MEDINA

First Impressions on Experimenting with Automated Monitoring Requirements of the Upcoming EU Cybersecurity Certification Scheme for Cloud Services

(Whitepaper)

Editor(s):	Jesus Luna Garcia
Responsible Partner:	Robert Bosch GmbH
Status-Version:	Final
Date:	18.10.2021
Distribution level:	Public

Project Number:	952633
Project Title:	MEDINA

Editor(s):	Jesus Luna Garcia, Bosch
Contributor(s):	Thomas Ruebsamen, Bosch Patrick Weiss, Bosch Valentin Acker, Bosch Tatu Suhonen, Nixu Jarkko Majava, Nixu
Reviewer(s):	Björn Fanta, Fabasoft Patrick Weiss, Bosch
Approved by:	All Partners
Recommended readers:	Cloud Service Providers, Auditors, IT Security-related

Keyword List:	ENISA, EUCS, OSCAL, Automated Monitoring, Continuous Certification
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	05.08.2021	First draft version	Bosch, Nixu
v0.8	08.09.2021	Revised draft	Bosch
v1.0	18.10.2021	Final version	Bosch

Table of contents

Terms and abbreviations 5
Executive Summary 6
1 Introduction 7
2 Background: EU-funded MEDINA Project 9
2.1 Compliance Metrics Catalogue 9
2.2 Risk-based approach for Security Controls 10
2.3 Certification Language 10
2.4 Evidence Collection and Continuous Audit 10
2.5 Standardization Roadmap 10
3 Performed Tests with EUCS Continuous Monitoring 11
3.1 Objective 11
3.2 Approach 11
3.3 Testbed 12
4 Results 13
4.1 Metrics for EUCS Requirements 13
4.2 Automated Assessment Policies 13
4.3 Visualizations - EUCS Dashboard (Proof of concept) 14
5 The CAB Perspective on Continuous Monitoring and Continuous Auditing 16
5.1 Analysis of the PoC 16
5.2 Changing from point-in-time audits to continuous auditing 16
5.3 Verifying results in continuous audits 17
5.4 From Continuous Auditing to Continuous certification 18
6 Recommendations 19
APPENDIX A. Draft EUCS Requirements Related To Continuous (Automated) Monitoring 21
APPENDIX B. Catalogue of elicited MEDINA Metrics for EUCS (Draft) 25

List of tables

TABLE 1. DETAILED DESCRIPTION OF ADOPTED APPROACH 11
TABLE 6. MEDINA RECOMMENDATIONS 19

List of figures

FIGURE 1. EUCS LEVELS OF ASSURANCE AT A GLANCE (ADAPTED FROM ENISA). 9
FIGURE 2. EUCS DASHBOARD (SCREEN 1). 14
FIGURE 4. EUCS DASHBOARD (SCREEN 2). 15

Terms and abbreviations

API	Application Programming Interface
CAB	Conformance Assessment Body
CISO	Chief Information Security Officer
CSA or EU CSA	EU Cybersecurity Act
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
EC	European Commission
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
ICO	Internal Control Owner
IoT	Internet of Things
KPI	Key Performance Indicator
NLP	Natural Language Processing
PII	Personally Identifiable Information
SaaS	Software as a Service
TOM	Technical and Organizational Measure

Executive Summary

This whitepaper reports on lessons learned related to the experimentation performed by the MEDINA team on the topic of continuous (automated) monitoring, just as required by the High Assurance baseline of the draft version of the European Cybersecurity Certification Scheme for Cloud Service (EUCS). Besides the reported process and obtained results, we also provide a set of recommendations to relevant stakeholders (in particular Cloud Service Providers and Auditors) with the goal of supporting the uptake of EUCS for High Assurance.

1 Introduction

One of the recognized reasons for the still limited adoption of Cloud Computing in the EU, is the customers' perceived lack of security and transparency in this technology. Cloud service providers (CSPs) usually rely on security certifications as a mean to improve transparency and trustworthiness, however European CSPs still face multiple challenges for certifying their services (e.g., fragmentation in the certification market, and lack of mutual recognition). In this context, the EU Cybersecurity Act (EU CSA) proposes improving customer's trust in the European ICT market through a set of EU-wide certification schemes. One of those schemes, the European Cybersecurity Certification Scheme for Cloud Service (EUCS[1]) is being developed by the European Union Agency for Cybersecurity (ENISA). For a selected set of high-assurance requirements, the EUCS proposes the following notion of continuous (automated) monitoring:

> *The requirements related to continuous monitoring typically mention "automated monitoring" or "automatically monitor" in their text. The intended meaning of "monitor automatically" is:*
>
> 1. *Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;*
> 2. *Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;*
> 3. *Report deviations to subject matter experts who can analyse the deviations in a timely manner;*
> 4. *If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and*
> 5. *If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.*
>
> *These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity. Nevertheless, the introduction of continuous auditing, at least for level High, remains a mid- or long-term objective, and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.*

The EUCS notion of continuous monitoring conveys important technological and organizational challenges for stakeholders, which need to be carefully analyzed and understood by all relevant stakeholders in order to benefit the adoption of this new certification scheme.

In this whitepaper we present the lessons learned and recommendations from the EU MEDINA project[2] related to the empirical implementation of continuous (automated) monitoring as defined by the draft EUCS. Our recommendations are provided from two different perspectives namely the public CSP's (Bosch[3] and Fabasoft) and the Conformance Assessment Body's (Nixu).

This whitepaper is based on the draft version of the European Cybersecurity Certification Scheme for Cloud Service (EUCS), published on December 22nd 2020, and available online at https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[1] Draft version available at https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[2] Please refer to https://medina-project.eu/
[3] Bosch is also member of ENISA AdHoc WG for EUCS. More information about Bosch, Fabasoft and Nixu can be found here https://medina-project.eu/partners

The rest of this document is organized as follows: Section 2 provides high-level background on the EU MEDINA project, Section 3 describes the objectives and approach of the performed EUCS experimentation, Section 4 presents the obtained results, Section 5 discusses the CAB's perspective, and Section 6 provides the MEDINA team's recommendations for continuous monitoring in EUCS.

