European Security Certification Framework

D5.3 - REQUIREMENTS AND VALIDATION CRITERIA – PILOT RESULTS

1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 31/05/2019	DELIVERY DATE: July 2019
AUTHOR: CSA	PARTNERS CONTRIBUTED: CAIXA, CSA, Fabasoft, Fraunhofer, NIXU, SixSQ.
DISSEMINATION LEVEL: PU	NATURE OF THE DELIVERABLE: R
INTERNAL REVIEWERS: CAIXA, Fraunhofer	
*PU = Public, CO = Confidential	**R = Report, P = Prototype, D = Demonstrator, O = Other

EXECUTIVE SUMMARY

The EU-SEC project introduced a novel continuous audit-based certification framework where cloud services are not just certified through a point-in-time audit but are also scrutinized continuously by running regular tests to obtain an uninterrupted level of assurance. This novel framework was tested in a pilot, as described throughout the Work Package 5 in the project. In this context, this document follows the deliverables D5.1 and D5.2 and concludes the pilot by examining feedback provided from all stakeholders.

The pilot is built around a set of tools that together aim to demonstrate the continuous security assessment of a mock application: a financial information sharing (FISH) platform, which is tested by CaixaBank to exchange data with other financial institutions and regulatory bodies. The tools supporting continuous auditing-based certification (CaC) include:

- *Clouditor: a cloud monitoring tool that continuously tests the security of FISH, verifying that a set of predefined security objectives are met (SLOs and SQOs), based on collected evidence.*
- *Nuvla: a trusted storage facility used as a secure repository for collected evidence, for the purpose of future review (e.g. to address a dispute).*
- *STARWatch: a platform that maintains a public registry of certified cloud providers, which is updated according to the results provided by Clouditor.*

The pilot showed that the tools work together as expected, enabling a continuous audit of selected SLO/SQOs. NIXU's analysis of the toolchain confirmed that they are adequate for the task. More generally, both internal and external stakeholders expressed a high degree of satisfaction with the pilot, which was notably showcased during a public workshop in Barcelona in April 2019.

When doing CaC, monitoring tools such as Clouditor need to be trustworthy and fit for purpose. This is the reason why the EU-SEC project envisioned that they would be certified as part of a more traditional audit which would precede the continuous certification phase. Feedback shows that many stakeholders are sensitive to this issue.

Continuous auditing relies as much as possible on automation. As a proof of concept, the pilot covered the automated continuous monitoring of 15 security objectives encompassing 5 CCM control objectives out of a total of 133. In a real-life use case, it will be necessary to expand this

coverage to more control objectives. A preliminary analysis shows that a total of 72 CCM controls can be partially or fully assessed by automated means. Still, human assessment will be needed in some cases, typically on a less frequent basis, for organisational controls that do not lend themselves to automated evaluation.

The conclusion of this pilot comes in a timely manner with the release in June 2019 of recommendations issued by the CSPCERT Working Group to the European Commission and ENISA regarding the implementation of cloud certification schemes. These recommendations notably highlight the potential role of continuous auditing in the case of sensitive cloud applications and even mention the EU-SEC project. The pilot demonstrates the feasibility of this approach.

ABBREVIATIONS

CCM	Cloud Control Matrix
CSP	Cloud Service Provider
EAB	External Advisory Board
FISH	Financial Information Sharing
SLO	Service Level Objective
SQO	Service Qualitative Objective

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 OBJECTIVE AND SCOPE

This third deliverable in Work Package 5 concludes the EU-SEC continuous audit-based certification pilot. It aims to summarize the results of the pilot by answering 3 main questions:

- Do the tools work together as expected, enabling a continuous audit of selected SLO/SQOs?
- Does the pilot show that the tools are adequate for the task?
- Based on the pilot, what is the opinion of internal and external stakeholders on the practicality of continuous audit-based certification?

1.2 BACKGROUND

Continuous audit-based certification (CaC) is a new paradigm in cloud assurance: instead of certifying a cloud service based on a point-in-time audit[1], we scrutinize it continuously by running regular tests to obtain an uninterrupted level of assurance. As detailed in Deliverable D2.1, this requires us to translate typical high-level control objectives, as defined in [ISO 27002] or CSA [CCM], into Service Level Objectives (SLOs) or Service Quality Objectives (SQOs), which can be regularly validated by automated tools or humans, following concrete and unambiguous metrics. Each SLO or SQO that is applicable to a cloud service needs to be evaluated periodically, according to a predefined frequency.

In this novel approach, a cloud service will be considered as "certified" if all applicable SLO/SQOs are validated and if this validation was done in a timely manner, in agreement with the evaluation frequency associated with each SLO/SQO. The fact that a cloud service is "certified" is published in a trusted public registry that is accessible by all stakeholders.

The validation of SLOs and SQOs is performed through the collection and evaluation of evidence: specific data collected from the target cloud service. For accountability purposes, this

[1] Or "period-in-time" audit.

evidence should be stored in a secure trusted location, where it can later be reviewed if necessary.

Based on this approach, in order to conduct a continuous audit on a target cloud service, at least four components must be involved:

- A cloud service or application under scrutiny.
- A monitoring tool that collects and analyses evidence from the cloud service to determine if SLO/SQOs are satisfied.
- A tool or service that stores collected evidence for future review.
- A public registry that keeps track of the certification status of a cloud service based on the results provided by the monitoring tool.

In practice, except for self-assessments, an independent auditor must also be involved in the process in order to check that the selected SLO/SQOs and evaluation frequencies correctly reflect the level of security that the cloud service aims to achieve. The auditor will also check that the monitoring tools are fit for purpose.

The pilot in Work Package 5 was designed to demonstrate how to build and integrate the 4 components we previously described in order to deliver continuous audit based certification. In this context we used:

- **FISH,** an example of financial data sharing cloud-based application tested by CaixaBank.
- **Clouditor**, a cloud security assessment tool developed by Fraunhofer AISEC.
- **Nuvla,** a trusted evidence storage service.
- **STARWatch**, a public registry of certified cloud services developed by CSA.

For convenience, the figure below provides a summary of the pilot architecture, which is otherwise extensively described in deliverables D5.1 and D5.2. In the pilot, the key processes that take place during a continuous audit are the following:

1) **Clouditor** is setup to continuously perform tests on a target service, i.e. the "FISH" application (in the following, FISH **App**), hosted by a Cloud Service Provider (**CSP**).
2) **Clouditor** stores all the evidence it collects during testing with **Nuvla**, a trusted secure storage service.
3) **Clouditor** sends the test results on a timely basis to **CSA STARWatch**. Each result contains a reference to the supporting evidence, which is stored with Nuvla.
4) **CSA STARWatch** updates a public registry that describes the continuous certification status of the **FISH App**.

