currently under revision), new and updated TOMs as well as new and updated metrics. It will also include the final version of the software component of the catalogue.

7 References

[1] MEDINA Consortium, “D5.1 MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v1,” 2021.

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

[3] 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.

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

[5] 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.

[6] 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 July 2020].

[7] ANSSI, “SecNumCloud – Referentiel,” ANSSI, 2018. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf.

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

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

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

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

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

[13] 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.

[14] 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.

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

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

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

[18] Fugue, "Fugue," [Online]. Available: https://www.fugue.co/cloud-security-posture-management.

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

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

[21] 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.

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

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

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

[25] MITRE, “DevSecOps – Security and Test Automation,” 2019. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-19-0769-devsecops_security_test_automation-briefing.pdf.

[26] ITU, “Cloud computing – Requirements for cloud service development and operation management,” [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3525-202009-I!!PDF-E&type=items.

[27] 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/.

[28] 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.

[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 .

[30] 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 .

[31] 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.

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

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

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

[35] MEDINA Consortium;, “D3.1-Tools and techniques for the management of trustworthy evidence-v1,” 2021.

[36] MEDINA Consortium;, “D3.4-Tools and techniques for collecting evidence of technical and organisational measures-v1,” 2021.

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

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

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

[40] 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.

[41] 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.

[42] 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.

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

[44] Center for Internet Security, “Center for Internet Security,” [Online]. Available: https://www.cisecurity.org/.

[45] NIST, “NIST 500-307 Cloud Computing Service Metrics Description,” [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-307.pdf.

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

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

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

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

[50] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations - NIST Special Publication 800-53. rev 4,” 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Appendix 1: Changelog C5:2016 vs. C5:2020

Table 15. Changelog C5:2016 vs. C5:2020

Area	C5:2016	C5:2020
Organisation of Information Security (OIS)	OIS-01	OIS-01
Organisation of Information Security (OIS)	OIS-02	OIS-02
Organisation of Information Security (OIS)	OIS-03	OIS-03
Organisation of Information Security (OIS)	OIS-04	OIS-04
Organisation of Information Security (OIS)	OIS-05	OIS-05
Organisation of Information Security (OIS)	OIS-06	OIS-06
Organisation of Information Security (OIS)	OIS-07	OIS-07
Security Policies and Instructions (SP)	SA-01	SP-01
Security Policies and Instructions (SP)	SA-02	SP-02
Security Policies and Instructions (SP)	SA-03	SP-03
Personnel (HR)	HR-01	HR-01
Personnel (HR)	HR-02	HR-02
Personnel (HR)	HR-03	HR-03
Personnel (HR)	HR-04	HR-04
Personnel (HR)	HR-05	HR-05
Personnel (HR)	KOS-08	HR-06
Asset Management (AM)	AM-01	AM-01
	AM-02	
	MDM-01	
Asset Management (AM)	AM-03	AM-02
	AM-05	
	AM-06	
	MDM-01	
Asset Management (AM)	-	AM-03
Asset Management (AM)	-	AM-04
Asset Management (AM)	AM-04	AM-05
	MDM-01	
Asset Management (AM)	AM-05	AM-06
	AM-06	
Physical Security (PS)	-	PS-01
Physical Security (PS)	-	PS-02
Physical Security (PS)	PS-01	PS-03
Physical Security (PS)	PS-02	PS-04
Physical Security (PS)	PS-03	PS-05
Physical Security (PS)	PS-04	PS-06
	BCM-05	
Physical Security (PS)	-	PS-07
Operations (OPS)	RB-01	OPS-01
Operations (OPS)	RB-02	OPS-02
Operations (OPS)	RB-04	OPS-03
Operations (OPS)	RB-05	OPS-04
Operations (OPS)	RB-05	OPS-05
Operations (OPS)	RB-06	OPS-06
Operations (OPS)	RB-07	OPS-07
Operations (OPS)	RB-08	OPS-08
Operations (OPS)	RB-09	OPS-09

Area	C5:2016	C5:2020
Operations (OPS)	RB-10	OPS-10
Operations (OPS)	RB-11	OPS-11
Operations (OPS)	-	OPS-12
Operations (OPS)	RB-12	OPS-13
	SIM-05	
Operations (OPS)	RB-13	OPS-14
Operations (OPS)	RB-14	OPS-15
Operations (OPS)	RB-15	OPS-16
Operations (OPS)	RB-16	OPS-17
Operations (OPS)	RB-17	OPS-18
Operations (OPS)	RB-18	OPS-19
Operations (OPS)	RB-19	OPS-20
Operations (OPS)	RB-20	OPS-21
Operations (OPS)	RB-21	OPS-22
Operations (OPS)	RB-22	OPS-23
Operations (OPS)	RB-23	OPS-24
Identity and Access Management (IDM)	IDM-01	IDM-01
Identity and Access Management (IDM)	IDM-02	IDM-02
	IDM-03	
Identity and Access Management (IDM)	-	IDM-03
Identity and Access Management (IDM)	IDM-04	IDM-04
Identity and Access Management (IDM)	IDM-05	IDM-05
Identity and Access Management (IDM)	IDM-06	IDM-06
	IDM-12	
Identity and Access Management (IDM)	-	IDM-07
Identity and Access Management (IDM)	IDM-07	IDM-08
Identity and Access Management (IDM)	IDM-08	IDM-09
	IDM-11	
-	IDM-12	-
-	IDM-13	-
Cryptography and Key Management (CRY)	KRY-01	CRY-01
Cryptography and Key Management (CRY)	KRY-02	CRY-02
Cryptography and Key Management (CRY)	KRY-03	CRY-03
Cryptography and Key Management (CRY)	KRY-04	CRY-04
Communication Security (COS)	KOS-01	COS-01
Communication Security (COS)	-	COS-02
Communication Security (COS)	KOS-02	COS-03
Communication Security (COS)	KOS-03	COS-04
Communication Security (COS)	KOS-04	COS-05
Communication Security (COS)	KOS-05	COS-06
Communication Security (COS)	KOS-06	COS-07
Communication Security (COS)	KOS-07	COS-08
Portability and Interoperability (PI)	PI-01	PI-01
	PI-04	
Portability and Interoperability (PI)	PI-02	PI-02
	PI-03	
Portability and Interoperability (PI)	PI-05	PI-03
Procurement, Development and Modification of Information Systems (DEV)	BEI-01	DEV-01

Area	C5:2016	C5:2020
Procurement, Development and Modification of Information Systems (DEV)	BEI-02	DEV-02
Procurement, Development and Modification of Information Systems (DEV)	BEI-03	DEV-03
Procurement, Development and Modification of Information Systems (DEV)	-	DEV-04
Procurement, Development and Modification of Information Systems (DEV)	BEI-04	DEV-05
	BEI-05	
	BEI-06	
Procurement, Development and Modification of Information Systems (DEV)	BEI-07	DEV-06
Procurement, Development and Modification of Information Systems (DEV)	IDM-13	DEV-07
Procurement, Development and Modification of Information Systems (DEV)	BEI-08	DEV-08
Procurement, Development and Modification of Information Systems (DEV)	BEI-09	DEV-09
-	BEI-10	-
Procurement, Development and Modification of Information Systems (DEV)	BEI-11	DEV-10
-	BEI-12	-
Control and Monitoring of Service Providers and Suppliers (SSO)	DLL-01	SSO-01
Control and Monitoring of Service Providers and Suppliers (SSO)	-	SSO-02
Control and Monitoring of Service Providers and Suppliers (SSO)	-	SSO-03
Control and Monitoring of Service Providers and Suppliers (SSO)	DLL-02	SSO-04
Control and Monitoring of Service Providers and Suppliers (SSO)	-	SSO-05
Security Incident Management (SIM)	SIM-01	SIM-01
Security Incident Management (SIM)	SIM-02	
Security Incident Management (SIM)	SIM-03	SIM-02
Security Incident Management (SIM)	SIM-04	SIM-03
Security Incident Management (SIM)	SIM-06	SIM-04
Security Incident Management (SIM)	SIM-07	SIM-05
Business Continuity Management (BCM)	BCM-01	BCM-01
Business Continuity Management (BCM)	BCM-02	BCM-02
Business Continuity Management (BCM)	BCM-03	BCM-03
Business Continuity Management (BCM)	BCM-04	BCM-04
Compliance (COM)	COM-01	COM-01
Compliance (COM)	COM-02	COM-02
Compliance (COM)	SPN-02	COM-03
	SPN-03	
	COM-03	
Compliance (COM)	SPN-01	COM-04
Dealing with investigation requests from government agencies (INQ)	-	INQ-01
Dealing with investigation requests from government agencies (INQ)	-	INQ-02
Dealing with investigation requests from government agencies (INQ)	-	INQ-03
Dealing with investigation requests from government agencies (INQ)	-	INQ-04
Product Safety and Security (PSS)	-	PSS-01
Product Safety and Security (PSS)	-	PSS-02
Product Safety and Security (PSS)	-	PSS-03

Area	C5:2016	C5:2020
Product Safety and Security (PSS)	-	PSS-04
Product Safety and Security (PSS)	-	PSS-05
Product Safety and Security (PSS)	-	PSS-06
Product Safety and Security (PSS)	IDM-07	PSS-07
Product Safety and Security (PSS)	-	PSS-08
Product Safety and Security (PSS)	IDM-09	PSS-09
Product Safety and Security (PSS)	-	PSS-10
Product Safety and Security (PSS)	-	PSS-11
Product Safety and Security (PSS)	RB-03	PSS-12

Appendix 2: Security Requirements relevant for continuous assessment – Description

Domain:	A.5
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 Cloud Service Provider has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.
ReqID:	AM-01.6
Requirement:	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date
Assurance Level:	High

Domain:	A.5
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:	The Cloud Service Provider has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the cloud service in the production environment, depending on its intended use and based on the applicable policies and procedures.
ReqID:	AM-03.6
Requirement:	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.
Assurance Level:	High

Domain:	A.5
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 Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service.
ReqID:	AM-04.4
Requirement:	The verification of the commitment defined in AM-04.1 shall be automatically monitored.
Assurance Level:	High

Domain:	A.12
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-03
Control:	TESTING CHANGES
Control Objective:	Changes to the cloud services are tested before deployment to minimize the risks of failure upon implementation.
ReqID:	CCM-03.10
Requirement:	The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues
Assurance Level:	High

Domain:	A.12
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-04.3
Requirement:	The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1
Assurance Level:	High

Domain:	A.12
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-05.3
Requirement:	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1
Assurance Level:	High

Domain:	A.17
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-03.4
Requirement:	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions.
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 internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the CSP’s code of ethics, before being granted access to any cloud customer data or system components under the responsibility of the CSP used to provide the cloud service in the production environment.
ReqID:	HR-03.5
Requirement:	The verification of the acknowledgement defined in HR-03.4 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 internal and external employees of the CSP on a regular basis.
ReqID:	HR-04.7
Requirement:	The CSP 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-05.4
Requirement:	The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2
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 internal employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them.
ReqID:	HR-06.7
Requirement:	The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers
Assurance Level:	High

Domain:	A.8
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-03.11
Requirement:	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03
Assurance Level:	High

Domain:	A.8
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-03.12
Requirement:	The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons

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-03
Control:	Documentation and reporting of security incidents
Control Objective:	Security incidents are documented to and reported in a timely manner to customers.
ReqID:	IM-03.4
Requirement:	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period
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-03.7
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:	A.1
Category:	ORGANISATION OF INFORMATION SECURITY
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-02.4
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:	A.7
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 personnel and IT resources are monitored.

