EUSEC
EU SECURITY CERTIFICATION

European Security Certification Framework

CONTINUOUS AUDITING CERTIFICATION SCHEME

1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 30. DECEMBER 2017

DELIVERY DATE: 26032017

AUTHOR:
Dorian Knoblauch, Fraunhofer Fokus

PARTNERS CONTRIBUTED:
CSA, PWC Germany, CAIXA Bank

DISSEMINATION LEVEL: PU

NATURE OF THE DELIVERABLE: R

INTERNAL REVIEWERS: NIXU, CAIXA Bank, CSA

*PU = Public, CO = Confidential

**R = Report, P = Prototype, D = Demonstrator, O = Other

This project has received funding from the European Union's
HORIZON Framework Programme for research, technological development
and demonstration under grant agreement no 731845

EXECUTIVE SUMMARY

This document is part of WP2 of the EU-SEC project.

EU-SEC is an extensive methodology for assessing the security level of cloud environments. In order to make this possible, EU-SEC does not only provide baselines and methods but also schemes that offer governance on implementation. This scheme lays out the principles, procedures, and methods for implementing continuous auditing. Continuous auditing introduces an enhancement for the traditional "point-in-time" certification by increasing the assessment frequency via automation and the continuous workflow. It is an approach of breaking controls down to their characteristic objectives and furthermore of providing suitable evidence on their fulfilments.

The document offers guidance on operationalizing the controls applied to an organizations' need for security and defines characteristics of automatable and non-automatable controls. Continuous auditing operates in phases and enables a trustworthy implementation, so that it provides assurance on compliance to all stakeholders. To implement this, a supporting governance structure is provided.

ABBREVIATIONS

Abbreviation	Description
CCM	Cloud Security Alliance Cloud Controls Matrix, a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance stated domains. (https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)
CSC	Cloud Service Customer
CSP	Cloud Service Provider - A cloud provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. (http://searchcloudprovider.techtarget.com/definition/cloud-provider)
ISMS	Information Security Management System (See Terminology and Definitions – Management System)
ISO	International Organization for Standardization (https://www.iso.org/home.html)
SLA	Service Level Agreement
SLO	Service Level Objective
SQO	Service Qualitative Objective

TERMINOLOGY AND DEFINITIONS

Term	Definition	Source
Assessment	Refers in this document to risk assessment, which overall process of *risk identification [ISO Guide 73:2009, definition 3.5.1], risk analysis [ISO Guide 73:2009, definition 3.6.1]* and *risk evaluation [ISO Guide 73:2009, definition 3.7.1]*.	ISO Guide 73:2009, definition 3.4.1
Audit	Systematic, independent and documented process for obtaining *audit evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled	ISO/IEC 19011:2011, 3.1
Audit evidence	Records, statements of fact or other information which are relevant to the *audit criteria* and verifiable.	ISO 9000:2005, definition 3.9.4
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	https://www.iso.org/certification.html
Continuous Auditing	An ongoing assessment process that aims to determine the fulfillment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.	EU-SEC D1.4
Continuous Certification	An information system is said to be the state of continuous certification if it meets a predefined set of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), which have been verified through continuous auditing.	EU-SEC D1.4
Control	Measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk	ISO/IEC 27000:2016

Term	Definition	Source
Information security control	A control, that in general lowers the risk information (and other correlated assets) is exposed to. Security requirements in this context is a set of information security controls, needed to achieve an envisioned level of information security in cloud computing environment.	
Risk	Effect of uncertainty on objectives, where uncertainty is the state of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.	ISO Guide 73:2009, definition 3.9.2
Security requirement	Customers have security requirements. In the procurement phase customers usually check which security requirements are met by the security objectives of the provider. This process is often referred to as due-diligence	ENISA MSM-DSP

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This certification scheme lays out the methods for establishing a continuous compliance assessment for cloud services based on security requirements. Focus of this scheme is to describe the necessary processes that will be executed during the assessments for the validation of controls in the scope of the certification. It enables the implementation of a continuous auditing infrastructure and provides a governance structure for this purpose. To establish trust over its implementation, this scheme also describes the necessary activities and conditions for the implementation of an approach that will led to a continuous auditing based certification, like, for instance, the operationalisation of security and privacy requirements.

This document is part of WP2 of the EU-SEC project. The EU-SEC project focuses on creating a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud. Part of this deliverable is to contribute to this promise of increasing efficiency of auditing and certification processes. It will be tested and validated in pilot involving industrial partners.

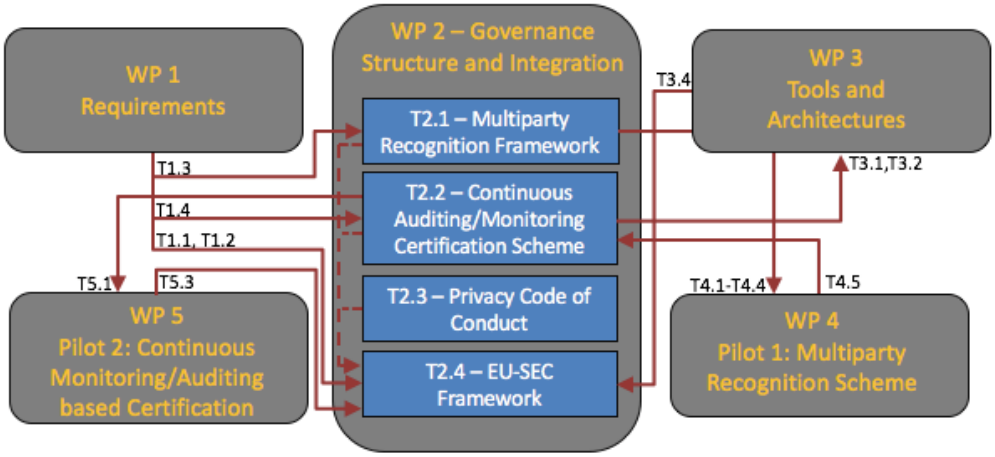

Figure 1: Work Package 2 Dependencies Diagram

Work package 2 presents itself with its tasks and dependencies as shown in Figure 1. This deliverable D2.2 takes into account the specific requirements from WP 1, task 1.4 (D1.4), as a basis for the continuous auditing certification scheme. Work package 3 will use this scheme as an input for implementing the tools necessary for continuous auditing. These tools are used

for the pilot in work package 5. The continuous auditing certification scheme developed here will be evaluated in the pilot of WP5 and the feedback might result in an update of the scheme.

1.1 SCOPE AND OBJECTIVES

The scope of this work is the development of a continuous auditing certification scheme and describes the principles, architectures and enabling methods. The focus of this document, as well as the overall focus of the EU-SEC project, are cloud security and privacy certifications. The implementation of continuous auditing will result in a more efficient compliance assessment and therefore introduces new ways of providing a proof of compliance according to an industry standard certification scheme.

It is important to remember that the objective of EU-SEC is not to issue a new certificate, but to provide the necessary framework to apply continuous auditing to new or existing cloud security certification approaches, like for instance CSA STAR or ISO/IEC 27001:2013.

While the principles, architecture and methods defined in this document focus on cloud computing, the approach defined in this document might be applicable to other business sectors to.

The scheme presented in this document consists of three enabling elements:

- Principles that are defining the foundation, directions and boundaries of continuous auditing. As well as the elements of interoperability with traditional point in time auditing.
- Architecture that facilitates the evidence gathering approach as well as support the achievement of the necessary levels of assurance in the process of continuous auditing.
- A guidance on how to develop measurement procedures for enabling the collection of evidence, on how to apply metrics and providing a measurement result.

It also consists of two organisational elements:

- A certification scheme framework that defines three assurance models. Those models differ in the involvement of an external auditor and therefore in the level of trust provided by a Governing Body.
- A governance structure that defines the key actors and processes for governing the certification scheme based on continuous auditing.

Activities within the scope of this work involve the exploration of the applicability and the boundaries of continuous auditing. While this document is based on existing definitions and concept (e.g. continuous auditing and continuous monitoring), it is also in the scope of this work to introduce necessary modifications and new definitions as well as procedures. The scheme models as well as the enablers are based on the existing point in time auditing approaches; the work done in this document shall be seen as an evolution of them. Since EU-SEC defines itself as a framework, the major focus of this methodology is in being applicable in various infrastructures, organisations and certification models. The emphasis on this scheme is to be applicable to all standard market certifications. A new continuous auditing certificate is not in this scope of this work but might be in the future.

The specific objectives of the work have been identified as follows:

- Enabling the process of continuous auditing via a set of principles, methods and implementations guidance.
- Providing a structured way of governing the continuous auditing implementation and execution.
- Developing processes for getting different levels of confirmation about the security characteristics of a cloud service via continuous auditing. These processes have to be applied in a scheme to asses if the information system is in the state of continuous certification or not, either because the certification has been suspended or because initial results are not sufficient to pass the first continuous certification threshold.

Activities therefore include the analysis of existing continuous monitoring and traditional auditing approaches as well as the traditional point in time auditing of a cloud service. A crucial part is also the exploration of boundaries and limitation of automatable assessments and suitable alternatives in case of the non-applicability of automation. All findings have to be introduced via an applicable process that enables continuous auditing.

1.2 METHODOLOGY

The development of this scheme was mainly driven by the need of improving traditional point in time certification and it is largely based on it, since this is the most common approach of getting assurance over the proper implementation of security requirements. While a point in time certification loses its topicality right after a manual audit is conducted and a certificate was granted, continuous auditing empowers to make precise statements on the compliance status at any time over the whole timespan in which the continuous audit process is executed.

Continuous auditing achieves this always up-to-date compliance status by increasing the frequency of the auditing process, for this purpose, it emphasizes on automating the verification of controls. With the need for being able to audit continuously at each given time, we have defined a simple methodology as shown in Figure 2 to improve on the existing scheme.

This new approach solves limitations by introducing new aspects, in our case we introduce, for instance, the classification of verifications into automatable and non-automatable, the automation itself and the assignment of reasonable frequencies. It is also important to note that when dealing with new aspects is crucial to not letting them become new limitations.

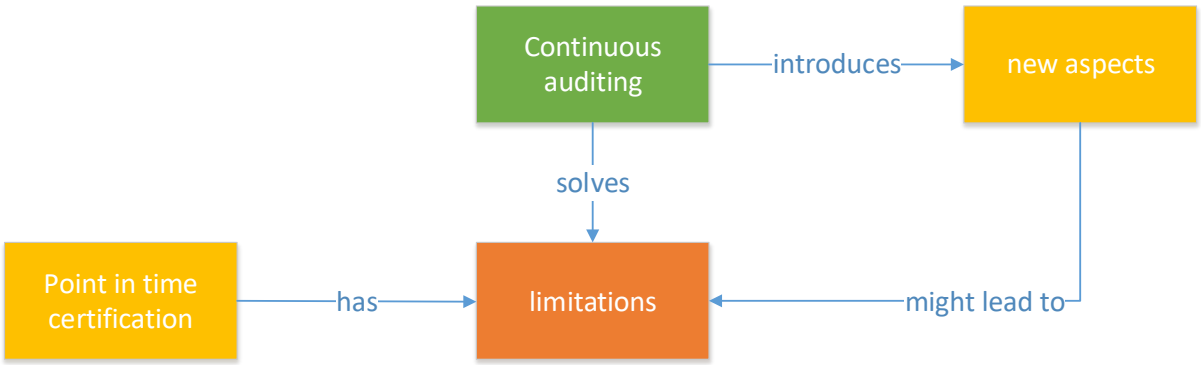

Figure 2: Methodology approach

The methodology for defining a new certification approach consists of the following steps:

1. Defining limitations of existing auditing
    a. Defining goals for new type of auditing which are addressing the limitations.
2. Elaborate on existing definitions and concepts. In this context what are the relevant actors, objects, procedures for point in time certifications?
    a. Adjust and exhibit definitions in new context. Verify if the existing definitions still suit the newly adjusted purpose. If necessary, adjust existing ones.
    b. Define new concepts if necessary. Sometimes adjustments cannot facilitate new aspect so new concepts have to be defined.
3. Model the interactions between concepts by defining relationships, procedures and results. E.g. the Auditee contracts an auditor.
4. Identify possible shortcomings.
5. Elaborate on shortcomings to avoid new limitations
6. Evaluate new approach.

2 CONTINOUS AUDITING CERTIFICATION PRINCIPLES AND CHALLENGES

2.1 POINT-IN-TIME CERTIFICATION VS. CONTINUOUS AUDITING CERTIFICATION

Let's take a step back here and summarize point-in-time certification and continuous audit-based certification. An in-depth description of both is provided in [1].