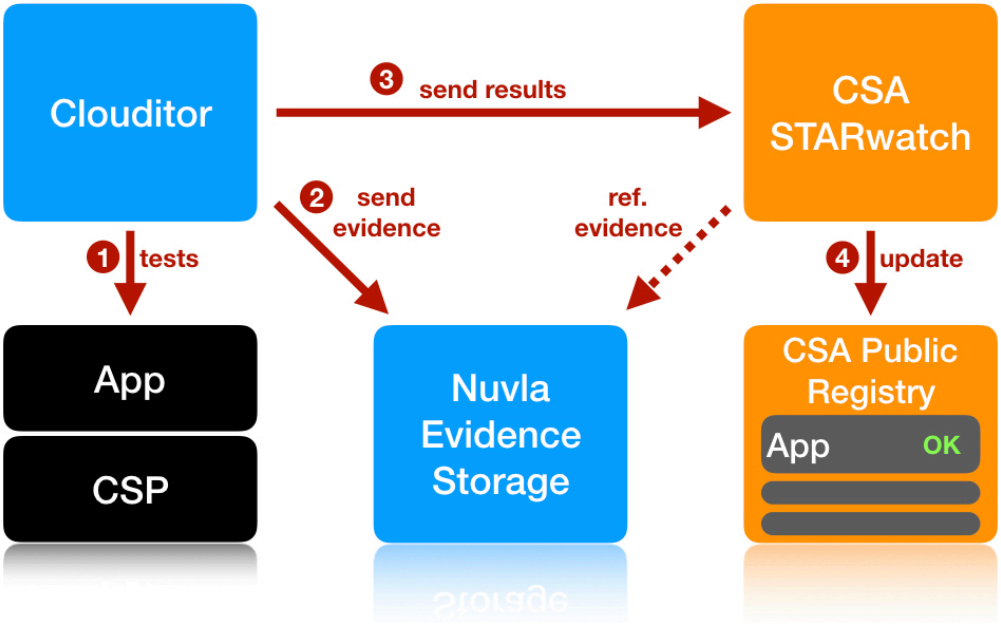

Figure 1. Pilot architecture summary

Using the architecture described in Figure 1, the pilot provided the opportunity to demonstrate the technical feasibility of continuous audit-based certification, with a mock application for Financial Information Sharing ("FISH") that simulated a secure financial information exchange platform targeting exchange of confidential documents between banks and regulators. In fact, two variations of the **FISH App** were tested in the pilot:

1) FISH as an independent application hosted on Amazon AWS (IaaS).
2) FISH as a SaaS (Software as a Service) application provided by Fabasoft.

I both cases, we were able to validate the tools, APIs and processes we developed in the previous two years in the project, as described in WP2 and WP3.

In accordance with a key requirement established in the early stage of the EU-SEC project, the whole architecture is hosted within the EU. In particular, all Amazon resources are explicitly constrained in European availability zones, including the hosting of the CSA STARWatch SaaS application, which was duplicated and modified to support the features required for the EU-SEC project.

In addition to this technical validation, the pilot provided the opportunity for all project stakeholders to get a more concrete feel for the constraints and benefits associates with CaC certification:

- **CaixaBank**, as a cloud customer, was able to see some of the extra costs and benefit of relying on continuous audit-based certification for sensitive applications in the cloud.
- **Fabasoft**, as a cloud provider having implemented some of the "APIs" needed to become "auditable" by the audit tool, had a view of the cost associated with continuous certification.
- **Fraunhofer** and **SixSQ** as technology providers, demonstrated their solutions in a novel context.
- **CSA** acting as a certification scheme owner, hosting a public registry of certified cloud services.
- **NIXU**, as an auditor, was in a position to understand how they might use such a framework with its own customers.

In addition, the project was showcased at a workshop in Barcelona in April 2019 to external stakeholders, which were able to provide a fresh view of our work and offered some useful feedback in the process.

Based on all these inputs, this deliverable D5.3 concludes WP5 and presents a summary of the feedback and insights we gathered from the pilot, using the following structure:

- **Section 2** provides a tool adequacy review from the point of view of an Auditor and additionally presents more informal feedback we received from cloud customers.
- **Section 3** presents the feedback from all stakeholder in the project, including EU-SEC partners, the External Advisory Board (EAB) members and external stakeholders that participated in our workshop in Barcelona.
- **Section 4** looks at the potential control coverage afforded through continuous auditing, looking first at the pilot, and next looking at theoretical coverage limitations, mainly due to the difficulty to automate some assessments.
- **Section 5** concludes the document with an outlook on the future development of the framework and one potential roadblock that will need to be addressed.

To fully understand the context and terminology used in this deliverable, it is advised to first get familiar with the EU-SEC project's deliverables D2.2, D5.1 and D5.2 which lay the basis for understanding the continuous audit-based certification model, pilot architecture and the included requirements.

2 TOOL ADEQUACY SUMMARY

This section provides an overview of the tools used in the pilot, from the point of view of NIXU, acting as an auditor and "end-user". NIXU did not participate in the development of the tools. As a consequence, they are in a good position to evaluate the pros and cons of the various tools in the pilot, from the perspective of a certification body.

2.1.1 CLOUDITOR

Clouditor is used to design and execute the selected assurance tests from on the target environment by collecting the evidence from selected controls as planned. Collection of the evidence can be modified based on the SLO/SQO criteria created for each control. As addressed earlier during the EU-SEC project in D5.2, automated tests can mainly be applied to technical SLO/SQOs, whereas organizational SLO/SQOs tend to require human input to be validated. For controls that can be automatically monitored, the pilot showed that Clouditor provides an adequate solution. From an auditor's perspective, a tool like Clouditor can be seen, within its limitations, as a helpful tool minimizing efforts for evidence collection in Continuous Auditing. One limitation of the pilot is the amount of SLO/SQOs that can be automatically monitored. Nevertheless, this limitation can be easily fixed in further development steps.

As described in D2.1, all tools should be fully audited before being used in a continuous certification scheme. As a consequence, tools such as Clouditor will need to be certified and trust must be built in auditor communities to achieve broad adoption.

Good: Clouditor is adequate for collecting SLO/SQO-based information from selected controls. It can provide real-time information about the status of audited controls.

Needs to be improved: In the future, it will be important to demonstrate Clouditor on a broader number of controls, derived into SLO/SQOs. Of course, as the pilot mostly aimed to test the functionality of the application, only a subset of all possible controls were included in the application. But beyond the pilot, the tool will need to demonstrate that it scales to a fully representative set of technically monitorable controls.

Missing: The monitoring application must be trusted. In a real audit, this application will need to be certified from development to implementation to gain trust among auditors, as envisioned in the EU-SEC framework.