2 Background: EU-funded MEDINA Project

In an effort to solve some of the challenges related to the topic of trustworthiness in cloud services, the EU Cybersecurity Act (EU CSA, approved in June 2019) in its Title III gives ENISA the mandate of defining and implementing a European security certification scheme for ICT products, processes and services. Being cloud computing one of the identified EU CSA priorities, Articles 54 (j) and 57 (9) propose the possibility of deploying a high-assurance, evidence-based and continuous certification of European cloud providers. In this context, the EU Cybersecurity Act (EU CSA) proposes improving customer's trust in the European ICT market through a **European certification scheme for cloud services (EUCS)**. The EUCS draft document introduces novel concepts including:

- Three different levels of assurance (Basic, Substantial, and High),
- Composition of certifications for the cloud supply chain,
- Automated/continuous monitoring for high assurance certification.

Figure 1. EUCS levels of assurance at a glance (adapted from ENISA).

Such novelties in EUCS convey new technological challenges for cloud service providers, which need to be solved for fully achieving the expected benefits (including those for cloud customers). In this context, the main objective of the MEDINA European research project is to **provide a holistic framework that enhances cloud customers' control and trust in consumed cloud services**, by supporting CSPs (IaaS, PaaS and SaaS providers) towards the successful achievement of a continuous certification aligned to the EUCS. The proposed framework will be comprised of tools, techniques, and processes supporting the continuous auditing and certification of cloud services where security and accountability are measurable by design. As the MEDINA framework is leveraged into a cloud supply chain, it will support continuously assessing the efficiency and efficacy of security measures to ultimately achieve and maintain a certification.

The rest of this section further elaborates on the main pillars from MEDINA, and their relevance for the uptake of EUCS' notion of continuous (automated) monitoring.

2.1 Compliance Metrics Catalogue

The current EUCS draft provides an organized set of security requirements, mostly based on international standards, which shall we leveraged to certify cloud services. A subset of such requirements (see Annex A) mandates the implementation of continuous monitoring through automated means.

At the time of writing this report, EUCS does not define the concrete guidelines or "compliance metrics" which can be used to automatically assess the requirements shown in Appendix A. The lack of standard EUCS-metrics can become a problem for CSP and CABs, which might need to leverage their own custom metrics for implementing/assessing EUCS requirements in an automated manner. Such levels of heterogeneity might add further complexity to the underlying EUCS' certification process for high assurance.

MEDINA is defining a catalogue of metrics associated to technical and organizational measures (TOMs) in EUCS. The metrics repository in MEDINA covers topics such as those related to system security and integrity, operational security, business continuity and incident management.

2.2 Risk-based approach for Security Controls

MEDINA proposes a risk-based, tool-supported methodology for the selection of EUCS-complementary controls and associated TOMs based on the CSP's risk appetite. Such controls and requirements shall address the concrete needs of a CSP, by also taking into consideration the targeted EUCS assurance level.

2.3 Certification Language

In practice, all security control frameworks (EUCS included) are defined in natural language, which at some point need to be "translated" into a machine-readable representation for purposes related to managing the security life cycle of cloud services. A machine-readable representation of frameworks like EUCS should facilitate the elicitation of metrics and controls as referred in the previous sections. MEDINA proposes to transform the natural-language specification of control frameworks like EUCS into a machine-readable expression, by using NLP (Natural Language Processing). The expected outcome should comprise aspects like scope of the certification, assurance level and conformity assessment method.

2.4 Evidence Collection and Continuous Audit

Essential for achieving continuous audit-based certification is the collection of actual, technical evidence related to the automated monitoring (EUCS). From a technical point of view, one could distinguish between tools and methodologies to address this at code level and at service level. The topic of managing digital evidence related to EUCS will become critical once CSPs start applying for a high-assurance certificate.

MEDINA aims to develop a framework for managing digital evidence related to EUCS. Collected evidences need to be continuously evaluated, so risks are also continuously monitored and updated. Collected evidence in MEDINA will explore leveraging DLT / blockchain techniques for implementing accountable tracking.

2.5 Standardization Roadmap

Standardization is a necessary milestone to guarantee both market adoption and future governance of EUCS. Despite EU/international standardization initiatives can take a long time to provide concrete results, it is required to develop a strategic roadmap (1-3 years vision) which prioritizes the MEDINA's framework components. MEDINA will drive efforts to influence relevant standardization bodies, on the basis of the project results. Whenever applicable, the project will promote the adoption of existing or emerging standards to its own R&D activities.

3 Performed Tests with EUCS Continuous Monitoring

In this section we describe the objective and overall approach for performing the referred EUCS experimentation with selected "continuous monitoring" requirements.

3.1 Objective

The main goal of the presented EUCS experimentation was creating a proof of concept (PoC) related to the *automated monitoring requirements from the EUCS High Assurance baseline*. It is worth to notice that such PoC is not a formal feasibility analysis of the referred EUCS requirements, but a first step in providing practical experience with its implementation and auditing.

Furthermore, because the PoC was fully carried over in the context of MEDINA, we want to acknowledge the following conditions related to its execution:

- The PoC is fully based on EUCS requirements and methodologies described on the draft specification published by ENISA on December 2020.
- No National Accreditation Body (NAB) was involved in the PoC.
- The automated assessments are based on cloud-native technology from a well-known hyperscaler.