Point-in-time certification is well established and, looking at an ISO 270001 certification, it validates that an organisation meets a standard set of requirements. Compliance in this case is described with reference to a set of control objectives and controls: either the control is implemented or not. Some more advanced schemes may also rate the "maturity" of the control implementation, as done in CSA STAR Certification [2].

The control objectives are translated into a set of controls (i.e. measures mitigating risks), which are more concrete than the control objectives they originate from. They still contain abstractions, context dependencies and other elements that may require human intervention. The principle remains the same: compliance is expressed as a qualitative objective that is often described with a certain level of abstraction and might require assessment by a human [1]. In a nutshell, the assessment of the implementation of a control objective or a control will often result in findings that can be expressed using a simple nominal scale such a "yes/no/not applicable" or as an ordinal scale such as "Critical, high, medium, low, negligible".

In order to conduct a continuous auditing certification, evidence must be continuously collected and assessed with a frequency that will be expressed in minutes, hours, days or months, depending on the case.

A continuous audit is the continuous process though which an information system is assessed to verify that a predefined set of objectives, (e.g. SQO and SLO) are met [1]. Finally, **continuous audit-based certification** is defined as the regular production of statements indicating that an information system meets a set a predefined of SLOs and SQOs, each reported at an expected frequency through continuous auditing.

For continuous auditing the following processes take place:

- Information is collected from the information system.
- A measurement is applied to that information, according to a metric, and produces a measurement results.
- The measurement result is then compared to an SLO (Service Level Objective) or SQO (Service Qualitative Objective) to decide whether or not the objective has been attained.

Continuous auditing provides methods for verifying each control with a frequency that relates to a particular need. In this context, verifying a control means assessing the compliance to the objectives/requirements of a control at any point in time. It is important to note that each control has to be verified individually and with a specific frequency. If all the controls objectives within the scope of the audit are positively verified and if they keep their status at any time, a valid certificate can be issued and confirmed. This approach gives the stakeholders a much more up to date information on the security level of the cloud service provider based on a certificate.

However, this requires setting a frequency for verification of each control that is aligned with the assurance needs of an organisation. Those needs can be expressed in objectives, that can be referred back to the idea of Service Level, and more in particular to the key components of a Service Level Agreement, i.e. Service Qualitative Objectives and Service Level Objectives.

Given the need of increasing the frequency of the control verification, a key factor in implementing a continuous certification approach is "automation" as human intervention in the assessment process is a high cost factor. For this reason, continuous auditing strives for a high percentage of automated controls to allow higher frequencies at a lower cost.

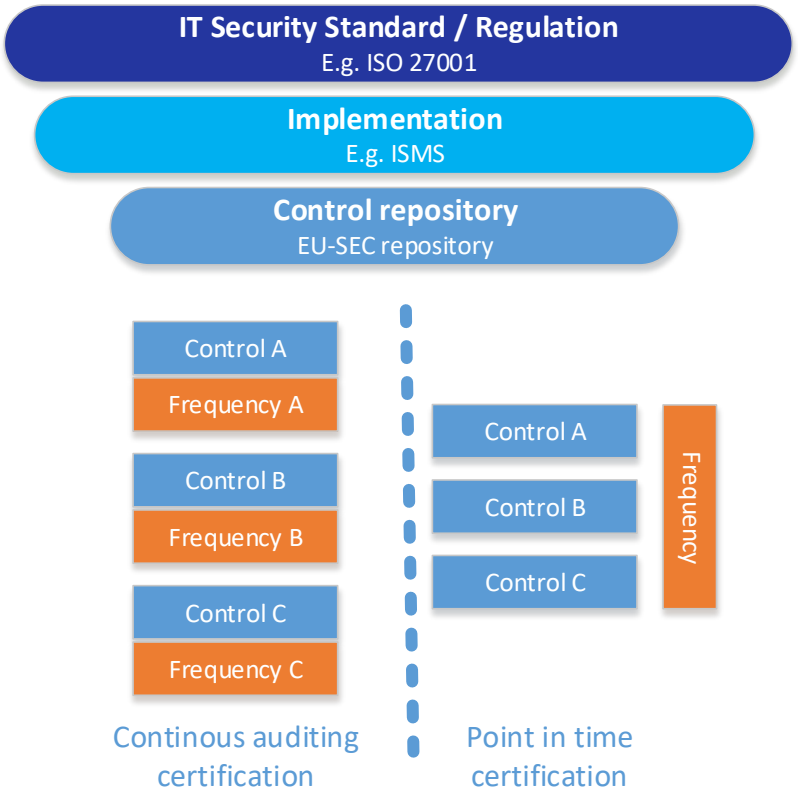

Figure 3: Comparison between point-in-time certification vs. continuous auditing certification

2.2 LIMITATIONS OF AUTOMATION

A more detailed explanation is given in chapter 4.1.2 in [1].

From a high-level perspective, risk management involves four important activities:

1) Identification: Identify environment, threats, risks and the risk appetite.
2) Analysis: Compute risks and select appropriate controls that mitigate those risks.
3) Implementation: Implement the selected controls.
4) Auditing: Verifying that the selected controls are in place.

This process is iterative: it is expected to cycle through these 4 steps constantly in order to adapt to a changing risk landscape. Certification of an ISMS will typically require that these four steps are implemented correctly.

The first three steps inherently require human intervention (that may be supported by computer assisted tools) through meetings, interviews, configuration, documentation, product selection, etc.

As for the fourth step, in an ideal world, we could take a set of controls from a reference such as the CCM and automated systems would verify the implementation of these controls on a continuous basis, leading to fully automated continuous auditing.

In practice, fully automation is difficult:

- First, for automation purpose the controls are at first translated into a set of technical and organizational measures, which are specific to the information system that needs to be secured. Automatically identifying the correspondence between a control and corresponding measures is not trivial.
- Second, some of these measures cannot be verified by automated means and require human assessment.

This is not to say that no automation is possible. On the contrary, one of the objectives of this project is indeed to automate auditing as much as possible wherever this is feasible. Some controls can indeed be translated into technical/organizational measures that are verifiable by automatic means. As discussed in this document, there is often a gap between what can be verified automatically and what a control encompasses. Yet the automated verification of the technical/organizational measures that underpin a control can provide us with strong confidence that the control is effectively in place. This automated verification, even if incomplete, would clearly provide a great boost to security in the cloud and elsewhere.

Since continuous auditing cannot be fully conducted by automated means, we need to also address the continuous verification of aspects of controls that require human intervention if we want to provide a complete framework for continuous certification in the cloud.

The main idea of continuous audit is to create a process were the verification of controls is "*conducted at a frequency requested by the purpose of audit*" [1]. All verifications, whether they are automated or not, share a common characteristic: they are constrained by time (a frequency). A control that is not verified in a timely manner is considered invalid. As a consequence, even for controls that require human intervention, there is one aspect that we can still control automatically: whether the evaluation took place within a predefined timeframe. We use this simple idea to integrate human intervention in our continuous framework as detailed in section 5.

Broadly speaking, automated verifications tend to target characteristics of a system, which can be counted, computed or evaluated as Boolean quantities, and then compared to a quantified objective. In contrast, many verifications which depend on a human assessment will be conducted against a qualified objective. In other words, automated verifications will tend to focus on SLOs, while non-automated verifications will lean towards SQOs (though these are not absolute rules).

A continuous auditing process, and therefore continuous certification is ultimately based on a combination of

- Automated verifications conducted regularly by specific tools.
- Human-led verifications that are time-constrained by automated tools

The solution we propose in this work takes both approaches into consideration.

2.3 CONCEPTUAL MODEL

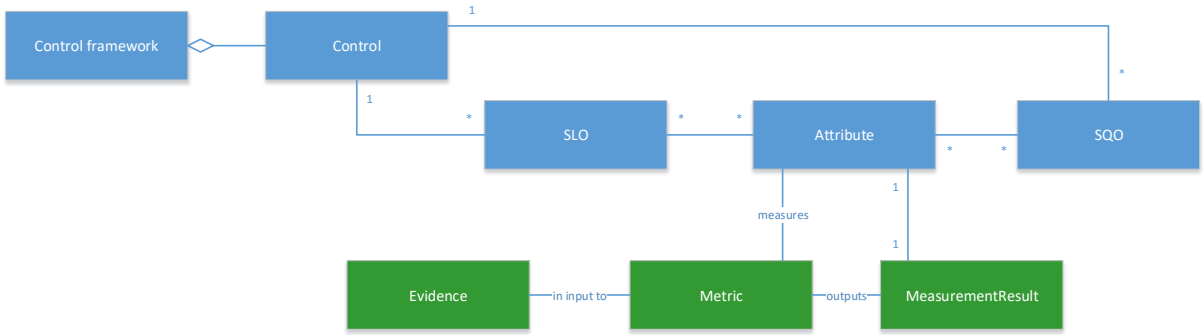

Figure 3: Conceptual UML model for continuous auditing

Figure 3 describes in UML notation the relations and hierarchy of the necessary components for continuous auditing. Blue represents the operational part and green the distinct technical, evidence producing level. This model describes the relations between the conceptual elements of continuous auditing. Each control framework (e.g. CSA CCM) consists of multiple controls, which are meant to give assurance on the fulfilment of a requirement. When preparing for a continuous auditing each one of those controls have to be described via its characterising objectives namely Service Level Objective (SLO) and Service Qualitative Objective (SQO). In the process, individually agreed-upon objectives have to be set per control. In this case an objective is specific to the requirements of the CSP. For instance, if one aspect of a control requires to monitor traffic this can be expressed in multiple objectives that may vary in number and goals. An IaaS provider will likely monitor inbound and outbound network traffic while a SaaS

provider providing a mail service may check incoming and outgoing emails. Objectives are described via multiple attributes; each attribute makes an aspect of the objective assessable. By assessing all those attributes, we can provide an evaluation on the achievement of the objective. In the example of traffic monitoring, possible attributes are type of traffic, unit or duration of monitoring. The concrete determination of an attribute is achieved via a measurement process. In this process information that either is obtained from an information system or that is produced manually is called evidence. A measurement is applied to that information, according to a metric, and produces a measurement result. This measurement result then provides a value for attribute.

Taking the CCM as our example framework and the particular control IVS-06 for the derivation of objectives, attributes and metrics. This control defines the necessity of network entities being securely designed, implemented, monitored and reviewed:

> *Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.*

What kind of objective gets derived, either a SLO or a SQO, depends on the implementing organisation and their capabilities. In this case the following way of operationalization is suggested:

- SLO
    - Configured to restrict between trusted and untrusted connections. In this case it is assumed that the configuration is measureable and expressible on an interval or ratio scale.
    - Configured to monitor traffic between trusted and untrusted connections. In this case it is assumed that the configuration is measureable and expressible on an interval or ratio scale.
    - Reviewed at least annually.
- SQO
    - Designed to restrict between trusted and untrusted connections.
    - Designed to monitor between trusted and untrusted connections.
    - Provide a document for justification of chosen configurations annually.

A possible attribution of the SLO to restrict traffic would be:

- Accepted input traffic rules
- Accepted output traffic rules

- Accepted forward traffic rules

A suitable metric for those attributes would be the ratio between valid configurations setting and all possible configuration parameters that ensure a restricted follow of data.

2.4 GAPS IN THE EVIDENCE CHAIN

Security Frameworks like the CSA CCM contains controls that are written in a comprehensive continuous text and their operationalization is mainly driven by the individual circumstances of the CSP and is adjusted according to factors like threat exposure or domain specific requirements. This operationalization of controls to specific objectives has to be performed manually and is subject to individual interpretation of the security practitioner. Likewise, during the audit process, contextual judgement in the interpretation of the soundness of the control implementation has to be applied. If the auditor is a human finding proper evidence that the objective of a control is met is not challenging. Semantic knowledge is not easy to implement, this is why same tasks as for now can't be performed by machines. Those limitation of course vary depending on the particular control under assessment, the more deterministic a control is the more likely is that the automated assessment could accurate.

To perform a continuous assessment of a control it's necessary to determine the characterizing SLO's and SQO's. Their attributes will define the finding.

The Objectives are determined by a metric and the corresponding measurement result provides the necessary evidence. This evidence is obtained either automatically by the tools within IT infrastructure or from a human assessment.

This process collection of evidences is bound to lead to two major challenges related to the semantic gaps created in the operationalization of controls (see Figure 4). The first gap might occur when deriving SLO's and SQO's from controls and the second one could result from implying that measurement results are evidence.

Figure 4: Possible semantic gaps

Let's elaborate this topic on the Example from 2.3 IVS-06 illustrates multiple possible gaps, resulting from multiple decision paths. One of the first decisions was to determine if an objective is an SLO or SQO. The control of a right configuration could have been also expressed in a SQO. The categorization of infrastructure entities into network environments and virtual instances depends on an individual judgement. Another example for a possible decision is the interpretation of reviewing, this could range from simply reading the documentation of the previous year up to a complete revise. Whenever a decision was made a gap is the result.