2.1.2 NUVLA

Nuvla is used to store collected evidence. Nuvla is an application management service for cloud, edge and hybrid environments. Nuvla is an extremely flexible tool that can be adapted to almost any scenario in terms of location and architecture, which is both a strength and an opportunity for misconfigurations. At this point Nuvla hasn't got any security-related certification and to gain trust in order to be used in an audit, it must be certified. It provides good functionalities to store technical evidence collected by Clouditor. Nevertheless, it must be noted, that there must be clear risk-based analysis done to evaluate where the collected information can be stored (due to classification of the data). From the point of view of security, Nuvla's most critical features are authentication/authorization, transfer security and data-at-rest security. The data processing facilities and the technical architecture used to operate Nuvla must be separately audited and certified in order to gain trust for the end-user and auditor communities.

Good: Nuvla is adequate for storing the SLO/SQO based information collected using Clouditor. It offers flexibility to adapt to many requirements. It provides good functionalities to effectively manage and process the stored evidence.

Needs to be improved: At this point, Nuvla is only adequate for the storage of structured data. In the context of automated auditing it is more than enough. As a general development recommendation for additional features, it would be beneficial to develop Nuvla's abilities to work as a full audit evidence storage to cover other types of evidence, such as written documents and photos. This would make the work of an auditor and auditee much more efficient if all evidence could be placed in one accessible location.

Missing: Similarly to a monitoring tool such as Clouditor, Nuvla will need to be be certified from development to implementation. The physical location of databases and data should also be audited and certified to verify the application's security.

2.1.3 STARWATCH

STARWatch is used to evaluate the certification status of a cloud service based on collected information. It is a SaaS application enabling users to perform self-assessment using CAIQ, a questionnaire based on CSA's CCM. In a continuous auditing process, STARwatch acts as a repository for continuous certifications: it maintains the status of the certificate by verifying whether it is still valid based on the results submitted by a monitoring tool such as Clouditor.

Good: STARWatch can work as a central location to collect assessment results from automated continuous auditing architecture and at the same time can be used to collect assessment results from human-based audits. As such, it provides one central location where to find out the status of the full audit. From the user's perspective it is easy to use and understand (certification status is valid/suspended/revoked depending on the assessment data).

Needs to be improved: For now, the application works as required by the architecture. However, it must be kept updated and under continuous development to address the needs of the continuous certification in the future as well.

Missing: STARWatch could work as a central location for all cloud-based continuous certification schemes but at this point, it solely focuses on the CSA CCM.

3 STAKEHOLDER FEEDBACK

This section provides a summary of the feedback provided by all stakeholders involved in the pilot. We first start with project partners and we follow with external stakeholders, based on the workshop we conducted in April 2019 in Barcelona.

3.1 CAIXABANK

From CaixaBank perspective, as a Cloud Service Customer, the continuous audit-based certification deployed in EU-SEC provides an interesting approach to increase the level of trust in a cloud service, by continuously assessing that a set of requirements specified to deploy a new cloud service are achieved. As such, it also helps to demonstrate trustworthiness to our own customers, which can positively enhance the reputation of the company towards its clients.

Furthermore, continuous certification also positively enhances our reputation towards regulators, which is potentially as important as our reputation towards our clients. The feedback obtained from regulators when attending the demo and training sessions of the pilots was very positive (See 3.7). They considered the pilot as a promising approach for enhancing the control of the CSPs in very sensitive sectors such as banking, having a more exhaustive and automated control of privacy and security features while migrating services to the cloud. If the level of reputation and trustworthiness towards the financial institution

increases from the regulator perspective, that could lead to more relaxed reviews and demands and faster processes for new cloud deployments and business operations in general.

Moreover, the EU-SEC continuous certification scheme aligns with the recently released (7th June 2019) *CSP CERT WG Recommendations for the implementation of the CSP Certification scheme,* which included that, "*considering the ever-evolving threat landscape for cloud services, a continuous certification process (which may include a continuous monitoring component) should be adopted as part of the requirements for a substantial and high certification."* With our experience in the pilot, we are in a good position to address such a recommendation.

Cost reduction is also taken into account considering that a continuous audit-based certification approach can reduce the number and complexity of point-in-time auditing and can reduce the amount of dedicated effort and personnel from the cloud customer. The continuous audit approach presented in EU-SEC does not completely remove the point-in-time audit, but it is only necessary for the certification that the technical architecture is still working as defined in the previous point-in-time audit. It can have a big impact in a large company, but it could imply an impact even larger for SMEs, which generally do not have dedicated people for those purposes.

Finally, it has a benefit in cloud vendor lock-in avoidance. The EU-SEC technical architecture provides a way for small CSPs and SaaS applications to be certified more easily and gain trust faster. That could enable their solution to achieve a similar level of trustworthiness of a large commercial provider. Hence, it can stimulate faster migrations from one cloud to another because the security assessment process would be also reduced (moving to cloud already with Continuous Audit-based Certification, or certification process easily automated).

Evaluation criteria from Cloud Customer perspective

EU-SEC CA Technical Architecture allows monitoring all the requirements

The first evaluation criterion is the validation of EU-SEC CA Technical Architecture as a mean to continuously monitor all the requirements previously defined in the scope of the audit. In the case of the pilot, the four high-level requirements (data location, data encryption, identity federation, logs stored in SIEM) defined by CAIXA are mapped consistently to several SLOs/SQOs (as defined in *EU-SEC Deliverable 5.2 - Section 3.2*) and continuously monitored.

EU-SEC CA Technical Architecture allows to monitor/validate the requirements by means of external tools (without the feedback of the CSP)

Even if the EU-SEC architecture provides a continuous monitoring and automated validation of the SLOs, it generally relies on the communication with the CSP, by means of the EU-SEC CA API. This approach will allow a faster extension of the number of supported clouds because it can provide an effective way to small cloud providers to be certified and assure a certain level of security to cloud customers. However, it still requires placing trust in the CSP in order to validate that the information provided is trustworthy. In the case of IaaS approaches, the service depends on the IaaS provider as well as on the application provider that has deployed the application over the IaaS platform. EU-SEC CA API directly requests the information of most of the SLO/SQOs from the IaaS provider, instead of the application provider. It means that once the continuous auditing APIs of AWS, Microsoft Azure and other large commercial IaaS providers are standardized and certified, the validation process of new applications over those IaaS providers will be simpler and faster.

EU-SEC CA Technical Architecture scalability/independence to the CSP

The EU-SEC architecture allows a fast and easy integration of multiple CSPs under the continuous audit-based certification thanks to the EU-SEC CA API. This API allowed integrating the two use cases (IaaS and SaaS) and it presents an approach to integrate other CSP in a scalable way.

EU-SEC CA Technical Architecture Security

NIXU has reviewed the architecture operation and has provided a set of recommendations for the data and evidence management, as well as other security aspects and features to take into account in order to assure that the EU-SEC CA Technical Architecture is completely secure. However, a complete security audit would be needed to assess and certify the security of all the modules of the architecture.

EU-SEC CA Technical Architecture provision of evidence

Clouditor is providing evidence records according to the requirements defined by CAIXA. The pilot has been tested including different approaches for external and on-premise evidence stores. It demonstrated also certain flexibility in the definition of the evidence store location, allowing the cloud customer to select the best option depending its profile, business sector and the characteristics of the service to be deployed.