3.2 Approach

The EUCS PoC took place between April-2021 and September-2021, and comprised the activities shown on the next table:

Table 1. Detailed description of adopted approach

Stage	Explanation	Comment
1	Selection of EUCS requirements	The requirements to implement came from the EUCS High Assurance baseline, where the keyword "automated monitoring" is used. Due to time constrains, only a subset of the requirements listed in Appendix A were implemented for the PoC.
2	Selection of automated monitoring policies	Automated monitoring policies were chosen based on the catalogue of metrics developed by MEDINA (cf. Appendix B). The monitoring policies came out-of-the-box from the built-in capabilities of the hyperscaler.
3	Experiment the EUCS concept of *operational effectiveness* for automated monitoring requirements	The selected monitoring policies were deployed in a testbed (see Section 3.3) for a period of 30 days to implement / audit the EUCS notion of *operational effectiveness*.
4	Document results, observations and challenges	The present whitepaper was produced to compile results and recommendations related to the real-world usage of the experimented EUCS requirements.

3.3 Testbed

For the presented experimentation with EUCS, we leveraged the cloud-native capabilities of a well-known hyperscaler. On such cloud platform were deployed few cloud resources with different security configurations, but all of these operated by the MEDINA team (based on the hyperscaler's shared responsibility model).

Furthermore, our experimentation relied on the hyperscaler's out-of-the-box Cloud Security Posture Management tool (CSPM[4]) which comprised a set of built-in assessment policies and visualization tools.

[4] Please refer to https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM

4 Results

This section summarizes the main results obtained from the EUCS PoC.

4.1 Metrics for EUCS Requirements

In order to choose the CSPM's automation policies corresponding to the EUCS requirements in scope of the experimentation (cf. Appendix A), we realized the need for eliciting "compliance metrics". Such metrics provide simple, yet concrete information for automating EUCS requirements, namely:

- Requirement ID: corresponding to the actual ID based on the EUCS core document.
- Metric Name: descriptive name for the metric, which can be used later for the automation policy.
- Metric Description: short explanation of the metric's purpose (i.e., how it relates to the corresponding EUCS requirement).
- Scale: possible set of values which can be taken by the metric depending on the referenced EUCS requirement.

The compliance metric bridges the gap between the EUCS requirement and its concrete machine-readable implementation in an CSPM's assessment policy (technology-dependent). Our experimentation demonstrated that with a metric containing the information mentioned above, plus the target value specified by the CSP[5], it was enough for developing the corresponding automation policies in our testbed.

A draft version of MEDINA's metrics catalogue can be found in Appendix B. Please notice that at the time of writing this whitepaper, the introduced metrics catalogue does not provide full coverage of all related EUCS high requirements. As mentioned above, only a handful of requirements from Appendix A were implemented in the CSPM given the PoC's time constrains.

4.2 Automated Assessment Policies

Once metrics have been written for the selected EUCS requirements, it was possible to select the corresponding automated assessment policies. It is worth to notice that at the state of practice, the language used to write automation policies is highly depend on the underlying CSPM. However, based on our practical experience with major hyperscalers and commercial CSPMs, most available policy languages support the minimum set of primitives / expressiveness features needed to represent metrics like the ones found in Appendix B.

It is also worth to notice that CSPM's polices usually relate to specific cloud services (e.g., Virtual Machine, SQL server, Virtual Network and so on) i.e., each service needs its own set of assessment policies even if the same EUCS requirement is being evaluated. Furthermore, we found that not all required metrics can be assessed for all relevant services. In practice, it means that some CSP-side effort will be needed to develop custom policies guaranteeing full coverage of the EUCS requirements to implement. For example, while a Virtual Machine could be automatically assessed for OPS-05.4 (antimalware scans), this was not possible for a Containers due to technical limitations on the CSPM-side.

During the performed experimentation, and due to time constrains, we only deployed out-of-the-box automation policies for the specific type of cloud resources related to our testbed. This resulted in a coverage of less than 50% of the targeted set of EUCS requirements/metrics. We acknowledge that a more comprehensive mapping between EUCS requirements (cf. Appendix

[5] For example based on the CSP's security policy.

A), compliance metrics (cf. Appendix B), and CSPM policies is needed to improve this observed coverage.

It is also important to notice that the deployed policies related only to the actual coverage of the CSPM tool (i.e., the hyperscaler's services), while other non-cloud systems in the focus of the requirements (e.g., HR-04.7 on IT security training records for employees) were out of scope.

4.3 Visualizations - EUCS Dashboard (Proof of concept)

As part of our EUCS PoC and to experiment the required notion of "operational effectiveness", we developed a draft dashboard to visualize EUCS compliance levels based on the deployed automated assessment policies. This custom development was needed given the technical restrictions found on the used CSPM, where it was not possible to visualize past compliance assessments.

The developed dashboard takes as input dataset the results from the automated assessments as supported by the hyperscaler i.e., either Compliant or Non-Compliant. During the experimentation, these compliance results were collected once per-day[6] for a period of 30 days. The developed visualizations are described in the rest of this section.

The first screen of the dashboard (see Figure 2) includes three visualizations. The first one shows the total number of non-compliances with a line chart. The second visualization on the right-hand side displays the average EUCS compliance in percentage. The third and last visualization on this page is a line chart which shows the non-compliances per assessed resource type. As described in Section 3.3, this visualization considers only the three resource types used for the specific purposes of this EUCS PoC[7].