ReqID:	OPS-02.3
Requirement:	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1
Assurance Level:	High

Domain:	A.7
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-05.3
Requirement:	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1
Assurance Level:	High

Domain:	A.7
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-05.4
Requirement:	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities
Assurance Level:	High

Category:	Operational Security
Domain:	A7
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-07.2
Requirement:	The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1
Assurance level:	High

Category:	Operational Security
Domain:	A7

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-07.3
Requirement:	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1
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-09.5
Requirement:	When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1
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-12.4
Requirement:	The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1
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-13.7

Requirement:	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2
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-18.6
Requirement:	The CSP shall equip with automatic update mechanisms 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-21.3
Requirement:	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications
Assurance Level:	High

Domain:	A.6
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 zone's security requirements and that are supported by an access control system.
ReqID:	PS-02.10
Requirement:	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9
Assurance Level:	High

Domain:	A.14
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-04.7
Requirement:	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).
Assurance Level:	High

Domain:	A.14
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-04.8
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 Cloud Service Provider for prompt assessment and action.
Assurance Level:	High

Domain:	A.20
Category:	PRODUCT SAFETY AND 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-04.3
Requirement:	An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images
Assurance Level:	High

Appendix 3: MEDINA Security metrics

Table 16. MEDINA Security metrics (source: MEDINA's own contribution)

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M1	N/A	Not in scope of EUCS for automated monitoring	Security budget measure	NIST SP800-55 v1	Percentage (%) of the agency's information system budget devoted to information security from the formula of (Information security budget/total agency information technology budget) *100	[1;100]	=	n/a	integer/real	Annual	Organization
M2	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Vulnerability Measure	NIST SP800-55 v1	Percentage (%) of high-risk vulnerabilities mitigated within organizationally defined time periods after discovery from the formula of (Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) *100	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management
M3	CS-04.5	CROSS-NETWORK ACCESS	Remote Access Control Measure	NIST SP800-55 v1	Percentage (%) of remote access points used to gain unauthorized access from the formula of (Number of remote access points used to gain unauthorized access/total number of remote access points) *100.	[1;100]	=	0	integer/real	daily	Resources that support remote access for privileged tasks

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M4	HR-04.7	SECURITY AWARENESS AND TRAINING	Security Training Measure	NIST SP800-55 v1	Percentage (%) of information system security personnel that have received security training from the formula of (Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) *100	[1;100]	=	100	integer/real	daily	Personnel
M5	CO-03.4	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	Audit Record Review Measure	NIST SP800-55 v1	Average frequency of audit records review and analysis for inappropriate activity	[1;365]	=	1	integer/real	daily	Resources which generate audit events
M6	CO-03.4	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	C&A Completion Measure	NIST SP800-55 v1	Percentage (%) of new systems that have completed certification and accreditation (C&A) prior to their implementation from the formula of (Number of new systems with complete C&A packages with Authorizing Official [AO] approval prior to implementation)/(total number of new systems) *100	[1;100]	=	100	integer/real	daily	Cloud services in the scope of EUCS

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M7	CCM-05.3	PERFORMING AND LOGGING CHANGES	Configuration Changes Measure	NIST SP800-55 v1	Percentage (%) approved and implemented configuration changes identified in the latest automated baseline configuration from the formula of (Number of approved and implemented configuration changes identified in the latest automated baseline configuration/total number of configuration changes identified through automated scans) *100	[1;100]	=	100	integer/real	daily	Resouces supporting automation of configuration management tasks
M8	N/A	Not in scope of EUCS for automated monitoring	Contingency Plan Testing Measure	NIST SP800-55 v1	Percentage (%) of information systems that have conducted annual contingency plan testing from the formula of (Number of information systems that have conducted annual contingency plans testing/number of information systems in the system inventory) *100	[1;100]	=	100	integer/real	Annual	Resources with a contingency plan in place
M9	N/A	Not in scope of EUCS for automated monitoring	User Accounts Measure	NIST SP800-55 v1	Percentage (%) of users with access to shared accounts from the formula of (Number of users with access to shared accounts/total number of users)*100	[1;100]	=	0	integer/real	daily	Personnel

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M10	IM-03.4	DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS	Incident Response Measure	NIST SP800-55 v1	Percentage (%) of incidents reported within required time frame per applicable incident category (the measure will be computed for each incident category described in Implementation Evidence) from the formula of (number of incidents reported on time/total number of reported incidents) *100	[1;100]	=	0	integer/real	daily	Personnel
M11	AM-01.6	ASSET INVENTORY	Maintenance Measure	NIST SP800-55 v1	Percentage (%) of system components that undergo maintenance in accordance with formal maintenance schedules from the formula of (Number of system components that undergo maintenance according to formal maintenance schedules/total number of system components) *100	[1;100]	=	100	integer/real	daily	Resources with a maintenance plan in place
M12	AM-01.6	ASSET INVENTORY	Media Sanitization Measure	NIST SP800-55 v1	Percentage (%) of media that passes sanitization procedures testing for FIPS 199 high- impact systems from the formula of (Number of media that passes sanitization procedures testing/total number of media tested) * 100	[1;100]	=	100	integer/real	daily	Resources with a sanitization plan in place, and where FIPS 199 applies

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M13	PS-02.10	PHYSICAL SITE ACCESS CONTROL	Physical Security Incidents Measure	NIST SP800-55 v1	Percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems from the formula of (Number of physical security incidents allowing unauthorized entry into facilities containing information systems/total number of physical security incidents) *100	[1;100]	=	0	integer/real	daily	CSP premises
M14	HR-03.5	EMPLOYEE TERMS AND CONDITIONS	Planning Measure	NIST SP800-55 v1	Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior from the formula of (Number of users who are granted system access after signing rules of behavior/total number of users with system access) *100	[1;100]	=	100	integer/real	daily	Personnel
M15	HR-03.5	EMPLOYEE TERMS AND CONDITIONS	Personnel Security Screening Measure	NIST SP800-55 v1	Percentage (%) of individuals screened before being granted access to organizational information and information systems from the formula of (Number of individuals screened/total number of individuals with access) *100.	[1;100]	=	100	integer/real	daily	Personnel with priviledge access

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M16	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Risk Assessment Vulnerability Measure	NIST SP800-55 v1	Percentage (%) of vulnerabilities remediated within organization-specified time frames from the formula of (Number of vulnerabilities remediated according to POA&M schedule/total number of POA&M-documented vulnerabilities identified through vulnerability scans) *100.	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management
M17	AM-04.4	ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS	Service Acquisition Contract Measure	NIST SP800-55 v1	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications from the formula of (Number of system and service acquisition contracts that include security requirements and specifications/total number of system and service acquisition contracts) *100	[1;100]	=	100	integer/real	daily	Resources considered IT security-relevant

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M18	N/A	Not in scope of EUCS for automated monitoring	System and Communication Protection Measure	NIST SP800-55 v1	Percentage of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation from the formula of (Number of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation/total number of mobile computers and devices)*100	[1;100]	=	100	integer/real	daily	Resouces supporting FIPS 140-2
M19	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	System and Information Integrity Measure	NIST SP800-55 v1	Percentage (%) of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated from the formula of (Number of vulnerabilities addressed in distributed alerts and advisories for which patches have been implemented, determined as non-applicable, or granted a waiver/total number of applicable vulnerabilities identified through alerts and advisories and through vulnerability scans) *100	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M20	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Mean Time to Deploy Critical Patches	The Center for Internet Security	Mean Time to Patch Deploy Patches (MTPCP) taken to deploy a critical patch to the organization's technologies. The sooner critical patches can be deployed, the lower the mean time to patch and the less time the organization spends with systems in a state known to be vulnerable. In order for managers to better understand the exposure of their organization to vulnerabilities, Mean Time to Deploy Critical Patches should be calculated for the scope of patches with Patch Criticality levels of "Critical". This metric result, reported separately provides more insight than a result blending all patch criticality levels as seen in the Mean Time to Patch metric.	[1;7]	=	3	integer/real	daily	Resources that support vulnerability management

M21	OPS-21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Percent of Systems Without Known Severe Vulnerabilities	The Center for Internet Security	Percent of Systems Without Known Severe Vulnerabilities (PSWKSV) measures the percentage of systems that when checked were not found to have any known high severity vulnerabilities during a vulnerability scan. Vulnerabilities are defined as “High" severity if they have a CVSS base score of 7.0-10.0 Since vulnerability management involves both the identification of new severe vulnerabilities and the remediation of known severe vulnerabilities, the percentage of systems without known severe vulnerabilities will vary overtime. Organizations can use this metric to gauge their relative level of exposure to exploits and serves as a potential indicator of expected levels of security incidents (and therefore impacts on the organization). This severity threshold is important, as there are numerous informational, local, and exposure vulnerabilities that can be detected that are not necessarily material to the organization’s risk profile. Managers generally will want to reduce the level of noise to focus on the greater risks first. This metric can also be calculated for subsets of systems, such as by asset criticality of business unit.	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M22	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Mean-Time to Mitigate Vulnerabilities	The Center for Internet Security	Mean-Time to Mitigate Vulnerabilities measures the average time taken to mitigate vulnerabilities identified in an organization's technologies. The vulnerability management processes consist of the identification and remediation of known vulnerabilities in an organization's environment. This metric is an indicator of the performance of the organization in addressing identified vulnerabilities. The less time required to mitigate a vulnerability the more likely an organization can react effectively to reduce the risk of exploitation of vulnerabilities. It is important to note that only data from vulnerabilities explicitly mitigated are is included in this metric result. The metric result is the mean time to mitigate vulnerabilities that are actively addressed during the metric time period, and not a mean time to mitigate based on the time for all known vulnerabilities to be mitigated.	[1;31]	=	15	integer/real	daily	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M23	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Mean Cost to Mitigate Vulnerabilities	The Center for Internet Security	The goal of this metric is to understand the effort required for vulnerability remediation activities. Risk management decisions can take into account the efficiency of vulnerability remediation and make more informed decisions around vulnerability policies, SLAs, and resource allocation in the IT environment.	>=0	>=	n/a	integer/real	monthly	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M24	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Patch Policy Compliance	The Center for Internet Security	Patch Policy Compliance (PPC) measures an organization’s patch level for supported technologies as compared to their documented patch policy. “Policy” refers to the patching policy of the organization, more specifically, which patches are required for what type of computer systems at any given time. This policy might be as simple as “install the latest patches from system vendors” or maybe more complex to account for the criticality of the patch or system. “Patched to policy” reflects an organization’s risk/reward decisions regarding patch management. It is not meant to imply that all vendor patches are immediately installed when they are distributed.	[TRUE; FALSE]	=	TRUE	Boolean	monthly	Resources that support patch management
M25	CCM - 05.3	PERFORMING AND LOGGING CHANGES	Percent of Changes with Security Review	The Center for Internet Security	This metric indicates the percentage of configuration or system changes that were reviewed for security impacts before the change was implemented.	[1;100]	=	100	integer/real	daily	Resources supporting automation of configuration management tasks