3.2 FABASOFT

As a Cloud Service Provider, Fabasoft has to deal with various certification schemes and their ongoing proliferation. This imposes a growing workload on employees, to monitor and check controls for all kinds of requirements for numerous schemes. It is Fabasoft´s strong belief that Continuous Auditing is a solution and countermeasure to this growing workload.

To achieve a good coverage of controls to be continuously audited, Fabasoft looked at the pilot in working package 5 as a proof of concept and helped to drive the idea of a specific Continuous Audit API, which enables tools like Clouditor to automatically, continuously verify the specified requirements. In the case of this pilot these were a few chosen requirements, set up by the project partner CAIXA. In the opinion of Fabasoft, the pilot is a success, because it shows that the efforts for continuously auditing certain controls are not skyrocketing:

Effort of implementing a pre-defined Continuous Audit API as a Cloud Service Provider

Fabasoft uses its own domain-specific language for the technical base of the Fabasoft Cloud SaaS: *app.ducx*, which is a domain-specific language for developing composite content applications based on use cases. With such a domain-specific language, solutions for documents, case handling and business process management can be developed quickly and cost-efficiently. Therefore, with this tool at hand, it is straightforward for Fabasoft to set up the Continuous Audit API, regarding the EU-SEC definition. With a full-fledged API definition available, the effort to implement and test the API can be estimated to 2 workdays:

- Setting up / administration a new Cloud App in the SaaS
  - Including the security standards for accessing the API
- Implementing a standard webservice to set the basic functionality
- Implementing the different calls / functions, specified in the swagger file (effort might vary, depending on the number/complexity of the calls)
- Testing the calls with some basic "CURL[2]" commands and verifying Clouditor "access".

It is safe to say that after leaving the prototype phase, the efforts for implementing a Continuous Audit API can be seen as quite low, meaning a CSP should be able to calculate with low costs on this part. Of course, such an API has to be maintained, but this is true for all audit-relevant evidence creation.

One element remains missing from Fabasoft's point of view: the cost of validating the API from an auditor's perspective. Indeed, the auditors need to be convinced that the API is trustworthy.

[2] CURL: command line tool and library for transferring data with URLs (https://curl.haxx.se/)

We can't estimate today what effort would be needed in order to "certify" the API in order to implement a full audit-based certification process as the project defined in D2.2.

3.3 SIXSQ

Nuvla (one of SixSq's flagship products) took the role of the Evidence Store within this pilot. Given that Nuvla is open source, we've tested two different deployment instances, each one bringing their own advantages to SixSq:

Using the publicly available Nuvla service[3]

In this case, the Evidence Store is a centralized service, publicly available to any registered user, and managed by SixSq.

With this setup, SixSq expected to first increase their user database by having the continuous auditing tools' users, auditors and auditees registering into Nuvla; and second, to obtain evidence records that could potentially be used (if allowed by the auditee) to assist in the continuous categorization of the quality of service of a CSP, which would ultimately aid other Nuvla users to optimize their selection of a CSP. The latter was unfortunately not accomplished, for several reasons: not enough evidence records collected; disparity of the tests performed in the continuous auditing; and the evidence records were unrepresentative of the CSP quality of service, given that the pilot was tailored for EU-SEC's use case.

The only possible recommendation for improvement here would be to increase and generalize the continuous testing to add more CSPs and different use cases.

Using a standalone on-premise instance of Nuvla

In this case, Nuvla has been deployed (and consequently managed) by CaixaBank. This ensures redundancy and additional privacy controls over the stream of evidence records being issued by Clouditor.

In this setup, SixSq was expecting to improve the user awareness about Nuvla and its internals. In result, this would help SixSq improve their user documentation and better market its tooling to the public. Such expectations were met, by working closely with CaixaBank during the deployment of their Nuvla instance.

[3] https://nuv.la

In both scenarios, SixSq was obviously expecting (and obtained) feedback from all involved parties in the pilot, about the usage of Nuvla and its respective interface for the management of evidence records.

3.4 FRAUNHOFER

Effort of implementing a pre-defined Continuous Audit API into a Cloud service as well as continuous auditing tool

The EU-SEC Project has developed the EU-SEC Continuous Audit API. It is an available Open Source definition of a set of REST API calls in a Swagger 2.0 format, available on GitHub[4]. This allowed for an automated generation of both a client as well as server implementation stubs for the API.

For integrating the API into a Cloud service, a node.js was automatically generated, already providing a stub of all REST endpoints. Additionally, an implementation of the mapping of the raw data produced by the cloud service to the data output of the REST endpoints was needed. There are essentially four types of mappings:

1. Log file information: all log files are constantly parsed and pushed into a mongodb database by a fluend daemon. In the process of calling the Audit-API endpoint the database gets queried according to the parameters of the REST request.
2. Database lookups: configurations that are persistent in a database are being queried and forwarded to the data output. Like certain settings of the web service stored in a MySql Database.
3. Config file lookups: The API logic reads a file at a predefined position and outputs the value.
4. Third-party API call: The request of a certain Audit-API call then triggers another REST-API, i.e. to the underlying Cloud provider, such as AWS or Azure. The result value gets mapped to the output of the Audit-API.

On the other hand, the API needed to be integrated into the continuous auditing toolchain, more specifically into Clouditor. Since Clouditor is an open source tool and allows for the extension of its "engines", the integration was straight-forward. The client, which communicates with the server-part of the Audit-API was autogenerated using the Swagger API

[4] http://github.com/eu-sec/continuous-auditing-api-spec

definition and is also available on GitHub[5]. Since Clouditor serves as a reference implementation to the overall technical architecture, the integration of the Audit-API into Clouditor was also made available, to further the adoption of the Audit-API[6].

In general, the implementation of the Audit-API was easily integrated into the Cloud Service and auditing tool.

3.5 NIXU

The CaC is particularly interesting for an auditor because it changes the traditional point-in-time approach completely by providing a method for continuous monitoring of an information system. This allows a completely new way of auditing which changes the business model from project-based services to continuous services. Therefore, this pilot was an excellent chance to test the approach and get a broader understanding of the model's possibilities.

The continuous monitoring provided by the CaC-model is a great opportunity for an auditor to make his/her evidence collection much more efficient. For example, the controls that can be automatically monitored can be checked much faster and more reliably with automated processes than by manually collecting the evidence. Humans are prone to errors whereas well-programmed machines can repeat simple tasks consistently. While increasing reliability, efforts required by an auditor are significantly reduced and the effort is targeted to evaluating requirements that can't be automatically monitored.

Nixu approached the pilot as a subject matter expert in cloud security assessments and provided its expertise along the way as the pilot progressed. Nixu's responsibility was to evaluate the architecture and its usability and security from the perspective of an auditor. This evaluation was based on documentation, interviews and joint workshops together with other partners. Since no technical testing as such was conducted, the analysis concentrated to evaluate whether the tools have any relevant security related weaknesses that would prevent the auditors from using the services.