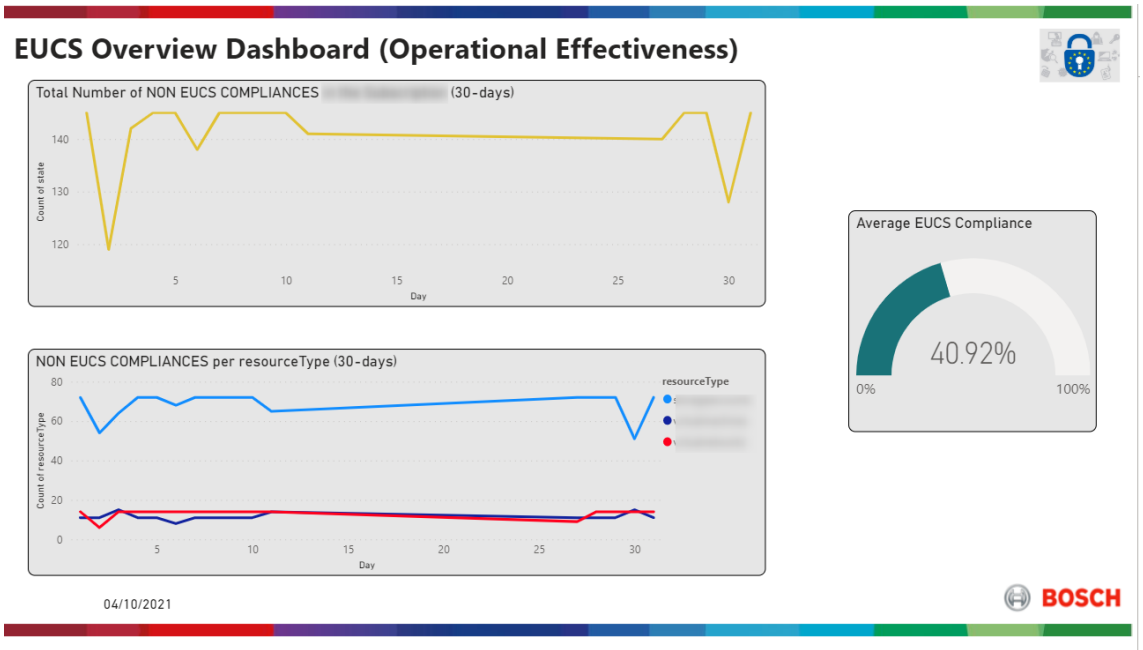

Figure 2. EUCS dashboard (Screen 1).

The second screen of the dashboard (see Figure 3) includes two bar charts. The first one displays the EUCS requirement OPS-12.4. and includes the matching non-compliant metrics/automation

[6] Despite EUCS does not mandate a specific frequency for the continuous assessments, we considered 24 hrs. as a good practice.
[7] To provide additional test capabilities, the configuration of the tested resources was changed during the 30-day period in order to simulate different compliances and non-compliances.

policies in a 30 days view. The second visualization shows the EUCS requirement CS-04.5 with its matching non-compliant policies.

Developed visualizations can be further extended for a productive version of an EUCS dashboard, which might include all relevant EUCS requirements and associated metrics/policies. Such improvement was out of scope for this PoC.

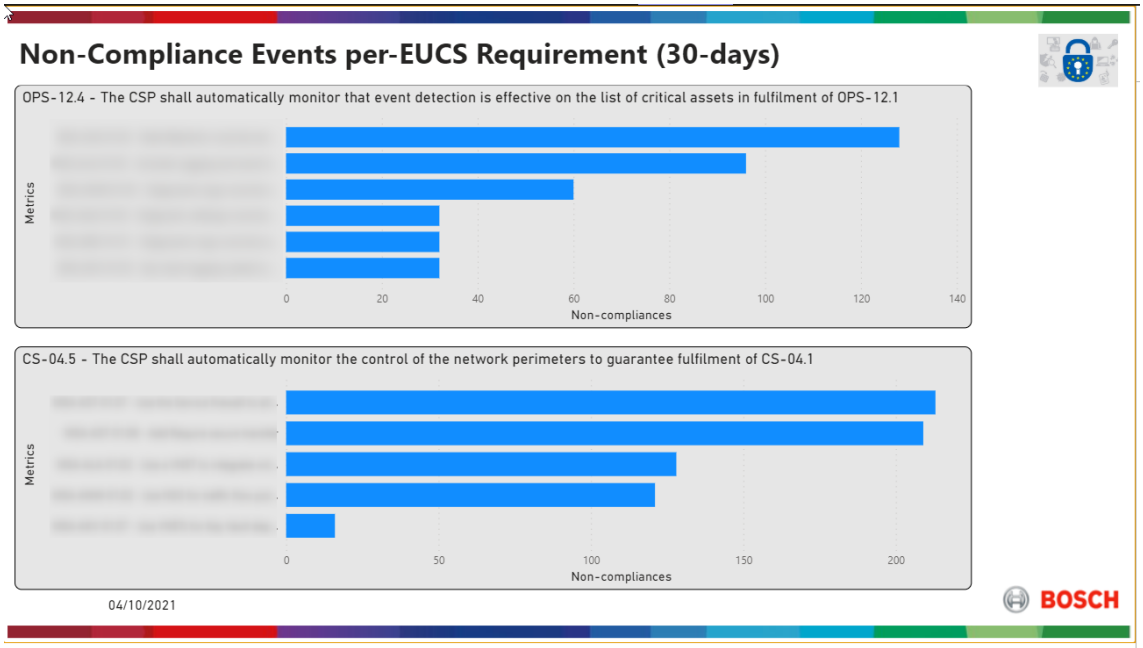

Figure 3. EUCS dashboard (Screen 2).

Developed visualizations were useful to start understanding the continuous compliance behaviour of the resources being assessed. For example, it was noticeable that the number of non-compliances fluctuated during the analysed period probably because of a cloud resource being updated or redeployed.

In the case of visualizations like those shown in Figure 3, we notice that one EUCS requirement can be fulfilled by more than one assessment policy. This fact might complicate the auditor's decision about the (non-)compliance status of the evaluated cloud service.

5 The CAB Perspective on Continuous Monitoring and Continuous Auditing

The PoC offered Nixu a great opportunity to analyse the concept of continuous auditing and provide feedback to develop the innovations. Although the change in audit practice is not governed by the certification bodies, they are the ones with the hands-on experience in auditing and therefore can provide valuable views to the development of continuous auditing. For example in the context of the PoC, having an auditor to interpret requirements and metrics derived from those requirements ensures that the continuous evaluation is done following the intent of the written requirements. Additionally, understanding of the current auditing and certification processes is beneficial when the focus of the research is to change these processes.