3 CONTINUOUS AUDITING CERTIFICATION ARCHITECTURES AND PROCEDURES

In this section, we describe the architectures and procedures for the implementation of continuous auditing.

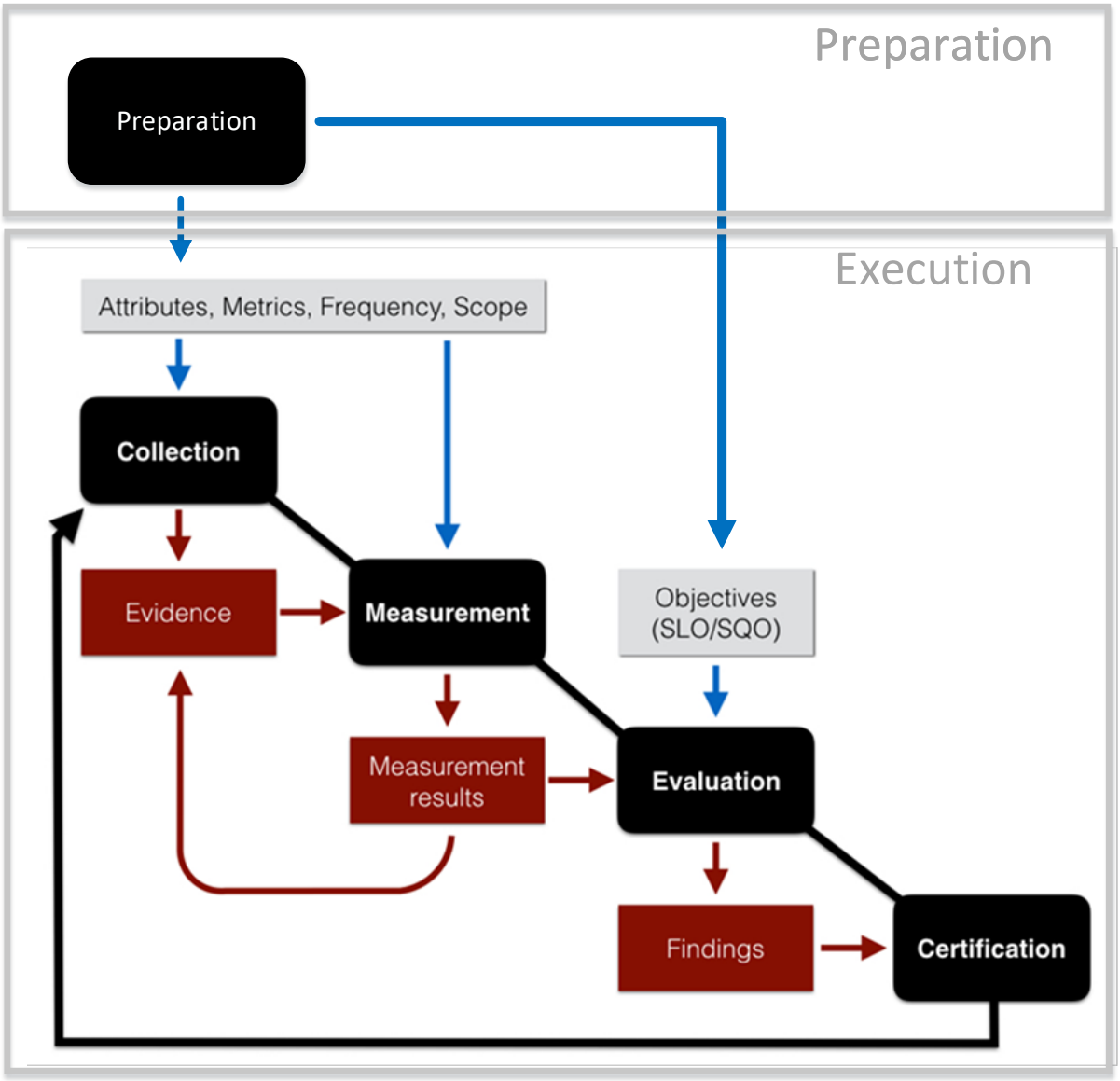

Figure 5 Model of continuous auditing phases

Certification via continuous auditing differs in the frequency of the verification of the controls compared to traditional "point-in-time" certification. While the "point-in-time" certification is an upright process performed at one time and producing one result at the end, continuous auditing is capable of giving assurance on the certification status continuously. This requires a specific suitable architecture that is capable of facilitating, both, automated and non-automated assessments. And also procedures that at one hand are implementing the proper operationalization of a control set and on the other are able to asses and provide the certification status continuously.

From a high level view the procedures can be separated into a "preparation phase" and the four "execution phases" (see Figure 5). The preparation phase produces specifications, which are the input for the following continually executed phases (see Figure 6).

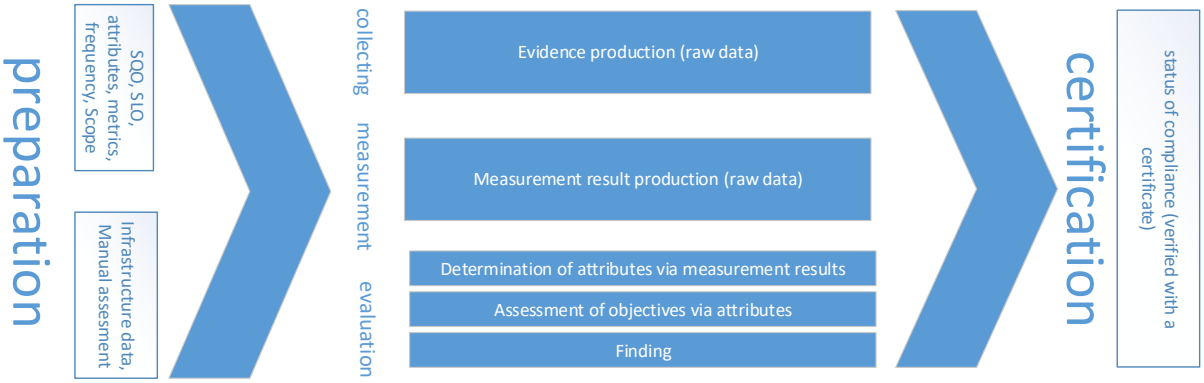

Figure 6 Model of inputs, processes and outputs

The architecture for continuous auditing has to facilitate the data gathering and processing as well as the data flow itself. The elements of the preparation phase are the input for the execution phases and result in a status of compliance (see Figure 6). The objectives, attributes, metrics, frequencies and the scope are utilized in the processes of the execution phases to process the infrastructure data and the manual assessments to a compliance statement.

3.1 PREPERATION PHASE METRICS COMPILATION METHODOLOGY

In the preparation phase the proper operationalization of the selected set of controls takes place. Key actions in this phase are the definition of the scope, the identification of the objectives (SQO, SLO) associated to each control, the determination of the frequencies at which each objective should be checked, the definition of attributes and metrics, as well as the identification of points where the measurements should be taken.

The EU-SEC scheme defines the following procedure for each control of a security framework:

1. According to the comprehensiveness and the coverage of a control a set of matching objectives has to be defined. According to requirement R-1.1 to R-1.5. [1]

   a. Objectives that describe a specific quantitative characteristic, where the value follows interval scale or ratio scale have to be defined as Service Level Objectives (SLO).
   b. Objectives that describe a specific qualitative characteristic, where the value follows the nominal scale or ordinal scale have to be defined as Service Quantitative Objectives (SQO).
2. Each Objective is described by defining attributes. Those attributes are more specific than an objective and do reflect just one measurable aspect of an objective. They are determinable via either a qualitative or a quantitative aspect.
3. Each attribute has to be assigned to a measurement procedure, which will provide a measurement result that describes the state of the attribute. Metrics have to be suitable for the infrastructure of the organization as well as the attributes characteristic. According to requirement R-1.7 to R-1.11. [1]
   a. The evidence is obtained on the infrastructure by performing measurements and stored in the evidence store.
   b. The measurement is than performed according to the metric.
   c. The measurement result expresses a qualitative or quantitative assessment of an attribute.
4. Since the process of operationalizing controls demands at certain points to compromise on the original control's statement, it is necessary to establish transparency. Therefore this process has to be documented. According to requirement R-1.6. [1]

Assistance for applying suitable measurement procedures is provided in chapter 4.

3.2 COLLECTION PHASE

The collection phase is the first step of the "execution phase" of an ongoing continuous auditing process. It facilitates the collection of data for the automated assessment as well as for the non-automated assessment. Collection of data is driven by the metric that has been chosen to provide input about an attribute. In the context of continuous auditing, data is referred to as evidence. Depending on the type of assessment the tools used could be various. Automated assessment is mostly driven by monitoring tools like log analytics, network statistics and monitoring, process statistics or resource utilization. While non-automated assessment requires humans to verify on the existence and the effectiveness of certain processes, and to read documents or examine records. In both cases the frequency at which the evidence is

collected is influenced by the objective and ultimately by the certification target. For reproducibility reasons the evidence gets stored in addition to being processed. The evidence collected in this phase can originate from various sources and therefore are in formats or representations which make proper processing difficult, for instance due to the unadjusted scale of two values or a log message that needs further processing.

3.3 MEASUREMENT PHASE

The measurement phase describes the processing that transforms the collected raw data into an usable measurement result. In the context of continuous auditing a measurement result quantifies or qualifies an attribute. Attributes require the measurement result to be in a particular format or representation. This way of conducting the measurement and interpreting the raw data is usually defined in a metric. Part of the control operationalization in the preparation phase, described in 3.1 was the assignment of suitable metrics for each attribute. This measurement phase is about the actual execution of the operations that qualify or quantify an attribute. The result can be considered an evidence like the raw data itself and should be treated and stored as the original evidence.

3.4 EVALUATION PHASE

In the evaluation phase the compliance status with the certification goal is determined by evaluating the controls. Technically a control is a set of objectives namely SLO's and SQO's and those have been derived from a control as laid out in section 3.1. Those controls are described as compilations of attributes, which are evaluated by a measurement. When the preparation phase was about deriving controls into attributes, then the evaluation phase is about compiling information on controls from attributes.

1. Evaluate the attributes.
    a. By performing a measurement.
    b. By requesting the latest value from the evidence store.
2. Assessing the control status by evaluation all corresponding attributes.
3. Evaluate the control status based on the evidence provided for each objective.

3.5 CERTIFICATION PHASE

The result of the evaluation has to be published according to the chosen continuous auditing certification scheme. In this document we propose three different models, which are laid out in section 5. All these three models share a set of common criteria, which are:

- The source of data has to be disclosed to the stakeholders, like for instance the CSC and the scheme owner. An allegation of quality has to include:
  - How the evidence data was collected, namely by human or automated assessment.
  - The frequency in which the result of the assessment gets updated.
- The assurance on truthful data does involve two traits:
  - An ethical statement from the CSP on the truthfulness
  - The implementation of technical safeguards into the data aggregation chain, which have to be traceable by the stakeholder.
- Data that is part of the continuous auditing process and is not confidential has to be published. This includes the values of the attribute, state of each objective and of each control.

Ultimately, the certification phase is about informing the stakeholders about the compliance status of an information system with a set of predefined objectives.

4 MEASUREMENT PROCEDURES

As described in section 2.3 a measurement provides assurance on the fulfilment of an attribute. In this context the measurement process consists of three elements which represent the three steps of data processing to obtain information on the attribute and ultimately on the objectives or SLO/SQO.

Figure 7: Measurement model

The core building blocks of defining a measurement is to decide on a meaningful metric are:

- Evidence can be reverted as the input in a measurement. Depending on the given factors it can vary from a single digit to an extensive unstructured document. The kind of evidence often defines whether it is suitable for an automated reasoning on an attribute or if its complexity requires a human interpretation. In an automated environment evidence is produced either via monitoring of already produced data or via a specific test. Those tests are often conducted by specific test suites, manually written scripts or enterprise targeted security monitoring solutions. In the case of evidence that requires manual intervention the number of sources is much broader in a sense that even a screenshot or a process documentation can for example be considered as valid evidence.
- Metric is the function that transforms the evidence into the measurement result. By doing so it implicitly gives it a unit and, in most cases, it normalises the output by returning a ratio or percentage value. Therefore, the metric requires a qualifiable or quantifiable measurable evidence to produce the result in an unambiguous manner.
- Measurement result refers to the output of the metric and does allow to reason on an attribute and ultimately on a control or objective.