The pilot showed that the tools have great potential and all the tools in the architecture are fit for purpose. When proper authentication and encryption methods are used, there shouldn't be any major security flaws in the architecture. Nevertheless, further development is still required to include more controls and standards to make the model more of a general tool

[5] https://github.com/eu-sec/continuous-auditing-api-java-client
[6] https://github.com/clouditor/clouditor/tree/eu-sec

which could be applied to all kinds of environments. Most importantly, trust towards the service must be increased to achieve broad adoption among auditors. One way of achieving this trust is to certify the architecture services as such. This is important since the auditor can't trust the results if the tool itself can't guarantee the integrity of the data. And of course, confidentiality of data is one of the top priorities especially when processing sensitive data. Lastly, the availability of the service itself must be ensured to primarily ensure collection of data and validation of the certificate and secondarily to make the auditor's work possible.

3.6 CSA

In the context of continuous certification, the Cloud Security Alliance aims to position itself as a certification authority that will:

1) Assure that the certification scheme is correctly implemented, using accredited certification bodies.
2) Address potential complaints from cloud stakeholders during certification,
3) Maintain a public registry of continuously certified cloud services, enforcing timely compliance reporting.

The pilot demonstrated that CSA has a path to address all these requirements from a technical point of view.

The pilot was an opportunity to globally confirm the technical feasibility of continuous certification, where different tools need to be integrated in order to provide continuous assurance. Importantly, the proposed continuous auditing architecture is largely technology neutral and can be adapted to different cloud service providers, different deployment models (IaaS, PaaS or SaaS), and other cloud monitoring tools, as alternatives to Clouditor.

The storage of evidence and the logging features added to STARWatch provide key instruments to address potential complains in the context of continuous certification.

On a lower level, the pilot enabled testing some of the key technical mechanisms supporting its role as a certification authority, through a modified version of the STARWatch SaaS application. The visible implementations of these mechanisms are:

- An API that enables a cloud service provider to upload a machine-readable *continuous certification target*, which describes a set of SLO/SQO and their associated assessment frequencies.

- An API that enables monitoring tools such as Clouditor to report the evaluation of each SLO/SQO, according to the frequencies defined in the *continuous certification target*.
- A public registry that lists all certified cloud services in real-time.

One of the challenges was the detection of failures to submit evaluations of SLO/SQOs in a timely manner, but CSA was able to find a solution that can scale across multiple certificates, with multiple SLO/SQO, each potentially with different validation frequencies.

Interestingly, for CSA, the pilot was also a timely demonstration of feasibility of continuous audit-based certification in the context of *the European Cybersecurity Act (EUCA), Title III, which aims to set the grounds to establish an EU-wide framework for cybersecurity certification of ICT services, products and processes, including those services provisioned by Cloud Service Providers (CSP)*.

In response to the EUCA, a working group called the Cloud Service Provider Certification Working group (CSPCERT WG) was set up and began working in April 2018 on recommendations for the certification of cloud services: *The objective of the CSPCERT WG is to explore the possibility of developing a European wide Cloud Certification Scheme in the context of the Cybersecurity Act and to provide the European Commission and ENISA with a set of recommendations that should be taken into consideration when implementing the cloud certification scheme*. These recommendations have been published in June 2019 and they have the potential to boost continuous audit-based certification, where CSA hopes to play a key role:

- The recommendations notably consider 3 target levels of assurance, depending on associated risk levels: basic, substantial and high. For high and substantial assurance levels, it is recommended to consider "continuous auditing" solutions as a policy (REC41).
- Crucially, the documents recommend *that ENISA assesses existing solutions for continuous auditing (like for instance the EC funded project EU-SEC) to understand how that can be leveraged to increase the level of assurance provided at level high* (REC83).

The pilot was thereby completed in what can now be considered as a favourable policy environment, providing proof that CaC is feasible. The EU has now an opportunity to lead the way in the adoption of continuous certification as a novel and stronger assurance tool for today's digital services.

3.7 WORKSHOP FEEDBACK: THE USER PERSPECTIVE

On April 9, 2019, EU-SEC organized a workshop in Barcelona designed to showcase CaC to a select group of stakeholders, which included cloud users in the financial sector and a national regulator.

The workshop started with a general presentation of the EU-SEC project, its goals, as well as the challenges and activities involved in developing the continuous auditing-based tool.

The presentation then continued with a description of the continuous audit-based certification architecture, and its translation into the concrete pilot scenario, as summarized in figure 1 in the introduction of this deliverable, with two variations of the FISH application.

Following these presentations, a hands-on demonstration of the tools was conducted, enabling participants to interact with the pilot.

The workshop was concluded with an extensive panel discussion, where participants offered a largely positive reception to CaC as developed in the EU-SEC project. The following paragraphs describe two interesting issues that were raised during the discussion.

3.7.1 AUDITING THE AUDITING TOOL

Workshop participants noted that the assurance provided by any continuous audit-based architecture that relies on automated tools to gather evidence and evaluate security objectives will largely depend on the trust that exists in those tools.

In the context of the project, the tools developed in the pilot were *de facto* assumed to be trusted. But of course, once continuous certification starts applying to real cloud applications, this question will need to be clearly addressed.

We can first observe that the same question initially applied to traditional certification were auditors need to be trusted for their competence, impartiality and independence. The solution to this trust issue has been the definition of formalized **accreditation** procedures for certification bodies that define criteria for the selection of auditors in a certification scheme. In essence, traditional auditors need to be "certified" in order to perform their work. As a cascading effect, we then trust that these auditors perform their assessments correctly.

The same should apply to certification tools used for continuous audit-based certification: they need to be audited to confirm they:

- "fit for purpose": the tools are designed to assess SLO/SQOs that satisfactorily describe the security of the information system under scrutiny.
- "trustworthy": the values reported by the tools can be trusted to correctly reflect the security or privacy attribute of the cloud service, in accordance with a predefined metric

Such an assessment is already an integral part the continuous certification model defined in Deliverable D2.2 of the EU-SEC project. In that model, an independent auditor is expected to conduct a "point-in-time" audit prior to the "continuous" audit. That "point-in-time" audit must notably include a validation of the continuous auditing tools.

Nevertheless, the fact that workshop participants still raised that point shows that we need to address this more concretely. As such, in May 2019, CSA started to contact some key cloud security solution vendors to initiate discussions regarding CaC. Reliable standards and procedures for the certification of audit tools will likely only emerge with an industry consensus from cloud monitoring solution vendors.

3.7.2 DISCUSSING CERTIFICATION STATUS

The other issue raised by cloud users at the workshop was about the way certification status is reported in the public registry, in particular with the notion of a "suspended" certificate. To understand their concern, we recall the current approach:

- If all objectives initially declared in the certification target are confirmed in due time, the certification of the cloud service is considered as **valid**.
- On the other hand, if an objective is not confirmed in due time, the certification is considered as **suspended** until the situation is corrected.
- If the certificate remains suspended beyond a specific duration, called the "grace" period, the certificate becomes **revoked** and gets removed from the public registry (a revoked certificate is never visible in the registry).