5.1 Analysis of the PoC

Based on the analysis of the metrics and framework created in the Medina project, it is possible to implement continuous monitoring which fulfils the intent of the written requirements by using automated evidence collection and analysis. This provides high expectations for the future, and it is likely that we will see a change in how audits are conducted and how the certification is managed. However, the implementation of the metrics must be evaluated case-by-case as each environment and scope is different in each audit. Like in many cases, industry best practices and guidance of governing bodies will eventually steer the implementation continuous audit towards a standardized way. The rest of this section elaborates on the CAB's perspective for transitioning from continuous monitoring to continuous auditing.

5.2 Changing from point-in-time audits to continuous auditing

The current audit practice follows a project-type approach where the auditee's certification follows an audit cycle consisting of individual audits, typically annually. Depending on the used standard, the cycle is started after the initial certification audit and then followed by surveillance audits aimed to ensure that the auditee is still complying to the requirements. When the cycle ends, a recertification audit comparable to the initial audit is conducted to start a new cycle. The challenge in this approach has always been that the audit is always a representation of the auditee's current state during one point in time, but there are limited ways to ensure that the auditee is maintaining the same quality level between audits. It could be that the auditee is considering the certification more as an annual project rather than as continuous and integral part of daily work and is thus focusing majority of the effort just prior to the audits.

Continuous auditing offers great opportunities both the auditee and the auditor. While the auditee can increase their security awareness and enhance their security posture by implementing continuous monitoring and auditing capabilities, the auditor gets more assurance of the auditee's compliance throughout the certification cycle. Additionally, a CAB can extend their service offering with new services and improve audit effectiveness by implementing new innovations and technologies to the auditing process. It is important to notice that the implementation of automated tools does not necessarily reduce the workload of an auditor in an audit, but instead it offers more ways to verify findings in more complex and larger environments. If we look at the current trends in information technology, it is evident that cloud-based solutions have become the go-to solution for many organizations. Assessing these environments can be challenging and any automated tools to help gather and analyse vast amounts of information are welcomed.

However, to accept the use of these tools in auditing is a challenge for the future. There is always a certain trust factor involved when the auditor is reviewing evidence from an information system. These include issues such as:

- How to ensure that the system itself is not manipulating the data?
- How to ensure that the system is configured correctly to provide acceptable evidence?
- How to ensure that the system covers all items in the scope of the audit?
- How is the integrity of the collected evidence ensured?
- Who has access and capability to modify the data?

Eventually the solution could be that the information system to collect data is certified with a relevant certification, but currently there are no such solutions. Additionally, certification of these tools does not guarantee reliable results since each installation is always depending on the environment and implementation where it is installed. While a certification would guarantee a certain security baseline, the implementation of the product in the target environment still has a significant impact on the results. The auditor must verify the trustworthiness of the configuration in each case separately and the level of detail this requires might vary. A widely adopted "industry accepted" tool might be rather simple to verify but a custom-made solution could require specialized skills to understand. Like in many cases, the acceptance criteria for the tools will likely develop as the tools become more common.

5.3 Verifying results in continuous audits

The fundamental change in auditing naturally means that the audit process is changed. The traditional approach to auditing, simplified, is to review documentation, interview persons and verify findings by conducting additional tests, such as process observations, sample reviews or technical tests. By utilizing continuous auditing, the verification of results can be done based on the results collected by automated tools.

Continuous auditing itself does not mean that the role of a certification body would be just to check measurement results and grant a certificate. While certain parts of requirements can be assessed automatically by using measurable metrics, it does not mean that assessing all requirements in compliance frameworks can be fully automated or that all results could be approved as such. For example, if a cloud service provider implements continuous monitoring capabilities to assess requirements, the auditor must go beyond the assessment results to approve them. In order to approve measurement results, at least the following must be ensured:

- The selected metrics are correct, suitable and meet the intent of the requirement
- The measurement is configured and implemented correctly
    - Measurement results are accurate and consistent
- The target asset is correct, and all required assets are monitored
- The measurement result integrity is ensured
    - There must be audit trail for the measurement to prevent alteration of results
    - Medina explores the leveraging of blockchain and other innovative solutions to ensure integrity and accountability.

The change of continuous auditing in the actual audit process is that the configuration check of the continuous monitoring tools will replace some of the manual evidence gathering. What this allows is that the sample sizes can be larger and expanded over longer periods of time. On the other hand, some manual work is still required. Automated tools can be used to verify that certain processes are documented in policies and implemented as required but the actual verification of these processes might require human input in terms of interviews or process observations. However, with good and standardized design of metrics this gap can be narrowed down significantly.

5.4 From Continuous Auditing to Continuous certification

Ideally, the continuous auditing should lead to continuous certification where the status of the certificate is automatically monitored and updated based on the assessment results. There could be multiple implementation methods for continuous certification varying from auditee implemented evidence storage solutions to sophisticated auditor-implemented SOC-type monitoring solutions. However, the approved solutions are to be chosen by the standard owners and industries since the automated certification will change the maintenance of certification. There are still some challenges to be solved such as:

- What are the criteria for certificate suspension?
- How are findings categorized as major and minor nonconformities automatically?
- Is certificate suspended automatically after a finding or after auditor's analysis?
- How is the certificate status logged throughout the cycle?

The optimal solution should be that all significant findings leading possibly to certificate suspension should be evaluated by the auditor, but the evidence of all nonconformities would be saved throughout the certification lifecycle. By this way the probability of false positive findings affecting certification is minimized.

6 Recommendations

Based on the performed experimentation, and departing from the draft EUCS document, the MEDINA team elaborated the following recommendations aimed to support stakeholders' adoption of the EUCS concept of continuous (automated) monitoring for high assurance requirements.