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M26	CO-03.4	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	Risk Assessment Coverage	The Center for Internet Security	Risk assessment coverage indicates the percentage of business applications that have been subject to a risk assessment at any time.	[1;100]	=	100	integer/real	monthly	Resources used for business applications
M27	CCM-03.10	TESTING CHANGES	Security Testing Coverage	The Center for Internet Security	This metric tracks the percentage of applications in the organization that have been subjected to security testing. Testing can consist of manual or automated white and/or black-box testing and generally is performed on systems post-deployment (although they could be in pre-production testing). Studies have shown that there is material differences in the number and type of application weaknesses found. As a result, testing coverage should be measured separately from risk assessment coverage.	[1;100]	=	100	integer/real	monthly	Resources with a security testing plan in place
M28	N/A	Not in scope of EUCS for automated monitoring	Number of Incidents	The Center for Internet Security	Number of Incidents measures the number of security incidents for a given time period.	>=0	=	0	integer/real	daily	All resources

M29	CCM - 05.3	PERFORMING AND LOGGING CHANGES	Configuration Management Coverage	The Center for Internet Security	This metric attempts to answer the question “Are system under configuration management control?” This question presumes the organization has a configuration management system to test and monitor the configuration states of systems. The percentage of total computer systems in an organization that are under the scope of a configuration monitoring /management system. Scope of configuration monitoring is a binary evaluation: a given system is either part of a system that can assess and report its configuration state or it is not. Configuration state can be evaluated by automated methods, manual inspection, or audit, or some combination. The computer system population base is the total number of computer systems with approved configuration standards. This maybe all systems or only a subset (i.e. only desktops, or only servers, etc.) Organizations that do not have approved standards for their computer systems should report “N/A” rather than a numeric value (0% or 100%). In Scope Examples of percentage of systems	[1;100]	=	100	integer/real	daily	Resouces supporting automation of configuration management tasks

					under configuration management may include: l Configuration of servers l Configuration of workstations/laptops l Configuration of hand-held devices l Configuration of other supported computer systems covered by the _x000B_organizations configuration policy Out of Scope Examples of computer system configurations that are not in scope include: l Temporary guest systems (contractors, vendors) l Lab/test systems performing to or in support of a specific non-production project l Networking systems (routers, switches, access points) l Storage systems (i.e. network accessible storage)						

M30	OPS-05.3	PROTECTION AGAINST MALWARE – IMPLEMENTATION	Current Anti-Malware Coverage	The Center for Internet Security	This metric attempts to answer the question “Do we have acceptable levels of anti-malware coverage?” This question presumes the organization has defined what an acceptable level of compliance is, which may be less than 100% to account for ongoing changes in the operational environments. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crime ware and other malicious and unwanted software. The percentage of total computer systems in an organization that have current, up-to-date anti-virus (or anti-malware) software and definition files. “Current” is a binary evaluation: a given system is either configured with both up-to-date detection engines and signatures or it is not. Compliance can be evaluated by automated methods, manual inspection, audit, or some combination. Current coverage of a system is defined as a the most recent version of the engine, and a signature file that is no more than14 days older than the most recent signature file released. In Scope_x000B_ Examples of systems under considerations for this metric include: l Servers _x000B_	[1;100]	=	100	integer/real	daily	Resources that support antimalware solutions

					l Work stations/laptops _x000B_ l Hand-held devices _x000B_ l Other supported computer systems _x000B_ Out of Scope_x000B_ Examples of systems that are not under consideration for this metric include: _x000B_ l Temporary guest systems (contractors, vendors) _x000B_ l Lab/test systems performing to or in support of a specific non-production project _x000B_ l Networking systems (routers, switches, access points) _x000B_ l Storage systems(i.e. network accessible storage) _x000B_						

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M31	AM-01.6	ASSET INVENTORY	Number of Applications	The Center for Internet Security	This metric counts the number of applications in the organization's environment.	>=0	=	n/a	integer/real	daily	Resources used for business applications

M32	N/A	Not in scope of EUCS for automated monitoring	Cost of Incidents	The Center for Internet Security	Cost of Incidents (COI) measures the total cost to the organization from security incidents occurring during the metric time period. Total costs from security incidents consists of the following costs: l Direct Loss Value of IP, customer lists, trade secrets, or other assets that_x000B_are destroyed _x000B_ l Cost of Business System Downtime Cost of refunds for failed transactions Cost of lost business directly attributable to the incident _x000B_ l Cost of Containment _x000B_ Efforts and cost Consulting services _x000B_ l Cost of Recovery Cost of incident investigation and analysis Effort required to repair and replace systems Replacement cost of systems Consulting services for repair or investigation Additional costs not covered by an insurance policy _x000B_ l Cost of Restitution_x000B_ Penalties and other funds paid out due to breaches of Contacts or SLAs resulting from the incident_x000B_ Cost of services provided to customers as a direct result of the incident (e.g. ID	>=0	=	n/a	integer/real	daily	Organization

					Theft Insurance)_x000B_ Public relations costs Cost of disclosures and notifications Legal costs, fines, and settlements						

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M33	N/A	Not in scope of EUCS for automated monitoring	Mean Time to Incident Discovery	The Center for Internet Security	Mean-Time-To-Incident-Discovery (MTTID) measures the effectiveness of the organization in detecting security incidents. Generally, the faster an organization can detects an incident, the less damage it is likely to incur. MTTID is the average amount of time in hours that elapsed between the Date of Occurrence and the Date of Discovery for a given set of incidents. The calculation can be averaged across a time period, type of incident, business unit, or severity.	>=0	=	n/a	integer/real	daily	Organization
M34	N/A	Not in scope of EUCS for automated monitoring	Mean Time Between Security Incidents	The Center for Internet Security	Mean Time Between Security Incidents (MTBSI) calculates the average time, in days, between security incidents. This metric is analogous to the Mean Time Between Failure (MTBF) metric found in break-fix processes for data center.	>=0	=	n/a	integer/real	daily	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M35	N/A	Not in scope of EUCS for automated monitoring	Mean Time to Incidence Recovery	The Center for Internet Security	Mean Time to Incident Recovery (MTIR) measures the effectiveness of the organization to recovery from security incidents. The sooner the organization can recover from a security incident, the less impact the incident will have on the overall organization. This calculation can be averaged across a time period, type of incident, business unit, or severity.	>=0	=	n/a	integer/real	daily	Organization

M36	N/A	Not in scope of EUCS for automated monitoring	Mean Cost of Incidence	The Center for Internet Security	Mean Cost of Incidents (MCOI) measures the mean cost to the organization from security incidents identified relative to the number of incidents that occurred during the metric time period. Total costs from security incidents consists of the following costs: l Direct Loss Value of IP, customer lists, trade secrets, or other assets that_x000B_are destroyed _x000B_ l Cost of Business System Downtime Cost of refunds for failed transactions Cost of lost business directly attributable to the incident _x000B_ l Cost of Containment _x000B_ Efforts and cost Consulting services _x000B_ l Cost of Recovery Cost of incident investigation and analysis Effort required to repair and replace systems Replacement cost of systems Consulting services for repair or investigation Additional costs not covered by an insurance policy _x000B_ l Cost of Restitution_x000B_ Penalties and other funds paid out due to breaches of Contacts or SLAs resulting from the incident_x000B_	>=0	=	n/a	integer/real	daily	Organization

					Cost of services provided to customers as a direct result of the incident (e.g. ID Theft Insurance)_x000B_ Public relations costs Cost of disclosures and notifications Legal costs, fines, and settlements						

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M37	N/A	Not in scope of EUCS for automated monitoring	Mean Incident Recovery Cost	The Center for Internet Security	Mean Incident Recovery Cost (MIRC) measures the cost of returning business systems to their pre-incident condition. The following costs may be taken into consideration: l Cost to repair and/or replace systems _x000B_ l Opportunity cost of staff implementing incident handling plan _x000B_ l Cost to hire external technical consultants to help recover from the_x000B_incident _x000B_ l Cost to installation new controls or procurement of new resources that directly addresses there-occurrence of the incident (e.g. _x000B_installation of AV software) _x000B_ l Legal and regulatory liabilities resulting from the incident _x000B_	>=0	=	n/a	integer/real	daily	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M38	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Mean Time to Patch	The Center for Internet Security	Mean Time to Patch (MTTP) measures the average time taken to deploy a patch to the organization's technologies. The more quickly patches can be deployed, the lower the meantime to patch and the less time the organization spends with systems in a state known to be vulnerable.	[1;31]	=	7	integer/real	daily	Resources that support patch management
M39	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Mean Cost to Patch	The Center for Internet Security	The goal of this metric is to understand the effort required for patch management activities. Risk management decisions can take into account the efficiency of patch deployment to make more informed decisions around patch compliance policies, Service Level Agreements, and resource allocation in the IT environment.	>=0	=	n/a	integer/real	daily	Organization

M40	PM-04.7	MONITORING OF COMPLIANCE WITH REQUIREMENTS	Percentage of Configuration Compliance	The Center for Internet Security	This document defines a metric for the effectiveness of configuration management in the context of information security. A percentage metric will allow benchmarking across organizations. This metric attempts to answer the question “Are system configuration compliance levels acceptable?” This question presumes the organization has defined an acceptable level of compliance, which may be less than 100% to account for the realities of ongoing change in the operational environments. The percentage of total computer systems in an organization that are configured in compliance with the organizations’ approved standards. Compliance is a binary evaluation: a given system is either configured correctly according to the standard or it is not. Compliance can be evaluated by automated methods, manual in spection, audit, or some combination. The computer system population base is the total number of computer systems with approved configuration standards. This may be all systems or only a subset (i.e. only desktops, or only servers, etc.) The Configuration benchmark used is the CIS benchmarks if available	[1;100]	=	100	integer/real	daily	Resouces supporting automation of configuration management tasks