Cloud users suggested that the notion of a suspended certificate makes sense, but it could create confusion in the public eye because it suggests a non-compliance, which should lead to direct certificate revocation. In practice, the suspended state does not mean that a cloud service is non-compliant:

- If a tool or person fails to report that an objective is confirmed is due time, this might simply be a temporary failure of the tool itself or the supporting network and systems used for reporting.
- Even if a tool or person reports that an objective was not reached, this might not necessary lead to a critical non-compliance, as often there are compensating controls across an information system, which ideally assures that there is not a single point of failure.

But in terms of public perception, we understand the issue that was raised, and it will need to be addressed before the commercial exploitation of this framework. We currently consider two approaches that would need to be tested in the field:

Approach 1: Do not display certificate as "suspended" in the public registry but use the date of last validation instead.

In this approach, the public registry would display "Last valid on <date>" where <date> represents the last time the certificate was considered as "valid". As such, the suspended state would be kept as an internal state of the certificate but is not made public explicitly. Certificates would still get revoked after a grace period.

This approach came as a suggestion from discussions at the workshop.

Approach 2: Use more complex rules for revocation, distinguishing a delay in reporting from reporting a failure.

This approach builds on approach 1 but adds more complex rules for revocation. In this approach, we could mark some objectives as "critical": if this objective is reported as failed, the certificate is revoked immediately. On the other hand, if an objective is not reported in due time, the principle of a "grace" period would still apply, but the grace period would be defined per objective, instead of a global "grace" period that applies uniformly to all objectives.

Again, from a public perspective, certificates would either be marked as "valid" or simply removed from the registry as described in approach 1.

While this approach might be "fairer", it introduces an additional level of complexity that could discourage cloud service providers from undergoing this new type of certification, which is in itself a important paradigm shift.

4 CONTROL COVERAGE

One of the key insights of the EU-SEC project is to translate traditional information security control objectives into SLOs/SQOs, which can each be evaluated regularly in order to provide an enduring level of assurance to users of an information system. In order to be cost-efficient, as many SLO/SQOs as possible should be subject to automated assessment, as opposed to requiring human input.

In the pilot, we tested 15 SLO/SQOs covering 5 control objectives from CSA's CCM reference framework, which contains a total of 133 controls. While the objective of the pilot was not to cover as many controls as possible but rather to demonstrate the overall architecture of continuous audit-based certification, it is useful to examine the potential control coverage we can estimate to achieve, taking into account whether controls can be monitored automatically or not.

As such, this section examines the control coverage offered by continuous-auditing based certification, through several angles:

- Control coverage in the pilot.
- Estimated control coverage achievable through automation.
- Human intervention where automation is not achievable.

4.1 IN THE PILOT

The following table recaps the security objectives that were covered in the Pilot as a proof of concept. They represent 15 SLO/SQOs covering 5 CCM controls.

Table 1. Security objectives covered in the pilot

Data Location	**SLO/SQO**	**CCM control**
Local VM data	For all applicable sensitive data in scope, it shall be checked every 60 minutes that the persistent data location is known and trusted. • Evidence: Location attribute • Metric: Whitelisted locations • Result: Pass/Fail	CCM-GRM-02
Persistent Data Storage	Upon request of sensitive data by a software or database, it shall be verified that the delivery/processing location is within the European Economic Space. • Evidence: Location attribute • Metric: Whitelisted locations • Result: Pass/Fail	CCM-STA-05

Encryption	SLO/SQO	CCM control
Encryption on data at rest	It shall be verified that the data at rest is encrypted at all times with acceptable encryption method (AES-256). These checks shall be done in 5-minute intervals. (yes/no) • Evidence: Encryption method used • Metric: Acceptable encryption methods • Result: Pass/Fail	CCM-EKM-04
Encryption on data transfers (1/2)	When establishing new connections between applications, it shall be ensured that the HTTPS (TLS) connection is configured correctly according to industry best-practices. • Evidence: Connection information • Metric: Best-practice configuration • Result: Pass/Fail	CCM-EKM-04
Encryption on data transfers (2/2)	Whenever sensitive data is transferred between applications and/or databases it shall be verified that the application encrypts all of the sensitive data with appropriate encryption methods. • Evidence: Encryption method and related information • Metric: Whitelisted encryption methods • Result: Pass/Fail	CCM-EKM-04
Key management (1/3)	Encryption keys shall not be stored in cloud. Verify that encryption keys are not stored in cloud (Yes/no) • Evidence: URL of the storage location where the keys • Metric: Storage location of the keys • Result: Pass/Fail	CCM-EKM-02
Key management (2/3)	Verify that the keys for data in rest symmetric encryption are in possession of owner (Cloud Customer) (yes/no)	CCM-EKM-02

	• Evidence: Verification and answer by Cloud Customer (SQO out of the scope of the automated tests of controls) • Metric: Storage location of the keys • Result: Pass/Fail	
Key management (3/3)	Verify that encryption keys are stored in an accepted location • Evidence: Location attribute • Metric: Allowed location attribute list • Result: Pass/Fail	CCM-EKM-02
Secure ciphers	Verify that all encryption procedures are done with predefined and accepted ciphers (yes/no) • Evidence: Used cipher • Metric: Allowed cipher list • Result: Pass/Fail	CCM-EKM-04
Identity Federation	**SLO/SQO**	**CCM control**
VM access control	Identity administration federated to the administrator of CaixaBank	CCM-IAM-12
Application authentication	Authorization of applications shall be checked when access to sensitive data is requested. • Evidence: Application name and domain**.** • Metric: Access list. • Result: Pass/fail**.**	CCM-IAM-12
Platform authentication	Used platform shall be checked upon request to sensitive data: ○ Evidence: Platform name and domain**.** ○ Metric: White list of permitted platforms. ○ Result: Pass/fail**.**	CCM-IAM-12
Evidence Security	**SLO/SQO**	**CCM control**

Logging is done in real-time	All critical data must be logged in real-time. • Evidence: Check the last time the application and evidence records are collected. • Metric: Grace period from present time to last recorded log timestamp. • Result: Pass/Fail.	CCM-IVS-01
CAIXA SIEM synchronization	Log file of information pushed to CaixaBank must be updated whenever such information transfer is done. • Evidence: Check the connection of the different modules pushing evidence records into CaixaBank SIEM. • Metric: Grace period from present time to last recorded evidence record timestamp. • Result: Pass/Fail.	CCM-IVS-01
Location of logs	Location of log files • Evidence: Location attribute. • Metric: Allowed location attribute list. • Result: Pass/Fail.	CCM-IVS-01

All the SQO/SLO presented in the table above where successfully assessed by Clouditor in the context of the FISH application. Evidence was stored in Nuvla as well as in the SIEM of CAIXA. Results of the evaluation were correctly reported back to the STARWatch platform and published in the continuous certification registry. Compliance failures were simulated for all SLO/SQOs and immediately resulted in a temporary suspension of the continuous certificate, either because at least one result was reported as a "Fail" or because at least one result was not reported in a timely manner (see section 3.7.2 for details). When non-compliances were present for more than 2 weeks, the certificate was revoked and removed from the CSA public registry, following the rules defined in D2.1 and also briefly described in 3.7.2.