Metrics are providing knowledge about the characteristics and attributes of an IT infrastructure, or in a broader context of organisational entities, through units, rules and the values from the analysis of the evidence. The evidence is processed into a measurement result via a metric. When looking at established security standards or regulatory constraints those are rarely focusing on a particular IT infrastructure. Commonly the focus is on security requirements and needs based on best practices or domain specific requirements, which introduces a challenge considering that evidences are obtained from a specific operating instance of an IT infrastructure. For example, CCM AIS-03 requires, among other aspects, data input and output monitoring routines for applications to be implemented. According to the kind of application the evidence that gets collected to obtain the status of the attribute does change. In an IaaS environment one possible evidence might be a documentation on reconciliation and edit checks on virtual storage changes like the creation of a backup, but in a SaaS application the evidence for the same objective has to be obtained totally different, e.g. a log file that proves the operation of the edit check. This example shows the difficulties when it comes to choosing proper evidence sources and therefore metrics. Those different types of evidence providing sources do not necessarily have to differ from one CSP to another. Technology changes do occur regularly, such as changes to certain API's or the selection of a different vendor. This issue has been addressed in in context of cloud services with the development of several metrics frameworks from different bodies. In the EU-SEC project we build on top of those

existing metrics frameworks by providing direction on applying metrics for continuous auditing.

4.1 BASIC CONDITIONS FOR IMPLEMNTING MEASUREMENTS

In the scope of continuous auditing, metrics are used to describe security related attributes and finally controls or objectives. The attributes have to hold up to certain principles to be considered of value in the process of continuous auditing. Those principles which are described in [1] as the base principles for continuous auditing. With regard to implementation those principles do vary in applicability, from not difficult up to challenging to apply.

Each principle has its own set of considerations to follow when being implemented:

- The repeatability principle requires the result of two independent entities that are conducting an audit of the same security or privacy attribute to be the same if the same scope and conditions are given [1]. On the level of measurements this means if the same measurement is executed twice under the exact same conditions the result should be the same. When speaking of automated measurement this is quite clear, since as long as the procedures are static and deterministic the results are the same. Setting up a manual measurement requires more elaborateness to ensure that the same measurements conducted by two different persons result in the same value.
- The equivalence principle requires a particular security or privacy attribute assessed on two independent systems to result in an equivalent security level if the measurement results are the same [1]. This refers to the unit of the metric as well as the particular attribute. This principle does more apply on traditional attributes that are part of SLA's, like availability and becomes more inapplicable when it comes to very specific attributes. The difficulty lays in the determination if the attributes are the same. Since the implementation of continuous auditing requires an operationalization according to a specific CSP it's likely that different attributes are the result. Equivalence implies comparability, which can be useful when comparing the same attributes of different IT infrastructure components or even the comparison between different aspects of CSP's when speaking of SLA's. But this introduces the major question of how the metric works. Are the evidences really comparable by using two metrics which might produce a result of the same unit but who are based on totally different premises? For example, let's

consider a suitable metric for the performance of vulnerability scans is the ratio between found vulnerabilities over known vulnerabilities. A widespread software component such as the apache webserver has more known vulnerabilities than an unknown self-developed solution. In the context of the EU-SEC project the emphasis is on certification which makes comparability is not the first priority. Measurements in the first place provide information on certain attributes, who are ultimately needed to assess the compliance to a set of controls. Measurement procedures therefore have to be expressive rather than comparable.

- The utility principle ensures to provide actionable information for provider of the certified system and its customers. In terms of measurements this means that all data that is gathered has to serve the continuous auditing process. Also, the collected data has to be of a quality that enables further usage in the compliance assessment.
- The trustworthiness principle requires the collecting, verifying and evaluation of evidence against audit criteria to be capable of providing a trustworthy representation of the security and privacy level of an information system [1]. The main consideration on this principle is how to establish trust among the whole process chain, beginning with the metrics. The automated as well as the non-automated implementation of the measurement does provide a way of ensuring the integrity of the evidence as well as the correct implementation of the proposed metric. Single evidences or even the whole continuous audit process can technically be secured, for instance by signing all data that's being produced while a continuous auditing. So, the whole chain of operations can be traced. It's more difficult to establish trust by traceability when an evidence is produced manually.

The implementation of metrics also introduces the issue of overlapping data sources or metrics. When using a single data source as evidence and then applying a metric to it and producing a measurement result this is a quite unambiguous way of assessing an attribute.

But an overlap can occur when two different measurement procedures are using the same data source, even if the measurement result and the metric itself are different. A loss of expressiveness is the consequence, which might lead to biased measurements. Other examples of overlaps are using the same measurement on the same control, using a joint of evidences on same level attributes or using the same attributes on objectives of the same control. Overlaps in general are good indicators for attributes or objectives being not distinctive enough, avoiding these overlaps is highly recommended.

Metrics do serve to quantify and qualify the level of which the CSP does meet the security and privacy requirements. Focusing on adherence with principals are secondary.

4.2 METHODOLOGY FOR DEFINING A MEASUREMENT PROCEDURE

Developing a measurement procedure is often an ad-hoc process aligned with the sources of evidence available. In the context of continuous auditing we propose the following methodology of developing a measurement. This methodology requires the attributes to be defined in a preferably atomic way. Which means that one measurement result has to be enough to attain a value for an attribute.

5. Decide on what's the most suitable source of evidence for the evaluation of an attribute in the following order:
    a. Research for proper data sources or tools that might produce machine readable evidences According to requirement R-1.1 and R-1.12. [1].
    b. If no exactly suitable machine-readable source of evidence can be provided, human readable source have to be considered According to requirement R-1.33. [1].
    c. In question of a less meaningful machine-readable evidence over a significantly more meaningful human readable evidence, go for the more precise one, human readable in this case.
    d. Base the metric on the specific need for information of the attribute, rather than just available data.
    e. Avoid same source of evidence for attributes of the same objective.
2. Identify the outcome structure of the measurement this includes:
    a. The achievable frequency, which is determined by the time of the measurement.
    b. The unit
    c. The gap between the knowledge that the evidence can provide and the need of information that is required to assess the attribute.
3. Define a metric that is transforming the evidence into a measurement result. According to requirement R-1.7 [1]
4. Review and test the metric.

4.3 EXAMPLES FOR DEVELOPING A METRIC

Applying measurement techniques to get information on organisational and infrastructural entities in the area of cloud services is widely researched and often manifests in frameworks and guidelines of public bodies. Their focus is not on comprehensiveness but rather on a specific targeted area, e.g., monitoring incidences or checking the vulnerability status. Although, they are focusing on security, the majority also emphasizes on SLA's and are often just relating to the IT infrastructure and less on the organisational requirements. This leads to a narrow coverage of a full-fledged standard like ISO 27001. The following lists a portion of documents supporting the development on a measurement:

- NIST Cloud Computing Service Metrics Description 500-307 [3] is about a cloud service metric model which can be applied to implement a measurement procedure in the context of continuous auditing. It proposes an alternative view on the metric composition by defining abstract metric, rule and parameter as characterizing elements of a metric. This document is still a draft.
- ETSI Information Security Indicators [4] are a full set of measurements or security indicators which do enable organizations to assess themselves accurately and to benchmark their level of assurance and the effectiveness of their security measures. Those proposed indicators are aiming at security incidents and vulnerabilities therefore only a fraction of the controls can be assessed with those indicators. It introduces a test framework to implement the majority of those indicators to be applied to live data continuously.
- Security metrics from the ESCUDO-CLOUD project [5]: The Appendix in this document represents the state of the art of cloud security metrics that is proposed from the industry and standards bodies. The list does not target completeness and is also a compilation from other sources like NIST or the CIS.
- ISO 19086-2 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric model [6]: This document has been developed to address the issues of incomplete, ambiguous, illogical, self-contradictory and undefined metric definitions. It provides help with the implementation by establishing a common terminology for cloud metrics and defines a model for specifying metrics. Examples do show the application of the model. Despite that this document is still a draft, it's of great value when implementing metrics.

5 CONTINUOUS AUDITING CERTIFICATION SCHEME

ISO/IEC 17000:2004 defines certification as the issuing by a third party of a statement declaring that the fulfillment of specified requirements has been demonstrated. In a traditional point-in-time certification, the fulfillment of control objectives by an information system (this is not the only element of course) is one of the key elements that has to be demonstrated. In continuous auditing-based certification, there are additional key elements to be considered, i.e. 1) demonstrating that auditing took place on a (near) continuous basis, 2) that the reporting happened in a timely manner and 3) that the information reported is accurate and unaltered.

Taking inspiration from the CSA Open Certification Framework, the EU-SEC project proposes a framework that contains three models for continuous auditing. Each of three models provides a different level of assurance by covering requirements of continuous auditing with various levels of scrutiny.

The three models that we define are represented in the Figure 8 and are:

1. **Continuous Self-assessment**
2. **Extended Certification with Continuous Self-assessment**
3. **Continuous Certification**

Figure 8: Assurance stack

Essentially the proposed framework starts from a simple certification of the timely submission of self-assessment compliance reports and moves up to a continuous certification of the fulfilment of control objectives. It should be noted that in two of the proposed levels, we rely on traditional "point-in-time" certification as a foundation to create by extension a continuously certified information system.

Before detailing these models in sections **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.** respectively, we will introduce a few concepts.

To describe these 3 models, we will refer to 3 main actors:

- **Auditee**: Organization being audited [1] (e.g. cloud customer or cloud provider).
- **External auditor**: A trusted party performing an audit with a view of delivering a certification or attestation for a cloud service. This trusted party is a qualified person or organization recognized by the Governing Body.
- **Governance Body** [7]: A trusted party that is responsible for the correct organization of a certification scheme, including the maintenance of a registry of certifications or attestations of cloud services.

We refer to "External Auditors" as opposed to simply "auditors" (as defined in [1]) to explicitly distinguish these actors from internal auditors and highlight that they have been qualified to perform audits by the Governing Body. In an ISO-style certification scheme, "external auditors" would be part of an "accredited certification body", also called "accredited registrar".

In the description of our models, the Governing Body performs several tasks. In practice, the governance Body may delegate some of these tasks to another trusted party.

In order to describe the three models, we will also refer to the following terms:

- **Finding**: Results of the evaluation of the collected audit evidence against audit criteria [1]. This notably refers to the result of an audit describing whether a control or SLO/SQO that is part of a statement of applicability is in place or not.
- **Continuous Audit-Based Certification Target (**from now on in this document **"The Certification Target")**: the combination of:
    - **A Reporting policy**: The policy describing how frequently findings for each control (or SLO/SQO) in the statement of applicability need to be updated, and the information related to it provided to the Governing Body (scheme owner).
    - **A Statement of applicability: T**he set of controls or SLOs/SQOs that are applicable to an audited cloud service, selected from a security baseline as the result of a risk assessment. [1]

The **Reporting Policy** specified in the "The Certification Target" should be pre-defined by the relevant **Governing Body** for each existing control/SLO/SQO, taking into account the best interest of all stakeholders and the nature of the technology implemented. We foresee the possibility to deviate from the frequency predefined in the **Reporting Policy** for a specific SLO/SQO in case the specific implementation of the control justifies an exception. Possible exceptions to the frequencies defined in the **Reporting Policy** of the **Certification Target** are to be foreseen especially in the case of the "Continuous Certification".

Controls/SLOs/SQOs that require human evaluation will typically have less frequent update requirements (e.g. monthly), whereas those that can be automatically evaluated will have more frequent update requirements (e.g. every 10 minutes). Deviations from the pre-defined frequencies prescribed by the Governing Body will need to be justified explicitly as described in the descriptions of models 2 and 3 (sections **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**).

All three proposed models can result in the issuance of a certificate that reflects the result of a continuous audit of a target cloud service, as reported to the Governing Body. Such a certificate has three possible states:

- **Valid**: a certificate is *valid* if all controls/SLOs/SQOs in the statement of applicability are declared to be in place and have been reported in a timely manner to the Governing Body according to the Policy.
- **Suspended**: a certificate is *suspended* if at least one of the following non-compliance conditions is true for a previously valid certificate:
    - At least one control/SLO/SQO in the statement of applicability was not reported to be in place in a timely manner to the Governing Body.
    - Following a complaint issued by a stakeholder, and after proper review by the Governing Body, it can be established that at least one control/SLO/SQO in the statement of applicability is not in place.

  A suspended certificate can become valid again if the non-compliance is corrected within a predefined "grace period".

- **Revoked**: a certificate is *revoked* if it remains *suspended* for a duration that is longer than a predefined "grace period".

The "grace period" is defined as part of the governance of the certification scheme and is enforced by the Governing Body. This "grace period" is measured with reference to the submission time limit set out in the Policy (e.g. 2 weeks after the submission time limit). The

Governing Body is responsible for keeping a public registry of all issued certificates, which lists all certificates that are either *valid* or *suspended*. If a certificate becomes *revoked* it is delisted from the public registry.