					(http://cisecurity.org). Additional metric results can be calculated for other or internal configuration benchmarks. Organizations that do not have approved standards for their computer systems should report “N/A” rather than a numeric value (0% or 100%) In Scope_x000B_ Examples of percentage of systems configured to approved standard could include: l Configuration of servers _x000B_ l Configuration of work stations/laptops _x000B_ l Configuration of hand-held devices _x000B_ l Configuration of other supported computer systems covered by the organizations patch policy Out of Scope_x000B_ Examples of computer system configurations that are not in scope _x000B_include: _x000B_ l Temporary guest systems (contractors, vendors) _x000B_ l Lab/test systems performing to or in support of a specific non-production project _x000B_ l Networking systems (routers, switches, access points)						

					l Storage systems(i.e. network accessible storage) _x000B_						

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M41	N/A	Not in scope of EUCS for automated monitoring	Mean Time to Complete Changes	The Center for Internet Security	The average time it takes to complete a configuration change request.	>=0	=	n/a	integer/real	daily	Organization
M42	ISP-03.7	EXCEPTIONS	Percent of Changes with Security Exceptions.	The Center for Internet Security	This metric indicates the percentage of configuration or system changes that received an exception to existing security policy.	[1;100]	=	0	integer/real	daily	Resouces supporting automation of configuration management tasks
M43	AM-01.6	ASSET INVENTORY	Percent of Critical Applications	The Center for Internet Security	The percentage of critical applications measures the percent of applications that are critical to the organization's business processes as defined by the application’s value rating.	>=0	=	n/a	integer/real	daily	Resources used for business applications
M44	N/A	Not in scope of EUCS for automated monitoring	Information Security Budget as a Percentage of IT Budget	The Center for Internet Security	Security budget as a percentage of IT Budget tracks the percentage of IT spending on security activities and systems. For the purposes of this metric, it is assumed that Information Security is included in the IT budget.	[1;100]	=	n/a	integer/real	Annual	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M45	N/A	Not in scope of EUCS for automated monitoring	Information Security Budget Allocation	The Center for Internet Security	Information security budget allocation tracks the distribution of security spending across a variety of security activities, systems, and sources, as a percentage of overall information security spending.	>=0	=	n/a	integer/real	Annual	Organization
M46	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Vulnerability Scan Coverage	The Center for Internet Security	Vulnerability Scanning Coverage (VSC) measures the percentage of the organization's systems under management that were checked for vulnerabilities during vulnerability scanning and identification processes. This metric is used to indicate the scope of vulnerability identification efforts.	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management
M47	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Number of Known Vulnerability Instances	The Center for Internet Security	Number of Known Vulnerability Instances (NKVI) measures the number of known vulnerabilities that have been found on organization's systems during the vulnerability identification process.	>=0	>=	0	integer/real	daily	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M48	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Patch Management Coverage	The Center for Internet Security	Patch Management Coverage (PMC) measures the relative amount of an organization’s systems that are managed under a patch management process such as an automated patch management system. Since patching is a regular and recurring process in an organization, the higher the percentage of technologies managed under such a system the timelier and more effectively patches are deployed to reduce the number and duration of exposed vulnerabilities.	[1;100]	=	100	integer/real	daily	Resources that support patch management
M49	N/A	Not in scope of EUCS for automated monitoring	Percentage of Incidents Detected by Internal Controls	The Center for Internet Security	Percentage of Incidents Detected by Internal Controls (PIDIC) calculates the ratio of the incidents detected by standard security controls and the total number of incidents identified.	[1;100]	=	100	integer/real	daily	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M50	N/A	Not in scope of EUCS for automated monitoring	Mean Time from Discovery to Containment	The Center for Internet Security	Mean Time from Discovery to Containment (MTDC) measures the effectiveness of the organization to identify and contain security incidents. The sooner the organization can contain an incident, the less damage it is likely to incur. This calculation can be averaged across a time period, type of incident, business unit, or severity.	>=0	>=	0	integer/real	daily	Organization
M51	N/A	Not in scope of EUCS for automated monitoring	Percentage of uptime	EU FP7 Cumulus	The percentage of time the resource was considered available, in comparison with the total elapsed time.	[1;100]	=	100	integer/real	daily	Resources (in general)
M52	N/A	Not in scope of EUCS for automated monitoring	Percentage of processed requests	EU FP7 Cumulus	The percentage of successful resource requests processed by the provider over the total number of submitted requests.	[1;100]	=	100	integer/real	daily	Resources (in general)
M53	N/A	Not in scope of EUCS for automated monitoring	Percentage of timely provisioning requests	EU FP7 Cumulus	Measures the provider's ability to respond to provisioning requests for a resource within a maximum predefined delay.	[1;100]	=	100	integer/real	daily	Resources (in general)
M54	N/A	Not in scope of EUCS for	Service provider data access level	EU FP7 Cumulus	This attribute describes the confidentiality level of the resource with respect to the personnel operating the CSP.	>=0	>=	n/a	integer/real	daily	Resources (in general)

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
		automated monitoring									
M55	N/A	Not in scope of EUCS for automated monitoring	Percentage of systems with time synchronization	EU FP7 Cumulus	This attribute describes the percentage of distinct clock sources in the resource that are synchronized with a reference point (usually through NTP). This is useful for reliable audit trails.	[1;100]	=	100	integer/real	daily	Resources supporting time sync
M56	N/A	Not in scope of EUCS for automated monitoring	Maximum measured time difference	EU FP7 Cumulus	This attribute describes the maximum absolute difference between distinct clock sources in the resource (independently of any reference time source such as NTP).	>=0	>=	n/a	integer/real	daily	Resources supporting time sync
M57	CO-03.4	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	Number of (successful) audits performed	EU FP7 Cumulus	This attribute describes the number of independent reviews and assessments performed during a predefined period of time (for example, annually).	>=0	>=	n/a	integer/real	daily	Resources with a defined audit plan
M58	N/A	Not in scope of EUCS for automated monitoring	Tenant isolation level	EU FP7 Cumulus	This attribute describes the level of isolation provided to a resource owned by a tenant with respect to other competing tenants.	>=0	>=	n/a	integer/real	daily	Resources (in general)

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M59	N/A	Not in scope of EUCS for automated monitoring	Data portability	EU FP7 Cumulus	Data contained in the resource and belonging to the customer can be exported in predictable time, in a documented, open format.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources (in general)
M60	N/A	Not in scope of EUCS for automated monitoring	Mean time between incidents	EU FP7 Cumulus	This attribute represents the average time elapsed between the recordings of two consecutive incidents applicable to the resource	>=0	=	n/a	integer/real	daily	Organization
M61	N/A	Not in scope of EUCS for automated monitoring	Percentage of timely incident reports	EU FP7 Cumulus	This attribute represents the percentage of incidents that are reported to the customer within a predefined time limit after their discovery, over the total number of incidents recorded.	[1;100]	=	100	integer/real	daily	Organization
M62	N/A	Not in scope of EUCS for automated monitoring	Percentage of timely incident responses	EU FP7 Cumulus	This attribute represents the percentage of incidents that are assessed and acknowledged by the provider within a predefined time limit after their discovery, over the total number of incidents recorded.	[1;100]	=	100	integer/real	daily	Organization
M63	N/A	Not in scope of EUCS for automated monitoring	Percentage of timely incident resolutions	EU FP7 Cumulus	This attribute represents the percentage of incidents that are resolved within a predefined time limit after discovery, over the total number of incidents recorded	[1;100]	=	100	integer/real	daily	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M64	IAM-03.11	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	User authentication and identity assurance level	EU FP7 Cumulus	This attribute measures the strength of the mechanism used to authenticate a user accessing a resource.	>=0	=	n/a	integer/real	daily	Resources supporting user authentication
M65	IAM-03.11	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	Mean time required to revoke a user	EU FP7 Cumulus	This attribute describes quantitatively how fast an organization revokes users' access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer)	>=0	=	n/a	integer/real	daily	Authorization management system
M66	IAM-03.11	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	Password storage protection level	EU FP7 Cumulus	This attribute describes how passwords are protected in the resource	[1;100]	=	n/a	integer/real	daily	Resouces supporting user authentication

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M67	N/A	Not in scope of EUCS for automated monitoring	Cryptographic brute force resistance	EU FP7 Cumulus	This attribute expresses the strength of a cryptographic protection applied to a resource based on its key length, using the ECRYPT 8 level. Instead of using key lengths alone, which are not always directly comparable from one algorithm to another, this normalizing scale allows comparison of the strengths of different types of cryptographic algorithms	>=0	=	n/a	integer/real	daily	Resouces implementing cryptography
M68	N/A	Not in scope of EUCS for automated monitoring	Key access control level	EU FP7 Cumulus	The attribute describes how strongly a cryptographic key is protected from access, when it is used to provide security to the resource (or assets within the resource).	>=0	=	n/a	integer/real	daily	Resouces implementing cryptography
M69	N/A	Not in scope of EUCS for automated monitoring	Country level anchoring	EU FP7 Cumulus	This attribute indicates that all processing operations applicable to the resource only take place within a set of predefined countries.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources which can be deployed in multiple geographical locations
M70	N/A	Not in scope of EUCS for automated monitoring	Data deletion quality level	EU FP7 Cumulus	This attribute measures the quality of data deletion, ranging from 'weak' deletion where only the reference to the data is removed, to 'strong' deletion where data is overwritten / destroyed.	>=0	=	n/a	integer/real	daily	Resources supporting different types of data deletion

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M71	N/A	Not in scope of EUCS for automated monitoring	Percentage of timely effective deletions	EU FP7 Cumulus	This attribute describes how many deletion requests made by the customer and applicable to the resource are effectively completed within a predefined time limit	[1;100]	=	100	integer/real	daily	Resources (in general)
M72	N/A	Not in scope of EUCS for automated monitoring	Percentage of tested storage retrievability	EU FP7 Cumulus	This attribute describes the percentage of data stored in the resource that has been verified to be retrievable during the measurement period.	[1;100]	=	100	integer/real	daily	Resouces supporting storage of data
M73	N/A	Not in scope of EUCS for automated monitoring	Durability	EU FP7 Cumulus	This security attribute describes the durability for stored data: the average percentage of data in the resource that will not be lost over a certain period, due to software or hardware failures.	[1;100]	=	100	integer/real	daily	Resouces supporting storage of data
M74	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Vulnerability exposure level	EU FP7 Cumulus	This attribute describes the vulnerability exposure level of the resource in terms of numbers of vulnerabilities found with regards to the number of vulnerabilities tested, and the number of vulnerabilities that are relevant to the platform/software of the resource and a reference vulnerability source.	>=0	>=	0	integer/real	daily	Resources that support vulnerability management