We must highlight that deriving a set of objectives from a series of controls and then implementing technical tests to validate these objectives requires a lot of effort in terms of analysis and development. The main reason for this is that there is no industry standard yet that supports this kind of work. While [ISO 19086-4] was released in early 2019, providing high-

level guidance for the creation of SLO/SQOs related to the security and protection of personally identifiable information, it does not provide the level of detail that "real world" SLO/SQO need to offer. Nevertheless, as continuous monitoring becomes more common, so will supporting tools and best practices.

4.2 AUTOMATION COVERAGE

The CCM version 3.0.1 offers 133 controls, grouped into 16 domains. As part of this project Fraunhofer did an evaluation of the level of automation that could be applied to evaluate each one of those controls. The table in Annex A summarizes the potential "automation coverage" of the CCM for continuous auditing. It basically classifies each control into 3 different categories:

- **YES:** It can be fully audited by automated means.
- **PARTIALLY:** A subset of objectives related to the control can be audited by automated means.
- **NO:** The control cannot be translated into a meaningful subset of objectives that can be audited by automated means.

It is important to stress that the existence of controls that cannot be audited by automated means does not imply that CaC is impossible. It simply means that some controls (or their corresponding objectives) will require human intervention for an audit and will therefore typically be assessed more rarely (e.g. every 4 months) to keep costs reasonable in the context of a continuous audit.

We further summarize the content of the Table in ANNEX A in the table below, where we show for each of the 16 domains in the CCM:

Table 2. SLO/SQO audit automation coverage

CCM Domain	Yes	Partially	No
Application & Interface Security	1	3	0
Audit Assurance & Compliance	0	0	3
Business Continuity Management & Operational Resilience	1	4	6
Change Control & Configuration Management	1	2	2
Data Security & Information Lifecycle	1	5	1
Datacenter Security	1	3	5
Encryption & Key Management	1	2	1
Governance and Risk Management	0	1	10

Human Resources	2	5	4
Identity & Access Management	3	7	3
Infrastructure & Virtualization Security	6	4	3
Interoperability & Portability	1	2	2
Mobile Security	6	3	11
Security Incident Management, E-Discovery & Cloud Forensics	2	0	3
Supply Chain Management, Transparency and Accountability	2	1	6
Threat and Vulnerability Management	0	2	1
Total	28	44	61

Globally, 21% of controls can be audited fully automatically and 33% can be partially assessed automatically. Conversely, a bit less than half of controls (45.8%) were considered difficult or impossible to evaluate automatically.

Most tellingly automation benefits domains that are technical in nature, such as "Infrastructure & Virtualization Security", "Identity and Access Management" or even "Data Security and Information Lifecycle". Domains that pose the greater challenge to automation are those that are governance and organizationally driven such as "Governance and Risk Management" or "Audit Assurance and Compliance". As domain, "mobile security" should be considered as a special case since it is a transversal domain, with elements of both technical and organizational dimension.

4.3 HUMAN INTERVENTION

As stated above, slightly less than half of the controls in the CCM do not lend themselves to automation. Indeed, a quick look at the CCM shows that the words "policies and procedures" appear in 48 controls.

These findings confirm one our initial intuitions: continuous monitoring should be seen as an enhancement to traditional certification, not as a replacement. The strongest assurance will be obtained by first conducting a traditional "point-in-time" audit where organizational aspects can be thoroughly investigated, followed by a continuous-audit that will focus on technical objectives that can be automatically evaluated. This was reflected in the certification models we defined in Deliverable D2.1.

As demonstrated in the pilot, the STARWatch application has been enhanced with API endpoints that allow machine inputs, such as provided by Clouditor. Nevertheless, during the

development of the EU-SEC Pilot, STARWatch was also enhanced to allow human input, enabling auditors to provide input related to objectives that cannot be automatically evaluated.

5 OUTLOOK AND POTENTIAL ROADBLOCKS

From the results of the pilot, we can positively answer the 3 questions we stated in the introduction of this document.

1) Yes, the tools work together as expected, enabling a continuous audit of 15 SLO/SQOs. The pilot summarized in section 1.2 was demoed multiple times to various stakeholder, testing both success and failures for each SLO/SQO. All tools are correctly integrated and work as expected.
2) Yes, the pilot shows that the tools adequate for the task. As described in section 2, NIXU reviewed the tools and concluded that they are adequate for the purpose of the pilot. In addition, during the workshop external stakeholders were also able to use the tools and see how they reported compliance in real time.
3) Yes, the internal and external stakeholders were able to witness the practicality of continuous audit-based certification. The feedback provided by internal stakeholders in this deliverable is generally positive, as summarized in section 3. The workshop organized in Barcelona was received with marked interest and vibrant discussions.

Some interesting feedback we received comes from questions we didn't ask initially. The pilot suggests that one potential roadblock needs to be more carefully addressed in order to transform our architecture into a viable certification framework: building trust in the continuous auditing tools. Indeed, in section 2, NIXU's feedback was largely dominated by the question of certifying the tools. And while the EU-SEC framework clearly identified early on the need to include a validation of the tools in the certification process, feedback from the workshop tells us that we still need to detail more precisely "how" this will be achieved. It also remains a question mark in terms of cost as noted by Fabasoft in the end of Section 3.

Section 4 provided a review of the control the coverage provided in the pilot as well as a discussion of the theoretical level of automation that can be achieved in a CaC. One thing is clear: translating traditional control objectives into SLO/SQO requires some significant effort because we cannot rely on existing standards and best practices. A new landscape needs to be created here.

As the EU-SEC project comes to an end and beyond, we will focus on getting more feedback from industry stakeholders in order to address these potential roadblocks. Frist, we will get a

better picture of the requirements for the certification of audit tools, as envisioned by the EU-SEC for the purpose of evaluating SLOs and SQOs. CSA has begun contacting cloud security solution providers in order to start this effort. Next, a review of existing tools in the market will also provide a better understanding of what kind of SQOs and SLOs can be realistically be defined in the current state of the art.

In related news, Fraunhofer AISEC has released an open-source version of Clouditor, the "Clouditor Community Edition" available at https://github.com/clouditor/clouditor. An open-source audit tool is also an opportunity to build trust by letting anyone examine the code and integrate best practices in cloud monitoring to the benefit of the community.