The nature of what is certified depends on the model selected, as detailed in each model description. Two of these three models are designed to complement existing certifications or attestations, and are therefore designed to be flexible enough to address various schemes such as ISO 27001, CSA STAR Certification, SOC2, CSA STAR Attestation, etc.

5.1 MODEL 1: CONTINUOUS SELF-ASSESSMENT

A continuous self-assessment is an assessment of a cloud service that is performed regularly by the Auditee, with results being published at a predefined frequency, under the supervision of a Governing Body.

5.1.1 FOUNDATIONS

Before any self-assessment can take place, the Governing Body will need to establish some foundations, notably:

1) Guidelines on establishing a suitable scope for self-assessment,
2) Specification of suitable control frameworks from which the Statement of Applicability can be composed of, in order to build the Certification Target,
3) Definition of acceptable Reporting Policies, to constitute the Certification Target.
4) Timeframes and rules governing the transition of certificates through various states ("valid", "suspended" and "revoked").

We note that the Governing Body may specify more than one Reporting Policy in order to reflect different assurance or sectorial needs. For instance, Policy ONE could be "each control shall be updated every month" which a flat policy applying to all controls, while Policy TWO (that for instance would reflect the specific needs of the Financial Sector) could be "Controls X, Y and Z, shall be updated every month, and controls A, C and C shall be updated every 10 days.

5.1.2 INITIATING THE PROCESS

At the start of the self-assessment process for a cloud service:

- The Auditee establishes a certification target by selecting a statement of applicability and a reporting policy for a cloud service and communicate it to the Governing Body.
    - The suitable reporting policy is selected form a list of possible reporting policies established by the Governing Bod, based on sectorial or assurance level considerations.
    - Deviations from the selected reporting policy are not permitted.
- The Governing Body creates an entry for the target cloud service in a publicly accessible "continuous self-assessment registry". This entry contains:
    - The submitted Certification Target.
    - A "start date" which defines when the certification target enters into effect as reported to the Governing Body.
    - A certification state, which is initially set as *valid*.

5.1.3 RUNNING THE PROCESS

After the start of the process:

- The Auditee performs a continuous audit of its cloud service, according to the Statement of Applicability defined in the certification target.
- The Auditee reports the findings of the audit to the Governing Body, according to the Reporting Policy defined in the certification target.
- Based on the timely submission of findings by the Auditee, as well as the review of any eventual complaint received from a stakeholder, the Governing Body establishes the state of the certificate issued to the Auditee as *valid* (or *suspended* or *revoked.)*. As noted previously, the Governing Body only certifies that the findings have been reported in a timely manner: it does not make any statement on the reality of the findings.
- The Governing Body continuously updates the corresponding public registry entry of the target cloud service with the state of the issued certificate.
- If the certificate becomes revoked, the public registry entry is removed, and the Auditee is required to begin the process from the start again.

No external auditor is involved in a continuous self-assessment.

The role of the Governing Body is to certify that findings are reported in a timely manner and that no valid complains have been issued against the Auditee with regards to the effective implementation of controls/SLOs/SQOs listed in the statement of applicability.

The Auditee is trusted to provide truthful findings. The Auditee is responsible for managing evidence and findings.

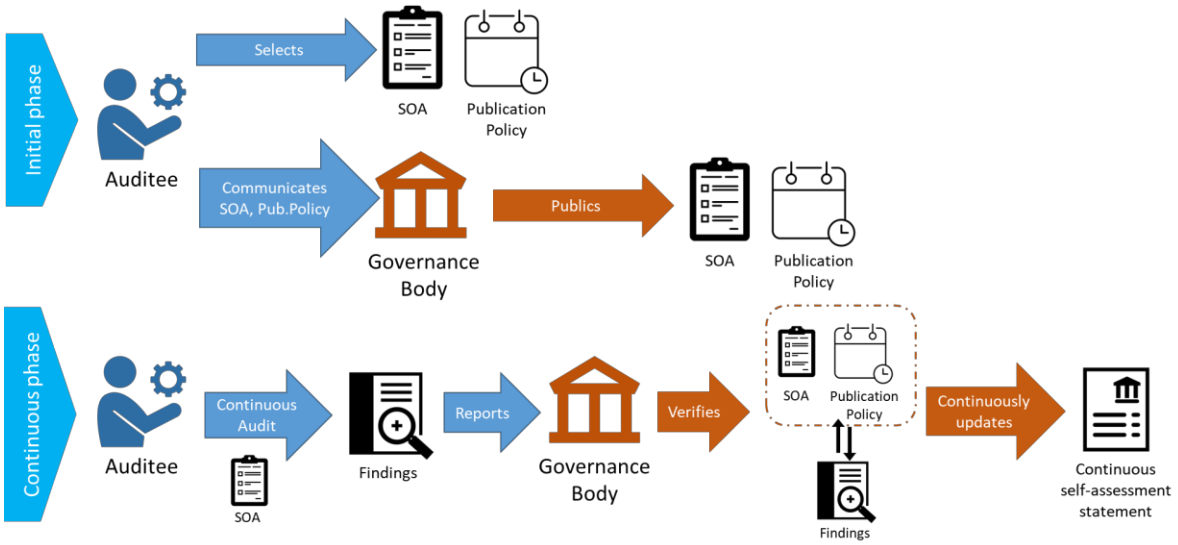

Figure 9: Model 1 – Continuous Self-Assessment

5.2 MODEL 2: EXTENDED CERTIFICATION WITH CONTINUOUS SELF-ASSESSMENT

An "Extended Certification with continuous self-assessment" combines a "point-in-time" certification conducted by an external auditor with the previously defined continuous self-assessment. We qualify this "point-in-time" certification as "extended" because it is based on a traditional third audit party audit with assessment activities that are further broadened to cover the processes, governance and tools used for the self-assessment. As such, while the continuous auditing process used in this second model is still based on a self-assessment, it has a stronger foundation than in the first model.

5.2.1 FOUNDATIONS

In addition to the foundations already defined in 5.1.1, the Governing Body will also establish:

1) Rules for the recognition[1] of external auditors (e.g. accreditation).

[1] The accreditation or recognition process is established by the Governing Body and is beyond the scope of this work.

2) Guidance on the additional assessments performed by the external auditor during the "point in time" certification performed as part of the initialization of the process (see below).

5.2.2 INITIATING THE PROCESS

At the start of the process:

- The Auditee establishes a certification target by selecting a statement of applicability and a reporting policy for a cloud service and communicate it to the Governing Body.
    - The suitable reporting policy is selected form a list of possible reporting policies established by the Governing Bod, based on sectorial or assurance level considerations.
    - Deviations from the selected reporting policy are not permitted.
- The Auditee undergoes a traditional "point-in-time" audit by an external auditor that is recognized by the Governing Body.
- The assessment activities performed in this traditional "point-in-time" audit are however extended to include the verification by the External Auditor that:
    - The processes, governance and tools used as part of the continuous self-assessment are correctly defined and implemented to achieve a correct assessment of the controls in the Statement of Applicability contained in the Certification Target.
    - The Certification Target is fit for purpose. This includes the verification that the appropriate reporting policy has been selected.

  These elements are explicitly described in the final audit report.
- The traditional "point-in-time" audit results in the issuance[2] of a certificate to the Auditee (pending success of the audit). This certification covers the extended assessment activities described in the previous points.
- The Auditee communicates the statement of applicability and the Policy to the Governing Body. If the External Auditor was the entity issuing the certificate, as it is the case in some "point-in-time" certification schemes, the Auditee also transmits the certificate to the Governing Body.
- The Governing Body creates an entry for the target cloud service in a publicly accessible "extended certification with continuous self-assessment registry". This entry contains:
    - A dated copy of the extended "point-in-time" certificate issued to the Auditee.
    - The submitted Certification Policy.
    - A "start date" which defines when these elements were first submitted to the Governing Body.

[2] Depending on the scheme, the certificate is either issued by the External Auditor directly or by the Governing Body, based on the report provided by the External Auditor.

- An "end date" which defines for how long the Certification Target is valid, before a new "point-in-time" certification is needed.
- A certification state, which is initially set as *valid*.

5.2.3 RUNNING THE PROCESS

After the start of the process:

- All steps involved are similar to the ones described for a continuous self-assessment above.
- If the certificate becomes revoked, the Auditee loses its right to be listed in public registry with an "Extended Certification with Continuous Self-assessment". Nevertheless, the Auditee is able to maintain its regular point-in-time certification. The regular point-in-time certification is suspended/revoked as well in case the non-conformity is not fixed according to the procedures established within the point in time certification scheme.

Contrary to a continuous self-assessment, an External Auditor is involved in the process. This involvement remains at a point-in-time. The self-assessment remains under the full control of the Auditee, albeit using processes and tools that have been verified by an External Auditor.

As in the self-assessment model, the role of the Governing Body is to certify that findings are reported in a timely manner and that no valid complains have been issued against the Auditee with regards to the effective implementation of controls/SLOs/SQOs listed in the statement of applicability. However, in addition to this, the Governing Body is also responsible for the relevant point-in-time certification scheme, including the accreditation of the auditors.

Any substantial changes made to the processes and tools used as part of the continuous self-assessment will require a re-certification of the target cloud service (the definition of what constitutes a "substantial change" is left to the Governing Body). Trust in the correct implementation of processes and tool configurations is provided through the extended assessment provided by the external auditor.

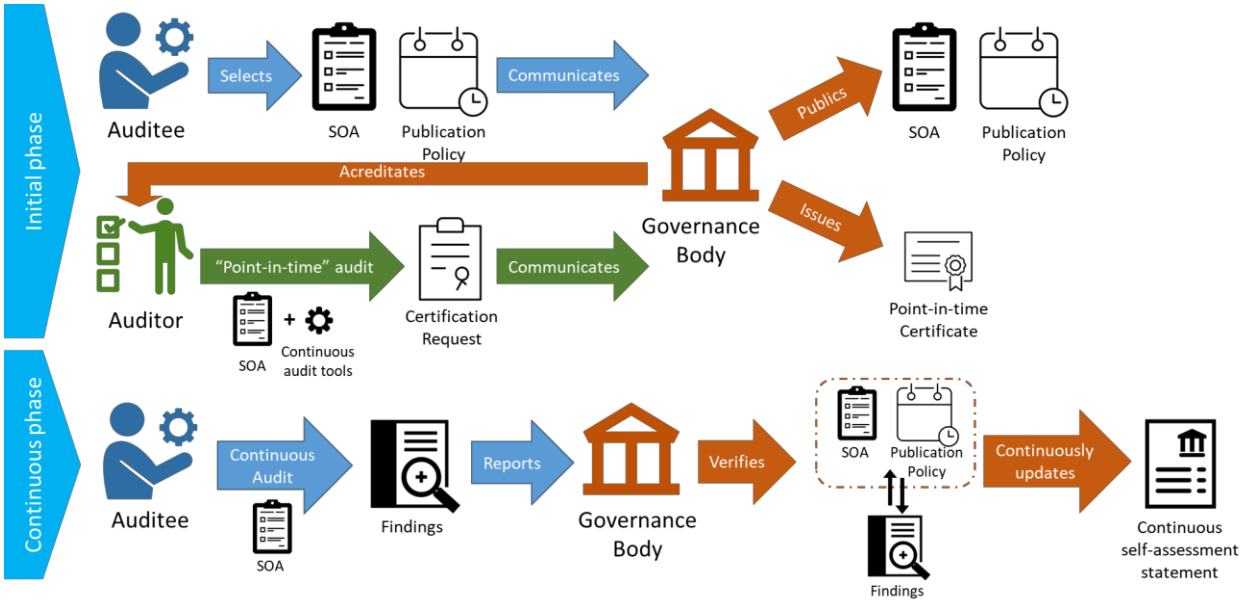

Figure 10: Model 2 – Extended Certification with Continuous Self-Assessment

5.3 MODEL 3: CONTINUOUS CERTIFICATION

A continuous certification consists of a combination of a point-in-time certification and a continuous audit that are both conducted by an accredited External Auditor. The point-in-time certification serves as a "reference" starting point and is followed by continuous audits, the findings of which are reported at a predefined frequency to the Governing Body.

The process is the same as with the Extended Certification with Continuous Self-assessment, except that all continuous auditing tasks that were performed by the Auditee are now performed by an External Auditor.

5.3.1 FOUNDATION

In addition to the foundations already defined in 5.1.1 and 5.2.1, the Governing Body will also:

- Publish recommendations on data formats and data exchanges for the purpose of enabling the external auditor to obtain measurement results from the auditee's information system, during the continuous auditing phase (see below).