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M75	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Percentage of timely vulnerability corrections	EU FP7 Cumulus	This attribute refers to the provider's ability to respond to vulnerabilities applicable to the resource with corrective measures within a maximum predefined delay.	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management
M76	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Percentage of timely vulnerability reports	EU FP7 Cumulus	This attribute refers to the provider's ability to report vulnerabilities about the resource to customers within a maximum predefined delay.	[1;100]	=	100	integer/real	daily	Resources that support vulnerability management
M77	OPS - 07.3	DATA BACKUP AND RECOVERY – MONITORING	Recovery point	EU FP7 Cumulus	This attribute describes the recovery point objective (RPO) or recovery point actual (RPA) of the resource. The RPA represents the data freshness of a backup – i.e. the time elapsed since data was stored for the purpose of eventually restoring the system in a stable state, for example in a backup	>=0	=	0	integer/real	daily	Resouces with a backup plan

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M78	OPS - 07.3	DATA BACKUP AND RECOVERY – MONITORING	Recovery time	EU FP7 Cumulus	This attribute describes the recovery time of the resource: this is the time that is needed after a failure to restore the system to a stable state.	>=0	=	0	integer/real	daily	Resouces with a backup plan
M79	HR-04.7	SECURITY AWARENESS AND TRAINING	Percentage of authorized personnel that received training on the	EU FP7 Cumulus	Percentage (%) of authorized personnel that have received security training	[1;100]	=	100	integer/real	daily	Personnel
M80	OPS - 07.3	DATA BACKUP AND RECOVERY – MONITORING	Percentage of recovery success	EU FP7 Cumulus	This attribute describes the percentage of successful backup restorations performed and verified to be correct (by a checksum, a format check, etc.).	[1;100]	=	100	integer/real	daily	Resouces with a backup plan
M81	CCM - 05.3	PERFORMING AND LOGGING CHANGES	Configuration change reporting capability	EU FP7 Cumulus	This attribute describes the capability of the provider to report changes to the resource. The value of the attribute should be able to represent configuration change types in a standardized manner.	Unknown					Resouces supporting automation of configuration management tasks

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M82	CCM-05.3	PERFORMING AND LOGGING CHANGES	Percentage of timely configuration change notifications	EU FP7 Cumulus	This attribute refers to the provider's ability to report resource configuration changes within a maximum predefined delay.	[1;100]	=	100	integer/real	daily	Resouces supporting automation of configuration management tasks
M83	PM-04.7	MONITORING OF COMPLIANCE WITH REQUIREMENTS	Percentage of compliant applications	EU FP7 Cumulus	This attribute describes the percentage of executable applications within the resource that have been explicitly approved for use. The monitoring of approved applications is performed by first detecting the available applications on the resource and cross checking them against a predefined list of applications or an approved baseline application set, using version control, pattern recognition and/or hashes.	[1;100]	=	100	integer/real	daily	Resources used for business applications
M84	N/A	Not in scope of EUCS for automated monitoring	Authorized collection of PII	EU FP7 A4Cloud	This metric describes the coverage of authorizations for collecting personally identifiable information (PII).	[1;100]	=	100	integer/real	daily	Resources used for business applications
M85	N/A	Not in scope of EUCS for automated monitoring	Privacy Program Budget	EU FP7 A4Cloud	This metric describes the percentage of the organization's IT budget that is allocated for establishing and maintaining a privacy program.	>=0	=	n/a	integer/real	Annual	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M86	N/A	Not in scope of EUCS for automated monitoring	Privacy Program Updates	EU FP7 A4Cloud	This metric describes the frequency of updates to the privacy program, policies and procedures by a competent role (e.g. Data Protection Officer (DPO)).	>=0	=	n/a	integer/real	Annual	Organization
M87	N/A	Not in scope of EUCS for automated monitoring	Periodicity of Privacy Impact Assessments for Information Systems	EU FP7 A4Cloud	This metric describes the periodicity of Privacy Impact Assessments for Information Systems.	>=0	=	n/a	integer/real	Annual	Organization
M88	N/A	Not in scope of EUCS for automated monitoring	Number of privacy audits received	EU FP7 A4Cloud	This metric describes the number of independent reviews and assessments performed to the privacy program, policies and procedures in place.	>=0	=	n/a	integer/real	Annual	Organization
M89	CO-03.4	INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM	Successful audits received	EU FP7 A4Cloud	This metric describes the percentage of independent reviews and assessments performed to the policies and procedures in place for complying with applicable contractual and regulatory obligations.	[1;100]	=	n/a	integer/real	Annual	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M90	N/A	Not in scope of EUCS for automated monitoring	Record of Data Collection, Creation, and Update	EU FP7 A4Cloud	This metric describes a percentage of the extent to which date is recorded when collecting, creating and updating private records. Date of data collection, creation and update is relevant for complying with data retention schedules.	[1;100]	=	n/a	integer/real	Annual	Organization
M91	N/A	Not in scope of EUCS for automated monitoring	Data classification	EU FP7 A4Cloud	This metric describes a percentage of the extent to which private data is identified and classified according to sensitivity and risk.	[1;100]	=	n/a	integer/real	Annual	Organization
M92	HR-04.7	SECURITY AWARENESS AND TRAINING	Coverage of Privacy and Security Training	EU FP7 A4Cloud	percentage of relevant employees who have received training on the privacy program and policies in place.	[1;100]	=	100	integer/real	daily	Personnel
M93	HR-04.7	SECURITY AWARENESS AND TRAINING	Account of Privacy and Security Training	EU FP7 A4Cloud	the quality of the accounts given with respect to the privacy training and awareness programs in place.	Unknown					
M94	N/A	Not in scope of EUCS for automated monitoring	Level of confidentiality	EU FP7 A4Cloud	This metric indicates the level of confidentiality achieved by a system regarding client data independently of the means used to achieve this objective.	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M95	N/A	Not in scope of EUCS for automated monitoring	Key Exposure Level	EU FP7 A4Cloud	This metric indicator of key exposure to reflect the level of confidentiality afforded to cryptographic secrets, from a cloud client point of view.	Unknown					
M96	N/A	Not in scope of EUCS for automated monitoring	Data Isolation Testing Level	EU FP7 A4Cloud	This metric describes the level of testing that has been done by the cloud provider to assess how well data isolation is implemented.	>=0	=	n/a	integer/real	Annual	Resouces supporting data storage
M97	N/A	Not in scope of EUCS for automated monitoring	Type of Consent	EU FP7 A4Cloud	This metric describes the type of consent obtained for collecting, using and sharing private data. The type of consent can be ranked in levels according to its preference.	>=0	=	n/a	integer/real	Annual	Organization
M98	N/A	Not in scope of EUCS for automated monitoring	Type of notice	EU FP7 A4Cloud	This metric describes the type of privacy notice provided by the collecting organization, depending on how the privacy notice is offered to the data subjects. Ideally, multi-layer notice should be provided so data subjects have the information necessary to make decisions at any point in time.	>=0	=	n/a	integer/real	Annual	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M99	N/A	Not in scope of EUCS for automated monitoring	Procedures for Data Subject Access Requests	EU FP7 A4Cloud	This metric describes the quality of the procedures in place for guaranteeing data subjects' access to their personal information.	Unknown					
M100	N/A	Not in scope of EUCS for automated monitoring	Number of Data Subject Access Requests	EU FP7 A4Cloud	This metric describes the number of data subject access requests received during a given period of time.	>=0	=	n/a	integer/real	Annual	Organization
M101	N/A	Not in scope of EUCS for automated monitoring	Responded data subject access requests	EU FP7 A4Cloud	This metric describes the percentage of data subject access requests that have been responded and for which a record of the request and the response exists.	>=0	=	n/a	integer/real	Annual	Organization
M102	N/A	Not in scope of EUCS for automated monitoring	Mean time for responding Data Subject Access Requests	EU FP7 A4Cloud	This metric indicates the mean time for responding to data subject access requests	>=0	=	n/a	integer/real	Annual	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M103	N/A	Not in scope of EUCS for automated monitoring	Readability (Flesch Reading Ease Test)	EU FP7 A4Cloud	This metric describes quantitatively the level of readibility of a given text, computed from the number of sentences, words and syllables. This is of interest for assessing readibility of privacy notices and notifications, which should be written in a clear and concise way.	Unknown					
M104	N/A	Not in scope of EUCS for automated monitoring	Rank of Responsibility for Privacy	EU FP7 A4Cloud	This metric describes numerically at what level within the organization hierarchy the person responsible for privacy is located.	>=0	=	n/a	integer/real	Annual	Organization
M105	N/A	Not in scope of EUCS for automated monitoring	Certification of acceptance of responsibility	EU FP7 A4Cloud	the percentage of employees who have certified their acceptance of responsibilities for activities that involve handling of private data.	[1;100]	=	100	integer/real	daily	Personnel
M106	N/A	Not in scope of EUCS for automated monitoring	Frequency of certifications	EU FP7 A4Cloud	This metric describes how often employees certify their acceptance of responsibilities for activities that involve handling of private data.	>=0	=	n/a	integer/real	Annual	Personnel
M107	N/A	Not in scope of EUCS for automated monitoring	Log Unalterability	EU FP7 A4Cloud	This metric describes the level of protection of the log management systems against tampering.	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M108	IAM-03.11	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	Identity Assurance	EU FP7 A4Cloud	This metric describes the quality of the authentication mechanisms in place.	Unknown					
M109	IAM-03.12	LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS	Mean time to revoke users	EU FP7 A4Cloud	This attribute describes quantitatively how fast an organization revokes users' access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer).	>=0	=	n/a	integer/real	daily	Authentication system
M110	N/A	Not in scope of EUCS for automated monitoring	Mean time to respond to complaints	EU FP7 A4Cloud	This metric indicates the average time that the organization takes for responding to complaints from stakeholders.	>=0	=	n/a	integer/real	monthly	Organization
M111	N/A	Not in scope of EUCS for automated monitoring	Number of complaints	EU FP7 A4Cloud	This metric indicates the number of complaints received during a given period of time.	>=0	=	n/a	integer/real	monthly	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M112	N/A	Not in scope of EUCS for automated monitoring	Reviewed complaints	EU FP7 A4Cloud	This metric indicates the percentage of complaints that have been reviewed during a given period of time.	>=0	=	n/a	integer/real	monthly	Organization
M113	N/A	Not in scope of EUCS for automated monitoring	Number of privacy incidents	EU FP7 A4Cloud	This metric provides the number of privacy incidents and breaches that have occurred in a given period of time.	>=0	=	0	integer/real	daily	Organization
M114	N/A	Not in scope of EUCS for automated monitoring	Coverage of incident notifications	EU FP7 A4Cloud	This metric provides the percentage of privacy incidents and breaches for which affected stakeholders were notified, for a given period of time.	[1;100]	=	100	integer/real	daily	Organization
M115	N/A	Not in scope of EUCS for automated monitoring	Type of incident notification	EU FP7 A4Cloud	This metric describes the quality of the notification procedures after a privacy incident or breach.	[1;100]	=	100	integer/real	daily	Organization
M116	N/A	Not in scope of EUCS for automated monitoring	Privacy incidents caused by third parties	EU FP7 A4Cloud	This metric indicates the number of privacy incidents caused by a third party to whom personal information was transferred (i.e. Data Processors)	>=0	=	0	integer/real	daily	Organization
M117	N/A	Not in scope of EUCS for	Number of Business Continuity Resilience	EU FP7 A4Cloud	This metric indicates the number of business continuity resilience and incident response plans that have been tested in a given interval of time.	>=0	=	n/a	integer/real	daily	Organization