Table 2. MEDINA Recommendations

Recommendation	Comments
Provide a clear *implementation* guidance about EUCS requirements where some degree of automated monitoring is needed.	Close examination of the "Continuous (Automated) Monitoring" definition in the core EUCS document opens questions related to aspects like frequency for gathering compliance data, reference to use for comparing gathered data, and so forth. More detailed/concrete implementation guidance is needed for CSPs aiming to achieve continuous monitoring. As needed, we even suggest referencing technologies like Cloud Security Posture Management systems, which can greatly support implementation of continuous monitoring.
Provide clear *audit/assessment* guidance related to EUCS requirements needing some degree of automated monitoring.	In analogy to the previous recommendation, we also suggest including concrete guidance for auditors working on continuous monitoring. Such guidance should tackle aspects like identification of deviations on the continuous monitoring systems, definition of operational effectiveness in the automated monitoring context, and so forth. Such guidance must also provide information about what CABs are expected to do with data coming from the CSPs' continuous monitoring systems. For example, to guide CABs (and CSPs) on actions to take with "compliance fluctuations" identified during the audit period.
Consider integrating a catalogue of metrics as part of the implementation guidance for EUCS.	The MEDINA team sees the need for a catalogue of metrics to be released as part of the implementation guidance related to continuous monitoring. Such catalogue will reduce the subjectivity of both CSPs and CABs while implementing/assessing a requirement related to continuous monitoring. For our team, the proposed Metrics Catalogue is seen as a necessary requirement for guiding CABs in assessing operational

	effectiveness, and understanding the definition of target values defined by CSPs. The lack of such catalogue might result in partial implementations/assessments of "complex" EUCS requirements like PM-04.7.
Consider focusing the EUCS requirements needing some sort of automated monitoring only on capabilities offered by cloud platforms, and not by external systems.	Our experimentation focused on EUCS requirements purely implemented on a cloud-based testbed, which proved challenging by itself. We recommend a first version of EUCS to focus mostly on such type of requirements, therefore eliminating dependencies/complexities of non-cloud systems.
Guidance on selecting tools/technologies for automated (continuous) monitoring	Stakeholders in EUCS, in particular CSPs and CABs, need further guidance on the tools/technologies implied as required for leveraging automated (continuous monitoring). Such tools/technologies can become a security risk by themselves if they cannot provide the required assurance to stakeholders e.g., if a tool has known vulnerabilities. Furthermore, it is necessary to discuss if the tool/technology itself must be also EUCS certified (if cloud-based), or should provide any other kind of assurance/certification. This might introduce additional complexities (e.g., compositional certification aspects) to the already challenging EUCS High.

APPENDIX A. Draft EUCS Requirements Related To Continuous (Automated) Monitoring

Requirement ID	Requirement Text
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.
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
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.
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program
HR-05.4	The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2
HR-06.7	The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers
AM-01.6	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date
AM-03.6	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.
AM-04.4	The verification of the commitment defined in AM-04.1 shall be automatically monitored
PS-02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1

Requirement ID	Requirement Text
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
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities
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
OPS-07.3	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1
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
OPS-12.4	The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1
OPS-13.7	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2
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
OPS-21.3	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications
IAM-03.11	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03
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

Requirement ID	Requirement Text
CS-04.5	The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1
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
CCM-04.3	The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1
CCM-05.3	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1
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).
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
IM-03.4	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period
CO-03.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions
CO-03.5	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

Requirement ID	Requirement Text
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
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

APPENDIX B. Catalogue of elicited MEDINA Metrics for EUCS (Draft)

Requirement ID	Metric Name	Metric Description	Scale
HR-03.5	Personnel with access rights granted without acknowledgement security policies	Check if exist employees with access rights granted without acknowledgement of security policies	{1;0}
HR-03.5	Automatic monitoring of acknowledgement of security policies	Check if there is a possibility to monitor the verification of acknowledgement of security policies automatically	{1;0}
HR-04.7	Automatic monitoring of security awareness and training programs completion	Check if exists a possibility to monitor the completion of the security awareness and training program automatically	{1;0}
HR-05.4	Internal employees with accesses granted after termination or change of employment	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	{1;0}
HR-05.4	External employees with accesses granted after termination or change of employment	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	{1;0}
HR-05.4	Existance of a procedure for decision making on access rights after termination or change of employment	Check if exists an established procedure for decision-making about access rights of an employee after termination or change of employment	{1;0}
HR-05.4	Timely execution of decision making procedure about access rights after termination or change of employment	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.	{1;0}
HR-05.4	Automatic revocation of rights on contract termination	Check if access rights are revoked on contract termination or change according to the decision making procedure automatically	{1;0}

Requirement ID	Metric Name	Metric Description	Scale
HR-06.7	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	Percentage of relevant internal employees who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	Percentage of relevant external service providers who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	Percentage of relevant suppliers who confirmed non-disclosure or confidentiality agreements	[0;100]
HR-06.7	Automatic monitoring of confirmation of non-disclosure or confidentiality agreements	Check if exists a possibility of monitoring confirmation of non-disclosure or confidentiality automatically	{1;0}
PSS-04.3	VM and container images integrity checks	Are integrity checks performed at start-up of VM and container images?	{yes; no}
PSS-04.3	Automatic monitoring of VM and container images integrity checks	Are integrity checks of VM and container images automatically monitored?	{yes; no}
PSS-04.3	Reporting to CSCs about VM and container images integrity checks	Are the reports of VM and container images' integrity checks presented to the CSCs?	{yes; no}
CO-03.4	SWWhitelistEnabled	This metric is used to assess if the software whitelisting has been enabled on a cloud service / asset	[TRUE; FALSE]
CO-03.5	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
CS-04.5	HTTPSecurity	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPSOnly]