5.3.2 INITIATING THE PROCESS

At the start of the process:

- The Auditee selects a statement of applicability and a Policy, with a view of conducting a continuous self-assessment.
    - The submission frequency defined for each control/SLO/SQO in the publication policy follows a standard established by the Governing Body.
    - Deviations from this standard are permitted but must be justified explicitly.
- The External Auditor and the Auditee together establish a set of processes and tools that will enable the auditor to perform a continuous assessment of the controls/SQOs/SLOs in the statement of applicability.
    - The selected continuous auditing tools and processes produce measurement results that will be transmitted to the external auditor, evidence is expected to be stored by the auditee for use in case of a complaints or any other relevant issue.
    - The selected continuous auditing tools and processes must produce measurement results in machine-readable formats facilitating interoperability between the Auditee and the External Auditor, following guidelines published by the Governing Body.
- The Auditee undergoes a traditional "point-in-time" audit by an external auditor, which is accredited by an Governing Body.
- The assessment activities performed in this traditional "point-in-time" audit are however extended to include the verification by the External Auditor that:
    - The processes and tools used as part of the continuous self-assessment are correctly defined and implemented to achieve a correct assessment of the selected statement of applicability.
    - The statement of applicability and the publication policy are fit for purpose. This includes the verification that any deviation from standard submission frequencies defined in the publication policy is justified.

  These elements are explicitly described in the final audit report.
- The traditional "point-in-time" audit results in the issuance[3] of a certificate to the Auditee (pending success of the audit). This certification covers the extended assessment described in the previous points.
- The Auditee communicates the statement of applicability and the Policy to the Governing Body. If the External Auditor was the entity issuing the certificate, as it is the case in some "point-in-time" certification schemes, the Auditee also transmits the certificate to the Governing Body.
- The Governing Body creates an entry for the target cloud service in a publicly accessible "continuous certification registry". This entry contains:
    - A dated copy of the extended "point-in-time" certificate issued to the auditee.
    - The submitted Certification Target, including any justifications for deviations from standard submission frequencies in the reporting policy,

[3] Depending on the scheme, the certificate is either issued by the External Auditor directly or by the Governing Body, based on the report provided by the External Auditor.

- A "start date" which defines when these elements were first submitted to the Governing Body.
- An "end date" which defines for how long the statement of applicability and the submitted publication policy are valid, before a new "point-in-time" certification is needed.
- A certification state, which is initially set as *valid*.

If the certificate becomes revoked, the Auditee loses its right to be listed in public registry with an "Extended Certification with Continuous Self-assessment". Nevertheless, the Auditee is able to maintain its regular point-in-time certification. The regular point-in-time certification is suspended/revoked as well in case the non-conformity is not fixed according to the procedures established within the point in time certification scheme.

5.3.3 RUNNING THE PROCESS

After the start of the process:

- The External Auditor performs a continuous audit of the Auditee's cloud service, according to the Certification Target:
  - The external auditor uses the relevant tools and processes that were agreed with the auditee during the initiation of the process.
  - The external auditor performs verifications on the integrity of the continuous auditing tools and processes (e.g. version verification, checksums, etc.)
  - The external auditor processes the collected measurement results and produces findings based on the Statement of Applicability defined in the Certification Target.
- The External Auditor reports the findings of the audit to the Auditee and the Governing Body, according to the reporting policy defined in the Certification Target.
- Based on the timely submission of findings by the External Auditor, as well as the review of any eventual complaint received from a stakeholder, the Governing Body establishes the state of the certificate issued to the Auditee as *valid*, *suspended* or *revoked*.
- The Governing Body continuously updates the corresponding public registry entry of the target cloud service with the state of the issued certificate.
- If the certificate becomes revoked, the public registry entry is removed, and the Auditee is required to begin the process from the start again.

The External Auditor is involved continuously in the auditing process.

The Governing Body has a similar role as in Extended Certification with Continuous Self-assessment. In addition, the Governing Body is also responsible for defining interoperability guidelines that will enable seamless continuous auditing by the external auditor.

This model provides the strongest level of assurance but is also the most complicated to implement.

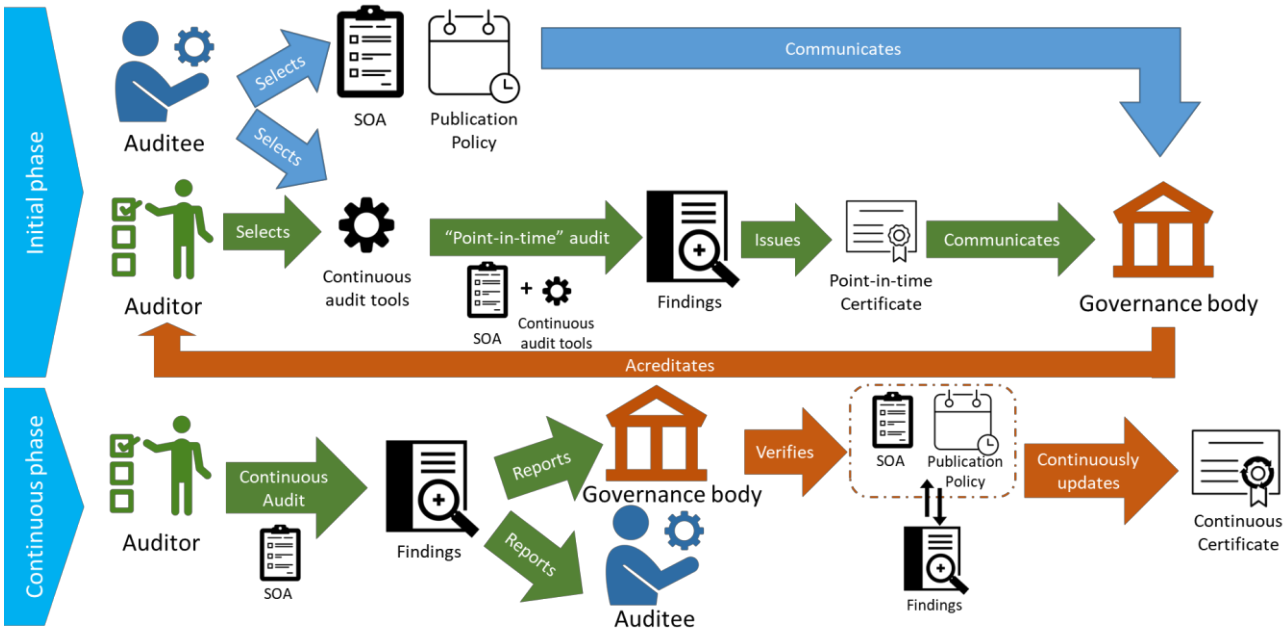

Figure 11: Model 3 – Continuous Certification

6 GOVERNANCE STRUCTURE FOR CONTINUOUS AUDITING

In this section, important elements of the governance structure are described. The Continuous Auditing concept requires a strong governance. This governance needs to guide the entire continuous auditing process from conceptual design through set up, implementation and parameterisation to operation and maintenance as well as further development. The governance needs to control all processes in which the actual auditing activities are performed in order to ensure a reliable audit outcome and with this, the assurance. Amongst others, these activities include assessing the control's design, the suitability of the evidence available or the measures applied to assess the evidence provided. Furthermore, the governance structures need to provide sound guidance on the introduction of the continuous auditing process.

In this case the entities are treated like a potential real asset, while describing the basic conditions, processes and potential evaluation of technical dependencies.

6.1 RESPONSIBILITIES IN GOVERNING CONTINUOUS AUDITING

The guidance and assessment of governance is executed through accountable bodies. These accountable bodies are the key players to provide quality and clarification into the governance and are also used as governing bodies for specific segments. They advise and execute the development of the continuous audit certification scheme as well.

Accountable/Governing Bodies are set to identify gaps, suggest improvements and initiate processes. Three key players are identified, consisting of the EU-SEC governance Body, the authority and the auditor. These three are completed by adding accountable bodies, which provide specific information to the continuous audit system.

Four accountable bodies are defined:

- Governance Body

The EU-SEC governance Body is a trusted party that qualifies external auditors to perform audits and established rules for recognition of external auditors. It is responsible for the correct organization of a certification scheme and maintains a repository of standards, best practices and control frameworks that provide reference to the specific requirements/controls in each standard. Furthermore they map, monitor and identify gaps in the evidence chain between the requirements of different certification schemes and maintain a registry of certifications or attestations of cloud services.

Moreover the governance Body provides guidelines on the establishment of a suitable scope of self-assessment, specifies a suited control framework for the creation of the Certification Target, defines acceptable Reporting Policies and monitors the transition of certificates through various states. Within continuous auditing, the governance Body publishes recommendations on data formats and data exchanges to enable measurability through external auditors and is also responsible for definition of interoperability guidelines.

Role	Responsibilities

Governing Body	• Publishes guidelines • Creates an entry for the target cloud service in a publicly accessible "continuous self-assessment registry" • Updates the corresponding public registry entry of the target cloud service with the state of the issued certificate • Certifies that findings are reported in a timely manner and that no valid complains have been issued against the Auditee

- Authorities/Scheme Owners

Authorities/Scheme owners are responsible to inform about current changes to the continuous auditing framework and implement regulation and rules to the framework.

Role	Responsibilities
Authority	• Executes the governance over the EU-SEC Security Requirements Repository • Reviews the continuous auditing concept and decides whether it complies with the statutes • Approves the concept before auditee and auditor begin to realise and build the concept • Oversees the auditing process and performs spot checks to examine compliance with statutes, repeatedly • Consolidates results from reviews and spot checks to identify room for improvement and derive action plans to realise improvement

- External/Authorized Auditor

The external auditor is a trusted party or organization, recognized and qualified by the governance Body, to perform audits. Its main functionality is performing an audit with a view of delivering a certification or attestation. In an ISO-style certification scheme, "external auditors" would be part of an "accredited certification body", also called "accredited registrar". The fact that the auditing itself is executed automatically, does not exclude auditors as they, at minimum, need to implement and maintain the auditing system. In the following, the roles are described in more detail.

Role	Responsibilities
Auditee	• Operates the system, the processes and controls to be audited

	• Initiates the continuous auditing process • Finances the continuous auditing process • Works with the results of the continuous auditing process • Leads the development of the continuous auditing concept • Provides information regarding room for improvement to the authority
Auditor	• Supports the development of the continuous auditing concept • Ensures that the audit is conducted by an independent third party • Ensures that the audit is conducted in compliance with applicable audit standards (e.g. ISAE 3000) • Ensures that the audit targets the correct systems components • Ensures that the audit techniques / test procedures are executed appropriately • Compiles and issues the audit report based on the continuous audit information • Provides information regarding room for improvement to the authority

- CSP

The cloud service provider provides data and auditing results to continuous audit.

Role	Responsibilities
CSP	• Providing data to be leveraged between continuous and cloud audit

Each of those accountable bodies are responsible to carry the governing structure. They are deployed to supervise, survey, monitor and report results and in addition agree to collaborate and support the governing bodies. In case of the implementation of new schemes/certifications those may be conducted to create a specific task force, which analyses and reacts according to the impact of processed changes.

Due to the self-assessment and self-certification character of continuous audit, the audited system may be considered as a further element for the accountable body, but not as an accountable body itself.

6.2 GOVERNANCE PROCESSES

The governance process defines the relationship between the governing bodies and a set of activities with which they are required to comply, in order to maintain a consistent management process.

6.2.1 Key Principles for the Governance Processes

In order to provide reliable information, governing bodies need to be accredited. Continuous Auditing relies heavily on trustworthy and current information of accountable bodies. In general, the continuous auditing certification scheme aims at increasing the level of transparency and accountability from the auditing point of view.

For governing continuous audit processes, four main goals are defined:

- Accountability

As targeted in more detail in 6.1, responsibilities are carried out by different governing bodies. Accountable/Governing Bodies are set to identify gaps, suggest improvements and initiate processes. They are also advising and executing the development of the continuous audit certification scheme.

- Transparency

Assuring transparency and integrity throughout the governance of events and triggers is a crucial goal, in order to provide high level assurance.

- Trustworthiness

Trustworthiness is key to the governing process of continuous auditing: If the process is not trusted, the resulting outcome will have lower value. Trustworthiness is achieved by a combination of mechanisms, notably the use of independent governing bodies, which are formally accredited.

- Currentness

Information and process outcomes have to be addressed in current situations and are not reliable, or trustworthy if not up to date. Currentness is achieved by continuous certification.

6.2.2 PROCESS SCHEME

Governing processes are defined by a specific event triggered input leading to a case sensitive outcome. In order to provide a sound governance during the continuous audit, a process scheme is implemented. This scheme is used to maintain and provide governance effectiveness and elaborated in more detail below.