Metric ID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
		automated monitoring	(BCR) plans tested								
M118	N/A	Not in scope of EUCS for automated monitoring	Maximum tolerable period for disruption (MTPD)	EU FP7 A4Cloud	This metric indicates the maximum tolerable period for disruption, as defined by the organizations' BCR plans.	>=0	=	n/a	integer/real	daily	Organization
M119	N/A	Not in scope of EUCS for automated monitoring	Sanctions	EU FP7 A4Cloud	This metric indicates the number and type of sanctions that the organization has received. The EU DPD defines different types of sanctions: (i) a notice addressed to the Data controller (e.g. for compulsory audit), (ii) a fine, (iii) an injunction dictating the end of processing operations, and (iv) a (temporary or permanent) revocation of the authorization allowing the processing of personal data.	>=0	=	n/a	integer/real	daily	Organization
M120	N/A	Not in scope of EUCS for automated monitoring	Incidents with damages	EU FP7 A4Cloud	This metric indicates the number of incidents that end up with compensatory or punitive damages.	>=0	=	0	integer/real	daily	Organization

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M121	N/A	Not in scope of EUCS for automated monitoring	Total expenses due to compensatory damages	EU FP7 A4Cloud	This metric indicates the total expenses incurred due to compensatory damages.	>=0	=	0	integer/real	daily	Organization
M122	N/A	Not in scope of EUCS for automated monitoring	Average expenses due to compensatory damages	EU FP7 A4Cloud	This metric indicates the average expenses due to compensatory damages per upheld complaint/incident	>=0	=	0	integer/real	daily	Organization
M123	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Cryptographic strength	EU FP7 SPECS	Brute force cryptographic resistance of the cloud service/implemented mechanism.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M124	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Forward secrecy	EU FP7 SPECS	Enables the use of forward secrecy (FS) on a cryptographic channel.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M125	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	HSTS (HTTP Strict Transport Security)	EU FP7 SPECS	Usage of HSTS protocol.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M126	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Secure cookies forced	EU FP7 SPECS	Enables use of secure cookies.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M127	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Client certificates	EU FP7 SPECS	Enables the use of client certificates for SSL/TLS-based authentication.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M128	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Certificate status request (a.k.a. OCSP stapling)	EU FP7 SPECS	Enables the use of OCSP for requesting the status of a digital certificate.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M129	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	Certificate pinning	EU FP7 SPECS	Related to the usage of pinning for digital certificates.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M130	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	DANE	EU FP7 SPECS	Enables compliance withDANE monitoring.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M131	OPS - 21.3	MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING	FIPS compliance	EU FP7 SPECS	Enables FIPS compliance.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Resources implementing cryptography
M132	N/A	Not in scope of EUCS for automated monitoring	Level of Diversity	EU FP7 SPECS	Unknown	Unknown					
M133	N/A	Not in scope of EUCS for automated monitoring	TLS Cryptographic Strength	EU FP7 SPECS	Using browser extension prevents MITM attacks where a custom JavaScript payload could be delivered that could read any secret.	Unknown					
M134	N/A	Not in scope of EUCS for automated monitoring	Vulnerability Report Max Age	EU FP7 SPECS	Unknown	Unknown					
M135	N/A	Not in scope of EUCS for	Vulnerability List Max Age	EU FP7 SPECS	Unknown	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
		automated monitoring									
M136	N/A	Not in scope of EUCS for automated monitoring	E2EE Crypto Strength	EU FP7 SPECS	Using browser extension prevents MITM attacks where a custom JavaScript payload could be delivered that could read any secret.	Unknown					
M137	N/A	Not in scope of EUCS for automated monitoring	dDoS Attack Report Max Age	EU FP7 SPECS	Unknown	Unknown					
M138	N/A	Not in scope of EUCS for automated monitoring	Write-Serializability	EU FP7 SPECS	Unknown	Unknown					
M139	N/A	Not in scope of EUCS for automated monitoring	Read-Freshness	EU FP7 SPECS	Unknown	Unknown					
M140	N/A	Not in scope of EUCS for automated monitoring	Backup	EU FP7 SPECS	Unknown	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M141	N/A	Not in scope of EUCS for automated monitoring	Attack Detection Latency	EU FP7 SPECS	Unknown	Unknown					
M142	N/A	Not in scope of EUCS for automated monitoring	Number of False Positives	EU FP7 SPECS	Unknown	Unknown					
M143	N/A	Not in scope of EUCS for automated monitoring	Number of Detected Attacks	EU FP7 SPECS	Unknown	Unknown					
M144	N/A	Not in scope of EUCS for automated monitoring	Number of Vulnerabilities (Family)	EU FP7 SPECS	Unknown	Unknown					
M145	N/A	Not in scope of EUCS for automated monitoring	Number of Vulnerabilities (Gravity)	EU FP7 SPECS	Unknown	Unknown					
M146	N/A	Not in scope of EUCS for	Number of Executed Vulnerability Tests	EU FP7 SPECS	Unknown	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
		automated monitoring									
M147	N/A	Not in scope of EUCS for automated monitoring	Number of Available Vulnerability Tests	EU FP7 SPECS	Unknown	Unknown					
M148	N/A	Not in scope of EUCS for automated monitoring	k-anonimity	http://www.worldscientific.com/doi/abs/10.1142/S02184885 02001648	Unknown	Unknown					
M149	N/A	Not in scope of EUCS for automated monitoring	l-diversity	http://dl.acm.org/citation.cfm?doid=1217299.1217302	Unknown	Unknown					

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M150	N/A	Not in scope of EUCS for automated monitoring	t-closeness	http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4221659	Unknown	Unknown					
M151	N/A	Not in scope of EUCS for automated monitoring	δ-Presence	http://dl.acm.org/citation.cfm?doid=1247480.1247554	Unknown	Unknown					
M152	N/A	Not in scope of EUCS for automated monitoring	€-Differential privacy	http://link.springer.com/chapter/10.1007%2F11787006_1	Unknown	Unknown					
M153		Encryption	TlsVersion	EUCS	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]	>=	1.3	String?	5 minutes	Resources that accept traffic from public networks

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M154	HR-03.5	Human Resources	Personnel with access rights granted without acknowlegement security policies	EUCS	Check if exist employees with access rights granted without acknowledgement of security policies	[TRUE; FALSE]	=	0	Boolean	daily	Access control system
M155	HR-03.5	Human Resources	Automatic monitoring of acknowledgement of security policies	EUCS	Check if there is a possibility to monitor the verification of acknowledgement of security policies automatically	[TRUE; FALSE]	=	1	Boolean	daily	Access control system
M156	HR-04.7	Human Resources	Automatic monitoring of security awareness and training programs completion	EUCS	Check if exists a possibility to monitor the completion of the security awareness and training program automatically	[TRUE; FALSE]	=	1	Boolean	daily	Peronnel monitoring system
M157a	HR-05.4	Human Resources	Internal employees with accesses granted after termination	EUCS	Check if exist internal employees with accesses granted after termination or change of employment, which should have been revoked according to the outcomes of the decision-making procedure	[TRUE; FALSE]	=	0	Boolean	daily	Access control system

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
			or change of employment								
M157b	HR-05.4	Human Resources	External employees with accesses granted after termination or change of employment	EUCS	Check if exist external employees with accesses granted after termination or change of employment, which should have been revoked according to the outcomes of the decision-making procedure	[TRUE; FALSE]	=	FALSE	Boolean	daily	Access control system
M157c	HR-05.4	Human Resources	Existence of a procedure for decision-making on access rights after termination or change of employment	EUCS	Check if exists an established procedure for decision-making about access rights of an employee after termination or change of employment	[TRUE; FALSE]	=	FALSE	Boolean	daily	Access control system

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M157d	HR-05.4	Human Resources	Timely execution of decision-making procedure about access rights after termination or change of employment	EUCS	Check if the procedure for decision-making about access rights of an employee after termination or change of employment is performed before contract termination/change.	[TRUE; FALSE]	=	TRUE	Boolean	daily	Access control system
M158	HR-05.4	Human Resources	Automatic revocation of rights on contract termination	EUCS	Check if access rights are revoked on contract termination or change according to the decision-making procedure automatically	[TRUE; FALSE]	=	TRUE	boolean	daily	Access control system
M159	HR-06.7	Human Resources	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	EUCS	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	[0;100]	=	100	integer/real	daily	Personnel

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M160	HR-06.7	Human Resources	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	EUCS	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	[0;100]	=	100	integer/real	daily	Personnel
M161	HR-06.7	Human Resources	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	EUCS	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	[0;100]	=	100	integer/real	daily	Personnel
M162	HR-06.7	Human Resources	Automatic monitoring of confirmation of non-disclosure or confidentiali	EUCS	Check if exists a possibility of monitoring confirmation of non-disclosure or confidentiality automatically	[TRUE; FALSE]	=	TRUE	boolean	daily	Access control system

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
			ty agreements								
M163	PSS-04.3	Product Security and Safety	VM and container images integrity checks	EUCS	Are integrity checks performed at start-up of VM and container images?	[TRUE; FALSE]	=	TRUE	boolean	continuous?	VM / container orchestration system
M164	PSS-04.3	Product Security and Safety	Automatic monitoring of VM and container images integrity checks	EUCS	Are integrity checks of VM and container images automatically monitored?	[TRUE; FALSE]	=	TRUE	boolean	continuous?	VM / container orchestration system
M165	PSS-04.3	Product Security and Safety	Reporting to CSCs about VM and container images integrity checks	EUCS	Are the reports of VM and container images' integrity checks presented to the CSCs?	[TRUE; FALSE]	=	TRUE	boolean	continuous?	VM / container orchestration system
M166	CO-03.4	Compliance	SWWhitelist Enabled	EUCS	This metric is used to assess if the software whitelisting has been enabled on a cloud service / asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support software whitelisting