Requirement ID	Metric Name	Metric Description	Scale
CS-04.5	InternetFacingEnabled	This metric is used to assess if a cloud service/asset has enabled internet reachability	[TRUE; FALSE]
CS-04.5	IPSourceFilteringEnabled	This metric is used to assess if IP source filtering has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	SSLEnabled	This metric is used to assess if a cloud service/asset is using SSL	[TRUE; FALSE]
CS-04.5	MutualAuthnEnabled	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	NetworkFirewallEnabled	This metric is used to assess if a network-level firewall has been enabled on a cloud service/asset	[TRUE; FALSE]
CS-04.5	JITAccessEnabled	This metric is used to assess if Just in time access (JIT) has been enabled on a cloud service / asset.	[TRUE; FALSE]
IAM-03.11	AuthNMechanism	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedIndentity, SSO]
IAM-03.12	AuthNMechanism	This metric is used to assess if a cloud service/asset is using a strong/centrally managed authentication method	[UserName, ManagedIndentity, SSO]
IAM-03.12	AnonAuthNForbiden	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[TRUE; FALSE]
IM-03.4	IncidentManagementEnabled	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
IM-03.4	IncidentRemediationUserApproval	This metric is used to assess if the automated incident remediation mechanism requires user approvals.	[TRUE; FALSE]
OIS-02.4	SecurityContactEnabled	This metric is used to assess if a security operator / security contact has been assigned on a cloud service/asset	[TRUE; FALSE]
OPS-02.3	ResourceProvisioningMonitorEnabled	This metric is used to assess if the CSP has enabled the automated monitoring of resources' provisioning and deprovisioning.	[TRUE; FALSE]
OPS-05.3	AntiMalwareEnabled	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]
OPS-05.4	AntiMalwareEnabled	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]
OPS-05.4	AntiMalwareResultsCompliant	This metric is used to assess if the antimalware solution reports no irregularities.	[TRUE; FALSE]
OPS-07.2	SelfServicePortalEnabled	This metric is used to assess if a self service portal for data backup monitoring is available.	[TRUE; FALSE]
OPS-07.3	BackupEnabled	This metric is used to assess if backups are enabled for a cloud service/asset	[TRUE; FALSE]
OPS-07.3	BackupRetention	This metric is used to assess the configured backup retention (days) on a cloud service/asset	[0; …; 99]
OPS-09.5	RemoteBackupLocation	This metric is used to assess the backup of a cloud service/asset is stored in a remote location	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
"OPS-12.4 "	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
"OPS-12.4 "	LoggingEnabled	This metric is used to assess if security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
"OPS-12.4 "	LogRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0; …; 99]
OPS-13.7	LoggingEnabled	This metric is used to assess if security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
OPS-13.7	LogRetention	This metric is used to assess the configured log retention (days) on a cloud service/asset	[0; …; 99]
OPS-18.6	AutomaticUpdatesEnabled	This metric is used to assess if automatic updates are enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	ATPEnabled	This metric is used to assess if Advanced Threat Protection is enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	CryptoStorageEnabled	This metric is used to assess if cryptographic storage has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	HTTPSecurity	This metric is used to assess if a cloud service/asset is using HTTPS	[HTTP, HTTPS, HTTPSOnly]
OPS-21.3	HTTPSVersion	This metric is used to assess the HTTP version used by the cloud service/asset	[1.0; 2.0]
OPS-21.3	JavaVersion	This metric is used to assess the Java Runtime version used by the cloud service/asset	[< 11; 11]

Requirement ID	Metric Name	Metric Description	Scale
OPS-21.3	LeastPriviledgeEnabled	This metric is used to assess if less priviledge access is enabled for the cloud service/asset	[TRUE; FALSE]
OPS-21.3	PHPVersion	This metric is used to assess the PHP version used by the cloud service/asset	[< 7.4; 7.4]
OPS-21.3	PythonVersion	This metric is used to assess the Python version used by the cloud service/asset	[< 3.8; 3.8]
OPS-21.3	SSLEnabled	This metric is used to assess if a cloud service/asset is using SSL	[TRUE; FALSE]
OPS-21.3	TlsVersion	This metric is used to assess if state-of-the-art encryption protocols are used for traffic served from public networks.	[1.0; 1.1; 1.2; 1.3]
OPS-21.3	WAFEnabled	This metric is used to assess if a cloud service/asset has enabled WAF functionalities	[TRUE; FALSE]
OPS-21.3	MutualAuthnEnabled	This metric is used to assess if mutual authentication, including client certificate, has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	ACLEnabled	This metric is used to assess if a service-level ACL has been enabled on a cloud service/asset	[TRUE; FALSE]
OPS-21.3	AnonAuthNForbiden	This metric is used to assess if anonymous authentication has been disabled on a cloud service / asset	[TRUE; FALSE]
OPS-21.3	SignedCommunicationEnabled	This metric is used to assess if the intra-cloud service / asset communication is digitally signed.	[TRUE; FALSE]
OPS-21.3	EncryptionAtRestEnabled	This metric is used to assess if encryption at rest has been enabled on a cloud service / asset	[TRUE; FALSE]

Requirement ID	Metric Name	Metric Description	Scale
PM-04.7	OSLoggingEnabled	This metric is used to assess if OS-level security logs are enabled for the cloud service/asset.	[TRUE; FALSE]
PM-04.8	IncidentManagementEnabled	This metric is used to assess if automated incident management (detection, response) and SIEM has been enabled on a cloud service / asset	[TRUE; FALSE]
AM-01.6	Assets_discovery	This metric is used to assess if the inventory of assets is regularly monitored	[TRUE; FALSE]
AM-01.6	Assets_evaluation	This metric is used to assess if the inventory if assets are regularly monitored against policies	[TRUE; FALSE]
AM-03.6	Commisioning_requests_log	This metric is used to assess the existence of digital record of the commissioning requests including the approval or denial	[TRUE; FALSE]
AM-03.6	Decommisioning_requests_log	This metric is used to assess the existence of digital record of the decommissioning requests including the approval or denial	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_public	This metric is used to assess existence of a commissioning procedure which is public to internal and external employees	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_content_risks	This metric is used to assess the existence risk management procedures in the commisiong procedure	[TRUE; FALSE]
AM-04.4	Commissioning_procedure_content_authorization	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]