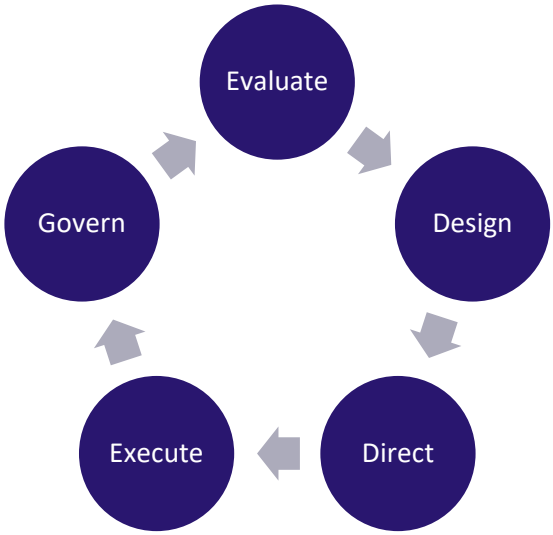

Figure 12 Process scheme

- Evaluate

Actions and conclusions need to be tracked, including a comprehensive range of activities and processes. Furthermore demands for assurance need to be satisfied, such as relevant and reliable information for decision making. This happens while using a holistic approach to governing each segment of the targeted auditee.

- Design

Design describes the manner of combining governing methods with technical procedures to act after predefined guidance.

- Direct

Direct is the phase to coordinate and address specific change, implementation and solution requests. Due to its analysing character this phase is used to bridge automated and non-automated systems, targeted in 2.2, even so deploying the manner to close gaps in the evidence chain, as addressed in 2.4 and furthermore providing guidance to real time assurance.

- Execute

After the directing phase, the defined continuous auditing governance shall be implemented and requests should be solved. This leads to the construction of governance measures, fulfilled by the different governing bodies.

- Govern

An essential element of continuous improvement is the permanent monitoring and updating of procedures. The continuous audit landscape regularly analysed (with respect to new standards and requirements) and relevant changes incorporated. Whenever crucial changes are implemented, event handling measures are triggered.

6.2.3 GOVERNANCE APPROACH

The objective of the governance approach for Continuous Auditing is the guidance through the entire continuous auditing process, from conceptual design through set up, implementation and parameterization to operation and maintenance as well as further development. The Governance Approach is shown in the following diagram and elaborated in more detail below.

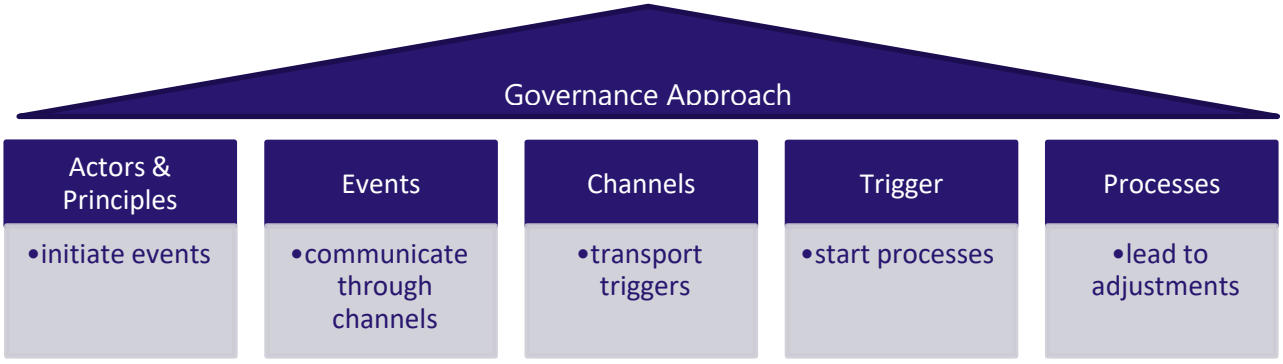

Figure 13 Governance approach

6.2.3.1 ACTORS & PRINCIPLES

Accountable/Governing bodies are set to initiate processes, identify gaps in the preparation and execution and suggest improvements. Additionally the accountable bodies, which provide specific information to the continuous audit system are relevant for the governance approach. Four accountable bodies are defined and targeted in detail in 6.1:

- Governance Body
- External/Authorized Auditor
- Authorities/Scheme Owners

- CSP

These key actors need to follow a set of applied principles. Activating the provided input of information, ethical and segregation of duties principles are applied, in order to verify the auditor and auditee's expertise, as well as for preventing the self-assessment and abuse of power by governing bodies.

- Ethical principles

Actual or apparent conflicts of interest are voided or solved by seeking guidance from appropriate authorities. The spirit of laws and regulations affecting the continuous audit are followed and reflected by the governing bodies.

- 4-eye-principle

Each measure, safeguard or communicated result has to be reviewed by another governance Body, than the one about to release the result.

- Mitigation

The Governing bodies are responsible for implementing an internal control system to mitigate risks of conflicting approvals or wrongly monitored processes. Compliance

- Compliance

Governing bodies are responsible to control and assess compliance obligations. Every governance Body declares to comply with applicable laws and regulations, also in terms of technical and organizational security measures, being able to demonstrate accountability.

6.2.3.2 EVENTS

Following the governance approach the defined key actors are responsible for initiating events in order to coordinate the Continuous Auditing procedures and react on deviations. Every role can initiate the following events:

- On-board new

This event focusses on the implementation of new schemes/auditors/process owners etc. For example: An auditor may leave the third party and may not be able to resume his/her work on governing/auditing multiparty recognition. This leads to an event, which has to be handled in a manner to succeed. In this case, a new auditor has to be on boarded. The same applies for every other instance.

- Update existing

Change and demand processes lead to adjustments on schemes/processes. An objective needs to be targeted by a proposition. In this case a change is requested and needs to be solved. This happens via Channels.

- Delist existing

Another event initiated by an actor is to delist existing schemes/auditors/process owners. To enable the correct and secure remove of existing actors, a termination process has to be initiated.

In order to successfully maintain the multiparty recognition framework, these events are used to react in a proper manner. All defined events are communicated through channels.

6.2.3.3 CHANNELS

Different channels are used to inform about specific events and transport triggers. This measure secures the attention and motivates the gov. body/scheme/process owner to react on incidents. Channels are described as tools to transfer information.

In this case, channels can be but are not limited to:

- Website
- Phone
- E-Mail
- Conference
- Personal contact
- Newsletter subscription
- Etc.

6.2.3.4 TRIGGER

Triggers are used to start the processes and are usually addressing certain issues. They may be indicated by actors or scheme owners and can be changes into a certification scheme or the decision to implement continuous auditing caused by competition, in case the competitors want to implement continuous auditing to ensure or achieve competitiveness. Triggers are transported via the communication channels used, such as:

- Request by actor

- Publication
- Research finding
- Newsletter subscription
- Competition

6.2.3.5 PROCESSES

It is the responsibility of the governance Body of the EU-SEC to provide guidance for the introduction of Continuous Auditing processes. This includes the specification of the conceptual design and its setup. Recommendations for the preparation and execution phase ensure the alignment of Continuous Auditing with regard to reliability and assurance. In the following, procedures for the improvement of the Continuous Auditing execution are formulated to give comprehensive advices. The process scheme follows a five-step approach, which is shown in the following diagram and elaborated in more detail below.

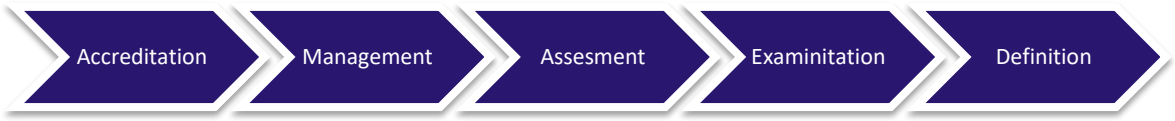

Figure 14 Processes

- Accreditation process of auditors

The governance Body of the EU-SEC oversees the accreditation process of auditors for Continuous Auditing. The selection procedure shall be conducted transparently and carefully to avoid conflicts of interest and illegitimacy. This process is conducted for all auditors that are new to Continuous Auditing, while existing auditors are assessed on a regular basis.

- Management of standards and policies

The management of changes includes the identification of new or changes of standards, regulations and policies that might have an impact on the Continuous Auditing process. Their impact and value is assessed comprehensively before a potential Request for Change (RfC) is initiated. A maintenance team is determined and requests are assigned clearly. After changes are applied, they are reviewed with regard to correct implementation. The corresponding documentation is updated accordingly and released afterwards.

- Assess design of controls

To ensure a reliable control design that is up-to-date, the design of controls is assessed regularly to identify potential need for action. The suitability of the design is investigated with regard to relevant standards, regulations and policies. The determination of the effectiveness of the control design allows the evaluation of its appropriateness.

- Evidence examination

Evidence used in the Continuous Auditing process shall be examined regularly with regard to suitability. In addition, measures to assess the evidence shall be applied and monitored.

- Measurement results

The governance Body of the EU-SEC sets guidelines and rules for the interoperability of measurement results. The impact and value is assessed comprehensively before a potential interoperation of results between auditee and auditor is initiated. A maintenance team is determined and reviews are assigned clearly. In a further step the governance Body establishes the state of the certification issue and updates the corresponding public entry, based on the measurement results.

- Define verification and publication guidelines

Guidelines that explain the verification of new and updated content with regard to the Continuous Auditing process shall be specified by the governance Body of the EU-SEC. Thereby, the next step of publishing the content is only initiated after review and verification.

6.3 REQUIREMENTS AND PREREQUISITES FOR TECHNICAL REALISATION

The level of acceptance of the continuous auditing certification is largely dependent on qualification of the auditor and the overall quality of the audited items. In order to accommodate this matter of fact, it is important to address the requirements and prerequisites for technical realisation and in addition cover the challenging task to govern the change management process. Therefore, we define certain requirements directed to the scheme auditor and the continuous audit system, which ensure a continuous and targeted involvement of the before mentioned parties.

6.3.1 EXPERTISE OF THE AUDITOR

Auditors involved into engagements concerning continuous auditing require advanced knowledge and deep insights into IT processes, Cloud technology and rules of auditing. Hence the roles are described in detail in 3.1., this section focuses on the Area of responsibilities and governing activities. The areas including illustrative examples are outlined below (non-exhaustive list).

Area	Responsibilities
IT processes	• Asset management • Business continuity management • Communication security • Compliance and data protection • Control and monitoring of subservice organisations • Cryptography and key management • Identity and access management • Mobile device management • Organisation of information security • Personnel / HR / workforce • Physical security / data centre • Portability and interoperability • Change management, development and maintenance • Safeguards for regular operations • Security incident management • Security policies and work instructions • DevOps • …
Cloud technology	• On-demand self-service • Broad network access • Resource pooling • Rapid elasticity / global spread / load balancing • Measured service • Service Models (IaaS, PaaS and SaaS etc.) • Deployment Models (Public, Private etc.) • Virtualisation • Containerization • Subservice organisations

	• …
Rules of auditing	• Ethical Requirements • Quality Management • Professional Scepticism • Professional Judgment • Planning and scoping • Assessment of subsequent events and other information • Applicable criteria and requirements to audit against • Assurance conclusion / opinion • Assurance / audit report • Communication

The following table describes the responsibilities along the process of setting up and operating a continuous auditing-system.