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M167	CO-03.5	Compliance	ATPEnabled	EUCS	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support integration with native ATP functionalities.
M168	CS-04.5	Communication Security	HTTPSecurity	EUCS	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPS Only]	=	HTTPSOnly	String	10	Resources that support HTTP/S protocol
M169	CS-04.5	Communication Security	InternetFacingEnabled	EUCS	This metric is used to assess if a cloud service/asset has enabled internet reachability	[TRUE; FALSE]	=	FALSE	Boolean	10	Critical resources which must not be internet reachable, and therefore configured on a Virtual Network (SDN).
M170	CS-04.5	Communication Security	IPSourceFilteringEnabled	EUCS	This metric is used to assess if IP source filtering has been enabled on a cloud service/asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources supporting IP source filtering configuration

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M171	CS-04.5	Communication Security	SSLEnabled	EUCS	This metric is used to assess if a cloud service/asset is using SSL	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support SSL protocol
M172	CS-04.5	Communication Security	MutualAuthnEnabled	EUCS	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support mutual authentication with client certificates
M173	CS-04.5	Communication Security	NetworkFirewallEnabled	EUCS	This metric is used to assess if a network-level firewall has been enabled on a cloud service/asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Virtual Networks supporting firewalls
M174	CS-04.5	Communication Security	JITAccessEnabled	EUCS	This metric is used to assess if Just in time access (JIT) has been enabled on a cloud service / asset.	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support JIT access configuration
M175	IAM-03.11	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT	AuthNMechanism	EUCS	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedIndentity, SSO]	=	SSO	String	10	Resources that support SSO integration
M176	IAM-03.12	IDENTITY, AUTHENTICATION, AND	AuthNMechanism	EUCS	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedInde	=	SSO	String	10	Resources that support SSO integration

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
		ACCESS CONTROL MANAGEMENT				ntity, SSO]					
M177	IAM-03.12	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT	AnonAuthNForbiden	EUCS	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support anonymous authentication
M178a	IM-03.4	Incident Management	IncidentManagementEnabled	EUCS	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support automation of incident management (detection, monitoring)
M178b	IM-03.4	Incident Management	IncidentRemediationUserApproval	EUCS	This metric is used to assess if the automated incident remediation mechanism requires user approvals.	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support automation of incident remediation actions

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M179	OIS-02.4	Organization of Information Security	SecurityContactEnabled	EUCS	This metric is used to assess if a security operator / security contact has been assigned on a cloud service/asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support configuration of a security operator/security contact
M180	OPS - 02.3	Operational Security	ResourceProvisioningMonitorEnabled	EUCS	This metric is used to assess if the CSP has enabled the automated monitoring of resources' provisioning and deprovisioning.	[true, false]	=	true	Boolean	10	CSP's resource manager or native functionality used to monitor the resource manager's health.
M181	OPS - 05.3	Operational Security	AntiMalwareEnabled	EUCS	This metric is used to assess if the antimalware solution specified by the CSP on its security concept/operation manual has been enabled on a cloud service / asset.	[true, false]	=	true	Boolean	10	Resources that are supported by the antimalware solution specified by the CSP on its security concept.

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M182	OPS - 05.4	Operational Security	AntiMalwareEnabled	EUCS	This metric is used to assess if the antimalware solution specified by the CSP on its security concept/operation manual has been enabled on a cloud service / asset.	[true, false]	=	true	Boolean	10	Resources that are supported by the antimalware solution specified by the CSP on its security concept.
M183	OPS - 05.4	Operational Security	AntiMalwareResultsCompliant	EUCS	This metric is used to assess if the antimalware solution reports no irregularities.	[true, false]	=	true	Boolean	10	Resources that support antimalware solutions
M184	OPS - 07.2	Operational Security	SelfServicePortalEnabled	EUCS	This metric is used to assess if a self-service portal for data backup monitoring is available.	[true, false]	=	true	Boolean	10	
M185	OPS - 07.3	Operational Security	BackupEnabled	EUCS	This metric is used to assess if backups are enabled for a cloud service/asset	[true, false]	=	true	Boolean	10	Resources supporting backups
M186	OPS - 07.3	Operational Security	BackupRetention	EUCS	This metric is used to assess the configured backup retention (days) on a cloud service/asset	[0, …, 99]	>	35	Integer	10	Resources supporting the notion of retention

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
											time for backups
M187	OPS - 09.5	DATA BACKUP AND RECOVERY – STORAGE	RemoteBackupLocation	EUCS	This metric is used to assess if the backup of a cloud service/asset is stored in a remote location	[true, false]	=	true	Boolean	24	Resources supporting backups
M188	OPS - 12.4	Operational Security	ATPEnabled	EUCS	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[true, false]	=	true	Boolean	10	Resources that support integration with native ATP functionalities.
M189	OPS - 12.4	Operational Security	LoggingEnabled	EUCS	This metric is used to assess if security logs are enabled for the cloud service/asset.	[true, false]	=	true	Boolean	10	Resources that support integration to native security logging functionalities.
M190	OPS - 12.4	Operational Security	LogRetention	EUCS	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0, …, 99]	>	7	Integer	10	Resources supporting the notion of retention

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
											time for security logs
M191	OPS - 13.7	Operational Security	LoggingEnabled	EUCS	This metric is used to assess if security logs are enabled for the cloud service/asset.	[true, false]	=	true	Boolean	10	Resources that support integration to native security logging functionalities.
M192	OPS - 13.7	Operational Security	LogRetention	EUCS	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0; ...; 99]	>	7	Integer	10	Resources supporting the notion of retention time for security logs
M193	OPS - 18.6	Operational Security	AutomaticUpdatesEnabled	EUCS	This metric is used to assess if automatic updates are enabled for the cloud service/asset	[true, false]	=	true	Boolean	10	Resources that support automatic update mechanisms.
M193a	OPS - 18.6	Operational Security	AutomaticUpdates Interval	EUCS	This metric is used to assess the update interval of automaticc updates for the cloud service/asset	[1, ..., 365]	<=	7	Integer	7	Resources that support automatic update mechanisms.

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M194	OPS - 21.3	Operational Security	ATPEnabled	EUCS	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[true, false]	=	true	Boolean	10	Resources that support integration with native ATP functionalities.
M195	OPS - 21.3	Operational Security	CryptoStorageEnabled	EUCS	This metric is used to assess if cryptographic storage has been enabled on a cloud service/asset	[true, false]	=	true	Boolean	10	Resources supporting storage of key on a secure cryptographic storage
M196	OPS - 21.3	Operational Security	HTTPSecurity	EUCS	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPS Only]	=	HTTPSOnly	String	10	Resources that support HTTP/S protocol
M197	OPS - 21.3	Operational Security	HTTPSVersion	EUCS	This metric is used to assess the HTTP version used by the cloud service/asset	[1.0, 2.0]	=	2.0	String	10	Resources that support HTTP/S protocol
M198	OPS - 21.3	Operational Security	JavaVersion	EUCS	This metric is used to assess the Java Runtime version used by the cloud service/asset	[< 11, 11]	=	11	String	10	Resources that support a Java Runtime

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M199	OPS - 21.3	Operational Security	LeastPrivilegeEnabled	EUCS	This metric is used to assess if least privilege access is enabled for the cloud service/asset	[true, false]	=	true	Boolean	10	Resources supporting segregation of roles
M200	OPS - 21.3	Operational Security	PHPVersion	EUCS	This metric is used to assess the PHP version used by the cloud service/asset	[< 7.4, 7.4]	=	7.4	String	10	Resources that support a PHP Runtime
M201	OPS - 21.3	Operational Security	PythonVersion	EUCS	This metric is used to assess the Python version used by the cloud service/asset	[< 3.8, 3.8]	=	3.8	String	10	Resources that support a Python Runtime
M202	OPS - 21.3	Operational Security	SSLEnabled	EUCS	This metric is used to assess if a cloud service/asset is using SSL	[true, false]	=	true	Boolean	10	Resources that support SSL protocol
M203	OPS - 21.3	Operational Security	TlsVersion	EUCS	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	10	Resources that accept traffic from public networks
M204	OPS - 21.3	Operational Security	WAFEnabled	EUCS	This metric is used to assess if a cloud service/asset has enabled WAF functionalities	[true, false]	=	true	Boolean	10	Resources supporting WAF
M205	OPS - 21.3	Operational Security	MutualAuthnEnabled	EUCS	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[true, false]	=	true	Boolean	10	Resources that support mutual authentication with client certificates

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M206	OPS - 21.3	Operational Security	ACLEnabled	EUCS	This metric is used to assess if a service-level ACL has been enabled on a cloud service/asset	[true, false]	=	true	Boolean	10	Resources that support network-level ACLs
M207	OPS - 21.3	Operational Security	AnonAuthNForbiden	EUCS	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[true, false]	=	true	Boolean	10	Resources that support anonymous authentication
M208	OPS - 21.3	Operational Security	SignedCommunicationEnabled	EUCS	This metric is used to assess if the intra-cloud service / asset communication is digitally signed.	[true, false]	=	true	Boolean	10	Resources that support digitally signed communication among them (e.g., nodes in a cluster)
M209	OPS - 21.3	Operational Security	EncryptionAtRestEnabled	EUCS	This metric is used to assess if encryption at rest has been enabled on a cloud service / asset	[true, false]	=	true	Boolean	10	Resources that support encryption at rest
M210	PM-04.7	Procurement Management	OSLoggingEnabled	EUCS	This metric is used to assess if OS-level security logs are enabled for the cloud service/asset.	[TRUE; FALSE]	=	TRUE	Boolean	10	Virtual Machines supporting OS monitoring