Requirement ID	Metric Name	Metric Description	Scale
AM-04.4	Decommissioning_procedure_content_public	This metric is used to assess existence of a decommissioning procedure which is public to internal and external employees	[TRUE; FALSE]
AM-04.4	Decommissioning_procedure_content_content	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]
PM-04.7	The percentage of compliance monitored	The percentage of monitored compliance of the third party with their regulatory and contractual obligations	[0;100]
PM-04.7	Automatic compliance monitored	The check that exists an automatic functionality to monitor compliance	{0;1}
PM-04.7	Automatic use of compliance results in other procedures	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}
PM-04.8	List of violations and discrepancies	Check if exists a list of violations and discrepancies (can be a list of rules)	{0;1}
PM-04.8	Automatically detected violations and discrepancies	The percentage of violations and discrepancies which can be automatically detected	[0;100]
PM-04.8	Automatic reporting of detected violations	Check if there is a procedure for reporting to responsible personnel	{0;1}
CO-03.4	The percentage of internal audit requirements automatically monitored	In relation to M221: Check the percentage of implemented compliance monitors in scope.	[0;100]

Requirement ID	Metric Name	Metric Description	Scale
CO-03.4	Compliance status of internal audit requirements	In relation to M222: Check the compliance status of each compliance monitor in scope	[0;1]
CO-03.5	Asset_vulnerable	Check whether asset is vulnerable by checking if software version matches known vulnerable versions	[TRUE;FALSE]
CO-03.5	Asset_deviating	Check if asset is deviating to any requirement in place for that asset. All requirements must be complying to pass.	[TRUE;FALSE]
ISP-03.7	Monitor validity of security exceptions / approvals	Check if security approvals and exceptions are automatically monitored	[TRUE;FALSE]
ISP-03.7	Validity of security exceptions / approvals - up-to-date check	Check if security reviews and approvals are up-to-date	[TRUE;FALSE]
IM-03.4	Security Incident Solution Review - avaliability	(BSI-C5 / Sim-04) Check if customers have the ability to review security incident solutions.	[TRUE;FALSE]
IM-03.4	Security Incident Solution Review - up-to-date check	(BSI-C5 / Sim-04) Check if security incident solutions are up to date.	[TRUE;FALSE]
INQ-03.4	Investigation Monitoring	Monitor the data access performed by or on behalf of investigators.	[TRUE;FALSE]
PS-02.10	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging	>=0
PS-02.10	Access Audit Enabled	This metric is used to assess if access monitoring is enabled	[TRUE;FALSE]
OPS-06.2	EncryptedBackup	Check if data is backed up in encrypted, state-of-the-art form.	[TRUE;FALSE]
OPS-09.2	EncryptedBackupTransmission	Check if backup data is transmitted in state-of-the-art encrypted form.	[TRUE;FALSE]

Requirement ID	Metric Name	Metric Description	Scale
OPS-11.1	SecureDataHandling	Check if derived data is handled securely.	[TRUE;FALSE]
OPS-13.3	AuthenticatedCommunicationChannelForLogging	Check if communication to logging servers uses a authenticated communication channel.	[TRUE;FALSE]
OPS-13.3	ProtectedCommunicationChannelForLogging	Check if communication to logging servers is protected by integrity and confidentiality.	[TRUE;FALSE]
OPS-13.4	EncryptedCommunicationChannelForLogging	Check if communication to logging servers is encrypted using state-of-the-art encryption.	[TRUE;FALSE]
OPS-15.3	StrongAccessAuthenticationToLoggingAndMonitoring	Check if access to logging and monitoring uses strong authentication.	[TRUE;FALSE]
IAM-07.2	AuthenticatedAccess	Check if access is authenticated	[TRUE;FALSE]
IAM-08.4	StronglyHashedPassword	Check if passwords are stored using cryptographically strong hash functions	[TRUE;FALSE]
CS-05.4	StronglyEncryptedTunnel	Check if a strongly encrypted tunnel is used.	[TRUE;FALSE]
CO-03.5	SoftareRuleCompliant	Check if software adheres to security policy.	[TRUE;FALSE]
PSS-02.1	ProtectedSessionManagement	Check if session management software uses state-of-the-art encryption and session management	[TRUE;FALSE]
PSS-02.2	AutomaticSessionInvalidation	Check if session management software invalidates session after it has been detected invalid	[TRUE;FALSE]
PSS-02.3	ConfigurableSessionTimeout	Check if session management software invalidates session after a configurable timeout	[TRUE;FALSE]

Requirement ID	Metric Name	Metric Description	Scale
AM-04.4	Commitment_employee_to_policies	No. of alerts raised for employees without or outdated acknowledgment record	[0;100]?
IAM-03.11	Monitoring_AuthNMechanism	Monitoring for log events produced by automated mechanisms to check if they are working properly	[TRUE;FALSE]
IAM-03.12	Monitoring_number_AuthAttempts	Monitoring the number of log events produced by automated mechanisms advising for authentication attempts	[0;100]?
CCM-03.10	NumberofExecuted_Required_funcTests	Number of executed functional tests versus number of required functional tests	[0;1]
CCM-04.3	NumberofExecuted_Required_Changes	Number of changes executed versus number of changes approved in line with defined criteria	[0;1]
CCM-04.3	NumberofChangesExecuted_Required_ProdEnv	Number of changes in production environments executed by the designated roles versus all number of changes	[0;1]