Phase	Governance Activity	Auditee	Auditor	Authority
Ideation	Governance process to provide: ⇨ Checklists for guiding the process ⇨ Templates for structuring the documentation	Responsible	Support	n/a
Conceptual design	Provide guidance for designing: ⇨ Systems in scope of continuous auditing ⇨ System components in scope of continuous auditing ⇨ Distinction of controls which are to be audited manually and automated ⇨ Individual objectives ⇨ Parameterization of SLO/SQO ⇨ Nature of evidence to be considered during continuous auditing ⇨ APIs for connecting system components relevant to continuous auditing ⇨ Identification and assessment of risks	Support	Responsible	n/a
Set up	Develop instructions to: ⇨ Define systems in scope of continuous auditing ⇨ Define system components in scope of continuous auditing ⇨ Identify controls which are to be audited manually and automatically	Support	Responsible	n/a

	⇨ Initiate parameterisation of SLO/SQO ⇨ Assess nature of evidence to be considered during continuous auditing ⇨ Identify APIs for connecting system components relevant to continuous auditing			
Implementation	Provide instructions on: ⇨ Implementation procedures for systems in scope of continuous auditing ⇨ Specified implementation procedures for system components in scope of continuous auditing ⇨ Providance of a list of controls which are to be audited manually and automated ⇨ Complete parameterisation of SLO/SQO ⇨ Determine nature of evidence to be considered during continuous auditing ⇨ Stipulate APIs for connecting system components relevant to continuous auditing	Support	Responsible	n/a
Parameterisation	Provide instructions on how to configure the continuous audit system	Support	Responsible	n/a
Go-live approval	⇨ Require approval for Go-live ⇨ Provide documentation templates for Go live			n/a
Operation	Describe processes for the operation of the continuous auditing system concerning: ⇨ Monitoring of the continuous monitoring process	Responsible	Support	Support

	⇨ Quality Management: Validating the outcomes of the continuous monitoring process (does the system come to the same audit results as a human auditor would have come)			
Maintenance and further development	Describe processes for the operation of the continuous auditing concerning: ⇨ Authorisation for changing the parameterisation and configuration ⇨ Change Control processes (including requirements for approval and documentation)	Responsible	Support	Support

6.3.2 REQUIREMENTS FOR THE CONTINUOUS AUDITING TOOL CHAIN

While governing the continuous auditing system, a comprehensible insight into the technical aspects is necessary. A continuous auditing system is executing audit procedures and with these, producing audit results. These results must be eligible to be included into audits, respectively audit reports, directly without being re-assessed by human auditors. Furthermore evidence must be collected and assessed with a frequency that will be expressed in minutes, hours, days or months. Keeping this in mind, it needs to be considered, that continuous audit is suited to lower level "service attributes", which can more easily be automatically evaluated.

To strive for a more complex result, continuous audit needs to apply to a set of controls, without being at expense of automation. This can be achieved through specific elements and a holistic approach. The continuous auditing system needs to be adjusted to ensure the needed auditing results. Several safeguards and measures should lead to the desired accuracy, while auditing continuously. Controls may be broken down into a set of attributes, which can be automatically evaluated and automatically audited.

While "Continuous Auditing" is still not framed in a widely recognized standard, the approach to define the requirements for the Continuous Auditing Tool Chain are derived from related domains, such as "Cloud Computing – Service Level Agreement (SLA) Framework" [ISO 19086-1]", "[BSI C5]" and "[ISO 27001]".

Audit results must be profound and trustworthy. In order to support the approach to comply with automation and deliver suitable results, requirements for the continuous auditing tool chain are defined.

Requirement	Elements	Rationale
Holistic	• Auditee's controls incl. supporting information • Compliance scheme's requirements • Audited system's characteristics	The continuous auditing system must take into account all elements which are relevant for control testing.
End-to-end process coverage	• Process triggers • Start and end • Process steps / activities • Input & Output integrity routines	The continuous auditing system must understand and capture the process entirely in

	• Accountabilities / responsibilities • Action on errors	order to be able to produce a sound audit result.
Security	• Protection from manipulation • Not suitable as attack vector • Vulnerability scanning Regular patching / updates • Monitoring of access, logging ports and addressing gaps • Integrity tests	The continuous auditing system must be protected against vulnerabilities and attacks.
Non-invasiveness	• Regular operation / production is not impaired by audit operation • Elasticity to address audit information, creation of VM instances on demand	The continuous auditing system must be designed and operated in a way which ensures that the production system runs smoothly.
Awareness	• Quality tests • Logging automated reports • Early detection and monitoring • Implemented audit trail	The continuous auditing system must derive impact and urgency of all associated configuration items
Scalability	• Deploy rules for modification • Detect data aggregation	The continuous auditing system must refer to the operating system, avoiding likelihood of delayed response or unused resources

6.3.3 PREREQUISITES FOR LEVERAGING RESULTS FROM CONTINUOUS AUDITING INTO CLOUD AUDITS

In addition to the requirements applicable for the continuous audit system itself prerequisites for the leveraging of audit results in Cloud audits are set. These are used to maintain audit quality and differentiate between suitable and not suitable results, as described in 6.3.2. From governance perspective the events, namely on-board, update, delist, rely heavily on the consistency of a continuous and cloud audit. Whereas audit activities are defined at the initial phase of the audit, these prerequisites may be used as base principles to enable the leveraging of results.

- **The repeatability principle**: If two different entities each conduct an independent audit of the same security/privacy attribute of an information system, under the same scope and conditions, then the results should be the same.

- **The equivalence principle:** If a security/privacy attribute is assessed in two independent information systems and if the measurement results are the same then the provided security level should be equivalent in both information systems for that particular security attribute.

- **The relevancy principle:** The security/privacy attributes and associated metrics that are used when assessing an information system should be selected so as to provide actionable information for provider of the certified system and its customers.

- **Trustworthiness principle**: The process of collecting, verifying and evaluating evidence against audit criteria should be considered as capable of providing a trustworthy representation of the security/privacy level of an information system.

Relying on the value of those base principles, it needs to be defined which of those need further implementation. While repeatability is not too difficult to apply and often used to describe the value of automated results, trustworthiness is the key for the further usage of results into the cloud audit procedure. The equivalence and relevancy principle need to be handled in a different manner, addressing a more complex approach and needing specific and defined prerequisites. .

Regarding automated continuous auditing, three additional concepts are set and need to be reflected while defining prerequisites. These are: Measurement, Measurement Result and Metric (from ISO/IEC 19086, borrowed from [NIST 500-307]).

Those aspects are reflected in the definition of prerequisites for leveraging results:

Prerequisite	Description
Repeatable	• The audit result will be achieved again, if the audit procedure is repeated under the same conditions
Comparable	• A human auditor would have come to the same conclusion in the control testing, applying professional judgment and professional scepticism.

Transparent	• Audit results are available upon request without further limitations to access details of technical measures, integrity of data flow is verified.
Trustworthy	• The process of auditing (incl. the decision for a certain audit approach and test procedure as well as the documentation of the test procedure and the result) must be non-changeable and protected against manipulation.
Validated	• The audit result must be validated by a second 'validation procedure' in order to increase trustworthiness and eliminate failures and deviances.
Mature	• Infrastructure of self-audit is formal, documented and evaluated, providing continuous assessment, especially gap and root cause analyses
Consistent	• Audit results are followed by frequent evaluation of control issues to achieve consistent and reliable performance data.
Measurable	• Reliability of audit results is granted through implementation of a predefined KPI, which is designed to maintain efficient data processing (e.g. amount x of data inspected in y seconds, if successful, no report, otherwise report issue)

6.3.4 CHANGES TO THE IMPLEMENTATION OF CONTINUOUS AUDITING

As in every IT system, changes to productive systems are a risk. This risk may materialize when for example undiscovered dependencies lead to unexpected and undesired behaviour, changes to code or configuration items do not trigger the desired or during the change the required order of action is not adhered to. The described risks logically also apply not only to the Cloud system but also to the continuous auditing system itself. Therefore, all changes to the continuous auditing system need to be managed by a change control procedure which must at minimum cover the following steps and activities:

- Change request

Identified news and changes shall be assessed on its impact and value for the current governing procedure.

- Risk assessment

The risk of changes gets assessed with an accepted risk assessment methodology. Based on this measure mitigating actions get developed.

- Test

Change request gets tested against success criteria.

- Approval

In this phase the tested change request gets decided upon implementation or rejection.

- Post implementation review

Updated elements are reviewed after the requested change has been implemented. During this review, the approver and the maintenance team are responsible for reviewing the applied changes based on the comparison between the previous version and the updated version.

Step	Activities	Auditee	Auditor	Authority
Change Request	• Document change request in a tool • Describe the change along defined structure and elements (e.g. desired new behaviour, change configuration items, dependencies etc.) • Define success criteria to perform testing against	Responsible	Support	n/a
Risk Assessment and Rollback Plan	• Assess risk of change with an accepted risk assessment methodology • Develop mitigating action for identified risks • Validate feasibility of risk mitigating actions • Document risk assessment and rollback plan in tool	Responsible	Support	n/a

Test	• Test the developed change against the defined success criteria • Document testing in tool • Suggest approval for change request or submit negative testing result incl. error log to developer	Support	Responsible	n/a
Approval	• Challenge request for change • Review and assess documentation (esp. change description, risk assessment, rollback plan, test approach and test result) • Decide to approve or reject • Document decision in tool • Verify transaction	Support	Responsible	n/a
Post Implementation Review	• Validate implemented change against success criteria • Perform broader review of functionalities which are connected with or depend on changed configuration items	Support	Responsible	Support

Changes to the continuous auditing system are possible at all times as far as the continuity of the audit process and quality of the results (see 6.3 and 6.4) are ensured.

6.3.5 REPORTING POLICY MANAGEMENT

The Reporting Policy Management is required in order to ensure that findings for each control (or SLO/SQO) are updated in the frequency required for the implemented Continuous Auditing Model and the specified Certification Target. Additionally the frequency of the communication of findings to the Governance Body is part of the Reporting Policy Management. All the three Continuous Auditing Certification Models mentioned in chapter 5 require different Reporting Policy Management. The Governance Body is responsible that the auditee manages the Reporting Policies. The Reporting Policy Management shall consider:

Model	Aspects
1. Continuous Self-assessment	- Changes in the findings updates and reporting frequency are easier to implement as the changes are not bound to a certification - Findings updates and reporting frequency require preparation for the auditee's evidence
2. Extended Certification with Continuous Self-assessment	- Changes in the findings updates and reporting frequency have to be aligned with the certification goal and be initiated early enough before the "point-in-time" certification - Findings updates and reporting frequency require preparation for the auditee's evidence - Alignment with external auditors is required
3. Continuous certification	- Changes in the findings updates and reporting frequency have to be aligned with the certification goal and be initiated early enough to be valid for the next certification - Findings updates and reporting frequency require preparation for the auditee's evidence - Alignment with external auditors is required

All the Reporting Policies shall be part of regular revision and adaption to organizational, legal and environmental changes.

7 CONCLUSIONS

This deliverable provides the scheme and the governance structure for continuous auditing. It introduces an important concept within the EU-SEC framework that allow cloud service providers to constantly assess and publish the compliance status with a given standard.

The development of the scheme is based on a common methodology for improving existing schemas by introducing aspects such as, the frequency of verifying a control and overcoming existing limitations, or the lag of up-to-date-ness. The latter refers to one of the major limitations of existing certification schemes, the point in time assessment, which makes the certification losing its up-to-date-ness right after the audit.

The continuous auditing certification scheme provides the necessary guidance to implement the required enabling processes for a continuous auditing. This is based on a method that lays out the breakdown of a control set to measurable attributes, and the model describing the relationships between control, objective, attribute and measurement. Once the processes are implemented the execution of the auditing is continuously repeated. The execution includes the collection of evidence, its measurement, and the evaluation and finally the certification results. The level of assurance such a certification provides depend on the type of assessment and the scope that is agreed upon for the continuous audit. The framework provides three different models, each one offering a unique way for an external auditor's involvement.

Continuous auditing certification introduces efficiency improvements by automating a subset of controls. However, the actual subset of automatable controls is relatively small compared to all necessary controls that have to be verified. The major reason for this is that some aspects of controls are very high-level concepts and do require a profound judgment about the proper interpretation in a specific context. Some examples are described in the following:

- The existence of security providing processes, methods and policies. One example for this is the existence and documentation of a business continuity plan.
- A proper documentation. Decision on what's suitable documentation for a specific origination.
- Need for a proper design. Reasoning on if a suitable design for items like architecture, implementation or processes has been applied.

As of today, these require human intervention. With future developments in automation progress, more complex controls can be verified automatically. Such developments will improve the efficiency of continuous auditing certification even more.

REFERENCES

[1] Cloud Security Alliance; Ministry of Finance Slovak Republic, "EU-SEC Deliverable D1.4 Principles, criteria and requirements for a multiparty recognition and continuous monitoring based certifications," 01 01 2018. [Online]. Available: http://www.sec-cert.eu/downloads/.

[2] C. S. Alliance, "STAR Certification," Cloud Security Alliance, [Online]. Available: https://cloudsecurityalliance.org/star/certification/#_overview.

[3] N. I. o. S. a. Technology, "NIST Cloud Computing Service Metrics Description 500-307," 2015. [Online]. Available: https://www.nist.gov/sites/default/files/documents/itl/cloud/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf.

[4] E. T. S. Institute, "Information Security Indicators," 2016. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/information-security-indicators.

[5] E.-C. Consortium, "ESCUDO-CLOUD," [Online]. Available: http://www.escudocloud.eu/.

[6] I. J. 1. 38, "ISO/IEC DIS 19086-2 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric model," 2017. [Online]. Available: https://www.iso.org/standard/67546.html.

[7] N. Mikko Larikka, "EU-SEC D1.3 – Auditing and Assessment Requirements V 1.0," 2016. [Online]. Available: http://www.sec-cert.eu/wp-content/uploads/2017/12/D1.3-Auditing-and-assessment-requirements-V1.0.pdf.