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M211	PM-04.8	Procurement Management	IncidentManagementEnabled	EUCS	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]	=	TRUE	Boolean	10	Resources that support automation of incident management (detection, monitoring)
M212	AM-01.6	ASSET MANAGEMENT	Assets_discovery	EUCS	This metric is used to assess if the inventory of assets is regularly monitored	[TRUE; FALSE]	=	TRUE	boolean	10	Regular resources discovery
M213	AM-01.6	ASSET MANAGEMENT	Assets_evaluation	EUCS	This metric is used to assess if the inventory if assets are regularly monitored against policies	[TRUE; FALSE]	=	TRUE	boolean	10	Regular evaluation of assets again policies
M214	AM-03.6	ASSET MANAGEMENT	Commisioning_requests_log	EUCS	This metric is used to assess the existence of digital record of the commissioning requests including the approval or denial	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M215	AM-03.6	ASSET MANAGEMENT	Decommisioning_requests_log	EUCS	This metric is used to assess the existence of digital record of the decommissioning requests including the approval or denial	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M216	AM-04.4	ASSET MANAGEMENT	Commissioning_procedure_public	EUCS	This metric is used to assess existence of a commissioning procedure which is public to internal and external employees	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M217	AM-04.4	ASSET MANAGEMENT	Commissioning_procedu	EUCS	This metric is used to assess the existence risk management procedures in the commisiong procedure	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
			re_content_risks								
M218	AM-04.4	ASSET MANAGEMENT	Commissioning_procedure_content_authorization	EUCS	This metric is used to assess the existence of the information related to the 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	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M219	AM-04.4	ASSET MANAGEMENT	Decommissioning_procedure_content_public	EUCS	This metric is used to assess existence of a decommissioning procedure which is public to internal and external employees	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M220	AM-04.4	ASSET MANAGEMENT	Decommissioning_procedure_content_content	EUCS	This metric is used to assess the inclusion of the complete and permanent deletion of the data or the proper destruction of the media in the decommissioing procedure	[TRUE; FALSE]	=	TRUE	boolean	daily?	Compliance with the approval?
M221	PM-04.7	Procurement Management	The percentage of compliance monitored	EUCS	The percentage of monitored compliance of the third party with their regulatory and contractual obligations	[0;100]	=	100	integer/real		Compliance/ system(cloud) in general

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M222	PM-04.7	Procurement Management	Automatic compliance monitored	EUCS	The check that exists an automatic functionality to monitor compliance	{0;1}	=	1	boolean		Compliance monitoring software
M223	PM-04.7	Procurement Management	Automatic use of compliance results in other procedures	EUCS	The check that the results of the monitoring automatically use in the listed procedures: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).	{0;1}	=	1	boolean		Compliance monitoring software
M224	PM-04.8	Procurement Management	List of violations and discrepancies	EUCS	Check if exists a list of violations and discrepancies (can be a list of rules)	{0;1}	=	1	boolean		Compliance monitoring software
M225	PM-04.8	Procurement Management	Automatically detected violations and discrepancies	EUCS	The percentage of violations and discrepancies which can be automatically detected	[0;100]	=	100	integer/real		Compliance monitoring software
M226	PM-04.8	Procurement Management	Automatic reporting of detected violations	EUCS	Check if there is a procedure for reporting to responsible personnel	{0;1}	=	1	boolean		Compliance monitoring software

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M227	CO-03.4	Compliance	The percentage of internal audit requirements automatically monitored	EUCS	In relation to M221: Check the percentage of implemented compliance monitors in scope.	[0;100]	=	100	integer/real	CSP definition	Compliance monitoring software / Assets in scope of internal audit
M228	CO-03.4	Compliance	Compliance status of internal audit requirements	EUCS	In relation to M222: Check the compliance status of each compliance monitor in scope	[0;1]	=	1	Boolean	CSP definition	Assets in scope of internal audit
M229	CO-03.5	Compliance	Asset_vulnerable	EUCS	Check whether asset is vulnerable by checking if software version matches known vulnerable versions	[TRUE; FALSE]	=	FALSE	Boolean	10	Assets in scope of internal audit
M230	CO-03.5	Compliance	Asset_deviating	EUCS	Check if asset is deviating to any requirement in place for that asset. All requirements must be complying to pass.	[TRUE; FALSE]	=	FALSE	Boolean	5	Assets in scope of internal audit
M231	ISP-03.7	Information Security Policy	Monitor validity of security exceptions / approvals	EUCS	Check if security approvals and exceptions are automatically monitored	[TRUE; FALSE]	=	TRUE	Boolean		
M232	ISP-03.7	Information Security Policy	Validity of security exceptions /	EUCS	Check if security reviews and approvals are up-to-date	[TRUE; FALSE]	=	TRUE	Boolean		

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
			approvals - up-to-date check								
M233	IM-03.4	Incident Management	Security Incident Solution Review - avaliability	EUCS	(BSI-C5 / Sim-04) Check if customers have the ability to review security incident solutions.	[TRUE; FALSE]	=	TRUE	Boolean		
M234	IM-03.4	Incident Management	Security Incident Solution Review - up-to-date check	EUCS	(BSI-C5 / Sim-04) Check if security incident solutions are up to date.	[TRUE; FALSE]	=	TRUE	Boolean		
M235	INQ-03.4	Inquiries	Investigation Monitoring	EUCS	Monitor the data access performed by or on behalf of investigators.	[TRUE; FALSE]	=	TRUE	Boolean		
M236	PS-02.10	PHYSICAL SECURITY	Monitor Attempts to Access Deactivated Accounts	The Center for Internet Security	Monitor attempts to access deactivated accounts through audit logging	>=0	=	0	integer	hourly	Physical access monitoring system
M237	PS-02.10	PHYSICAL SECURITY	Access Audit Enabled	The Center for Internet Security	This metric is used to assess if access monitoring is enabled	[TRUE; FALSE]	=	TRUE	Boolean	hourly	Physical access monitoring system

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M238	OPS - 06.2	Operational Security	EncryptedBackup	EUCS	Check if data is backed up in encrypted, state-of-the-art form.	[true, false]	=	FALSE	Boolean	Event driven	Software
M239	OPS - 09.2	Operational Security	EncryptedBackupTransmission	EUCS	Check if backup data is transmitted in state-of-the-art encrypted form.	[true, false]	=	FALSE	Boolean	Event driven	Software
M240	OPS - 11.1	Operational Security	SecureDataHandling	EUCS	Check if derived data is handled securely.	[true, false]	=	FALSE	Boolean	Event driven	Software
M241	OPS - 13.3	Operational Security	AuthenticatedCommunicationChannelForLogging	EUCS	Check if communication to logging servers uses a authenticated communication channel.	[true, false]	=	FALSE	Boolean	Event driven	Software
M242	OPS - 13.3	Operational Security	ProtectedCommunicationChannelForLogging	EUCS	Check if communication to logging servers is protected by integrity and confidentiality.	[true, false]	=	FALSE	Boolean	Event driven	Software
M243	OPS - 13.4	Operational Security	EncryptedCommunicationChannelForLogging	EUCS	Check if communication to logging servers is encrypted using state-of-the-art encryption.	[true, false]	=	FALSE	Boolean	Event driven	Software
M244	OPS - 15.3	Operational Security	StrongAccessAuthenticationToLoggingAndMonitoring	EUCS	Check if access to logging and monitoring uses strong authentication.	[true, false]	=	FALSE	Boolean	Event driven	Software

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M245	IAM-07.2	Identity, Authentication, and Access Control Management	AuthenticatedAccess	EUCS	Check if access is authenticated	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software
M246	IAM-08.4	Identity, Authentication, and Access Control Management	StronglyHashedPassword	EUCS	Check if passwords are stored using cryptographically strong hash functions	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software
M247	CS-05.4	Communication Security	StronglyEncryptedTunnel	EUCS	Check if a strongly encrypted tunnel is used.	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software
M248	CO-03.5	Compliance	SoftareRuleCompliant	EUCS	Check if software adheres to security policy.	[TRUE; FALSE]	=	FALSE	Boolean	Scheduled	Software
M249	PSS-02.1	Product Security and Safety	ProtectedSessionManagement	EUCS	Check if session management software uses state-of-the-art encryption and session management	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software
M250	PSS-02.2	Product Security and Safety	AutomaticSessionInvalidation	EUCS	Check if session management software invalidates session after it has been detected invalid	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M251	PSS-02.3	Product Security and Safety	ConfigurableSessionTimeout	EUCS	Check if session management software invalidates session after a configurable timeout	[TRUE; FALSE]	=	FALSE	Boolean	Event driven	Software
M252	AM-04.4	ASSET MANAGEMENT	Commitment_employee_to_policies	EUCS	No. of alerts raised for employees without or outdated acknowledgment record	[0;100]?	=	100?	integer/real	daily	Personnel
M253	IAM-03.11	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT	Monitoring_AuthNMechanism	EUCS	Monitoring for log events produced by automated mechanisms to check if they are working properly	[TRUE; FALSE]	=	TRUE	Boolean	Event driven	Software
M254	IAM-03.12	IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT	Monitoring_number_AuthAttempts	EUCS	Monitoring the number of log events produced by automated mechanisms advising for authentication attempts	[0;100]?	=	0	integer/real	Scheduled	Personnel
M255	CCM-03.10	TESTING CHANGES	NumberofExecuted_Required_funcTests	EUCS	Number of executed functional tests versus number of required functional tests	[0;1]	=	1	integer/real	Event driven	Software

MetricID	EUCS ReqID	Control	Metric Name	Source	Description	Scale	Operator	Target Value	Target Value Datatype	Interval (hours)	Target/Asset
M256	CCM - 04.3	TESTING CHANGES	NumberofExecuted_Required_Changes	EUCS	Number of changes executed versus number of changes approved in line with defined criteria	[0;1]	=	1	integer/real	Event driven	Software
M257	CCM - 04.3	TESTING CHANGES	NumberofChangesExecuted_Required_ProdEnv	EUCS	Number of changes in production enviroments executed by the designated roles versus all number of changes	[0;1]	=	1	integer/real	Event driven	Software

Appendix 4: MEDINA Glossary

This appendix provides a glossary of the terms that are often used in MEDINA. It extends and corrects the previous edition of the glossary presented in Deliverable D1.1, which is confidential.

1 Terms and definitions

1.1 Relevant terms in MEDINA

This section provides an overview of the terms that will be used in the context of MEDINA, along with definitions and examples. These definitions will be improved in the course of the project and new terms added, if needed.

- **Assurance Level:** Ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme and states at what level it has been evaluated; the assurance level does not measure the security of an ICT process, product or service themselves. The EU Cybersecurity Act defines the following assurance levels:
  - Basic
  - Substantial
  - High

  Source: EU Cybersecurity Act [3]

- **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 [46]

- **Cloud Service:** One or more capabilities offered via cloud computing invoked using a defined interface.

  Source: ISO/IEC 17888 [46]

- **Cloud Service Provider (CSP):** Party which makes cloud services available

  Source: ISO/IEC 17888 [46]

- **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

- **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

- **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

- **Reference Technical and Organizational Measure:** 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.

- **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:

  - Requiremtent 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.

- **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 Orgnizational 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 [47]

- **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 Ky 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 [47].

- **Security Control Framework:** Set of security control categories, namely a scheme.

  Examples:

  - ISO/IEC 27001 [48]
  - NIST SP 800-53 [47]
  - 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 includingS 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 [49]

- **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***:

$$\textbf{obl} = \text{op}(M(A), TV)$$

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 {**=, >, <** …}

- **Security requirement:** see Technical and Organizational Measure.

- **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*

1.2 Terms coming from the Cybersecurity Act Article 2

The following terms are defined in Article 2 of the Cybersecurity Act [3]. 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 [3]:

(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.