But perhaps the greatest opportunity for continuous audit-based certification comes from the freshly released recommendations from the CSPCERT Working Group discussed in 3.6 [CSPCERT], which recognize continuous auditing as a key component for assurance cloud assurance. This policy document asks ENISA to examine the feasibility of continuous auditing: this pilot shows that it can be done.

APPENDIX A ASSESSMENT AUTOMATION

Control name	Control ID	Coverage
Application & Interface Security Application Security	AIS-01	partially
Application & Interface Security Customer Access Requirements	AIS-02	partially
Application & Interface Security Data Integrity	AIS-03	yes
Application & Interface Security Data Security / Integrity	AIS-04	partially
Audit Assurance & Compliance Audit Planning	AAC-01	no
Audit Assurance & Compliance Independent Audits	AAC-02	no
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	no
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	partially
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	no
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	partially
Business Continuity Management & Operational Resilience Documentation	BCR-04	yes
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	no
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	partially
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	no
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	partially
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	no

Business Continuity Management & Operational Resilience Policy	BCR-10	no
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	no
Change Control & Configuration Management New Development / Acquisition	CCC-01	no
Change Control & Configuration Management Outsourced Development	CCC-02	no
Change Control & Configuration Management Quality Testing	CCC-03	partially
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	yes
Change Control & Configuration Management Production Changes	CCC-05	partially
Data Security & Information Lifecycle Management Classification	DSI-01	partially
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	partially
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	yes
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	partially
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	partially
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	partially
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	no
Datacenter Security Asset Management	DCS-01	partially
Datacenter Security Controlled Access Points	DCS-02	no
Datacenter Security Equipment Identification	DCS-03	yes
Datacenter Security Off-Site Authorization	DCS-04	no

Datacenter Security Off-Site Equipment	DCS-05	no
Datacenter Security Policy	DCS-06	no
Datacenter Security Secure Area Authorization	DCS-07	partially
Datacenter Security Unauthorized Persons Entry	DCS-08	no
Datacenter Security User Access	DCS-09	partially
Encryption & Key Management Entitlement	EKM-01	yes
Encryption & Key Management Key Generation	EKM-02	no
Encryption & Key Management Sensitive Data Protection	EKM-03	partially
Encryption & Key Management Storage and Access	EKM-04	partially
Governance and Risk Management Baseline Requirements	GRM-01	partially
Governance and Risk Management Data Focus Risk Assessments	GRM-02	no
Governance and Risk Management Management Oversight	GRM-03	no
Governance and Risk Management Management Program	GRM-04	no
Governance and Risk Management Management Support/Involvement	GRM-05	no
Governance and Risk Management Policy	GRM-06	no
Governance and Risk Management Policy Enforcement	GRM-07	no
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	no
Governance and Risk Management Policy Reviews	GRM-09	no
Governance and Risk Management Risk Assessments	GRM-10	no
Governance and Risk Management Risk Management Framework	GRM-11	no
Human Resources Asset Returns	HRS-01	yes
Human Resources Background Screening	HRS-02	no

Human Resources Employment Agreements	HRS-03	partially
Human Resources Employment Termination	HRS-04	no
Human Resources Mobile Device Management	HRS-05	partially
Human Resources Non-Disclosure Agreements	HRS-06	no
Human Resources Roles / Responsibilities	HRS-07	yes
Human Resources Technology Acceptable Use	HRS-08	partially
Human Resources Training / Awareness	HRS-09	partially
Human Resources User Responsibility	HRS-10	partially
Human Resources Workspace	HRS-11	no
Identity & Access Management Audit Tools Access	IAM-01	no
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	partially
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	yes
Identity & Access Management Policies and Procedures	IAM-04	yes
Identity & Access Management Segregation of Duties	IAM-05	partially
Identity & Access Management Source Code Access Restriction	IAM-06	partially
Identity & Access Management Third Party Access	IAM-07	no
Identity & Access Management Trusted Sources	IAM-08	no
Identity & Access Management User Access Authorization	IAM-09	partially
Identity & Access Management User Access Reviews	IAM-10	partially
Identity & Access Management User Access Revocation	IAM-11	partially
Identity & Access Management User ID Credentials	IAM-12	partially
Identity & Access Management Utility Programs Access	IAM-13	yes
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	partially

Infrastructure & Virtualization Security Change Detection	IVS-02	yes
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	yes
Infrastructure & Virtualization Security Information System Documentation	IVS-04	yes
Infrastructure & Virtualization Security Vulnerability Management	IVS-05	no
Infrastructure & Virtualization Security Network Security	IVS-06	yes
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	yes
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	yes
Infrastructure & Virtualization Security Segmentation	IVS-09	no
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	partially
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11	partially
Infrastructure & Virtualization Security Wireless Security	IVS-12	partially
Infrastructure & Virtualization Security Network Architecture	IVS-13	no
Interoperability & Portability APIs	IPY-01	yes
Interoperability & Portability Data Request	IPY-02	no
Interoperability & Portability Policy & Legal	IPY-03	no
Interoperability & Portability Standardized Network Protocols	IPY-04	partially
Interoperability & Portability Virtualization	IPY-05	partially
Mobile Security Anti-Malware	MOS-01	no
Mobile Security Application Stores	MOS-02	no
Mobile Security Approved Applications	MOS-03	no
Mobile Security Approved Software for BYOD	MOS-04	no
Mobile Security Awareness and Training	MOS-05	no

Mobile Security Cloud Based Services	MOS-06	partially
Mobile Security Compatibility	MOS-07	no
Mobile Security Device Eligibility	MOS-08	no
Mobile Security Device Inventory	MOS-09	yes
Mobile Security Device Management	MOS-10	no
Mobile Security Encryption	MOS-11	partially
Mobile Security Jailbreaking and Rooting	MOS-12	no
Mobile Security Legal	MOS-13	no
Mobile Security Lockout Screen	MOS-14	yes
Mobile Security Operating Systems	MOS-15	yes
Mobile Security Passwords	MOS-16	yes
Mobile Security Policy	MOS-17	partially
Mobile Security Remote Wipe	MOS-18	yes
Mobile Security Security Patches	MOS-19	yes
Mobile Security Users	MOS-20	no
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	no
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	no
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	yes
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	no
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	yes
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01	partially

Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	yes
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03	no
Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04	yes
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	no
Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06	no
Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07	no
Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08	no
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	no
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	partially
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	no
Threat and Vulnerability Management Mobile Code	TVM-03	partially

APPENDIX B REFERENCES

[ISO 27002] ISO/IEC JTC 1/SC 27, ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. https://www.iso.org/standard/54533.html

[CCM] Cloud Security Alliance, Cloud Control Matrix. https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview

[CSPCERT] CSPCERT WG, (Milestone 3) Recommendations for the implementation of the CSP Certification scheme, Borja Larrumbide Martinez and Leire Orue-Echevarria final editors, https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view

[EUCA] 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 526/2013 (Cybersecurity Act) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2019/881/oj