EUSEC
EU SECURITY CERTIFICATION

GUIDELINE

Implementing Continuous Audit-Based Certification

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

What is continuous audit-based certification and how important it will be?

Imagine the following use case. Bob is the CTO of a major bank. Among other things, he is responsible for ensuring that all client data is handled securely and in accordance with regulations. **Many industries have already moved to the cloud** since it introduces advantages over an in-house-solution, like on demand scalability or increased security. But **regulators**, especially in the banking sector, rightly **demand a high level of security and data protection**. In his own datacenters, where checks are implemented to reduce the risk of cybercrime and other threats, Bob is capable of proving his compliance with security regulations. If necessary, even via a **third-party audit**.

Cloud Service Providers (CSPs) usually have certifications that show they comply with industry security standards but they **rarely** provide information **on a frequent enough basis** to help Bob **demonstrate compliance with the strict regulatory environment of the finance industry**. Since the certifications are usually performed on an annual basis CSPs **do not provide day-to-day information on their security and privacy compliance**. Being able to prove the level of security to the regulator is very crucial for Bob.

After some research, Bob finds Alice's company. They have a **new type of certification**, which proves that the CSP is compliant on an **ongoing basis**. This compliance status is **based on data which is audited almost in real time**. This fits perfectly with Bob's expectations of a cloud service.

1 Continuous audit-based certification: process overview

How can we deal with those difficulties of assuring and certifying continuous assessment of our cloud services? The EU-SEC project has developed a process that will throw some light on this question, the ***continuous auditing-based certification (CABC)****.*

You may say: *Another certification?*

Well, yes and no, it will complement point-in-time audits and will deal with the limited frequency and proactivity of traditional "point-in-time" certifications. Using technology to monitor and flag non-compliant activity on an ongoing basis, continuous auditing delivers an enhancement to traditional certification. It increases the assessment frequency via an automated continuous workflow.

EU-SEC's continuous auditing changes the nature of auditing from a traditional, process-driven, point-in-time certification towards a **data-driven real-time certification**.

Cloud customers with sensitive data, such as financial institutions or companies in the health sector, really need a certification based on more frequent assessment of controls. Currently, they cannot obtain an up-to-date verification that their

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

data is subject to good practice by CSPs. By applying continuous certification, the level of trust, transparency and assurance is greatly improved. EU-SEC continuous auditing-based certification fills the gaps.

Let's see how we do it…

1.1 From monitoring data to certification.

Nowadays, it is critical to have monitoring systems that allows your entity to work in a data-driven basis, as well as controlling the security of your systems in real time.

So, what else is needed? Are you saying it is not enough?

To be able to assess security properties of a system, you would need to have a standard to assess controls in a standardised way. It will make it possible to compare and validate the security characteristics of your information systems.

The EU-SEC project's certification scheme is based on this foundation of standardised comparison and validation. Knowing that cloud services, based on their scope, have different requirements in terms of transparency and assurance, EU-SEC proposes three models for certification, each of which provides different levels of transparency and assurance and requires varying levels of implementation complexity, as shown in Figure 1.

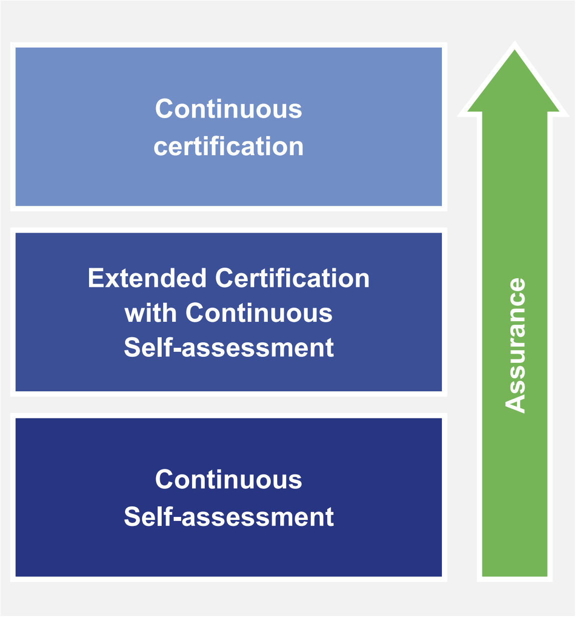
Continuous certification
Extended Certification with Continuous Self-assessment
Continuous Self-assessment
Assurance

***Figure 1:** Assurance stack*

1. **Continuous self-assessment:** A continuous self-assessment that can be implemented in a cost- and time-effective manner on the CSP's premises with no third-party involvement.

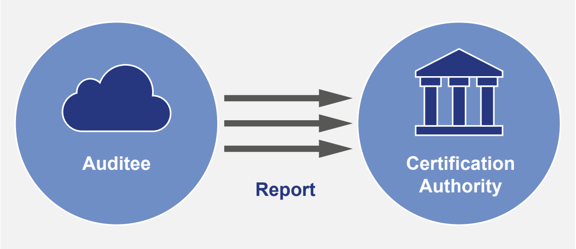

***Figure 2:** Continuous self-assessment auditing*

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

2. **Extended Certification with Continuous Self-assessment:** Combines a “point-in-time” third party certification with a continuous self-assessment by the CSP, giving more assurance to the stakeholder while building upon the existing security and privacy certification of CSPs. It ensures that the goals met by traditional audits are also subject to continuous self-assessment.

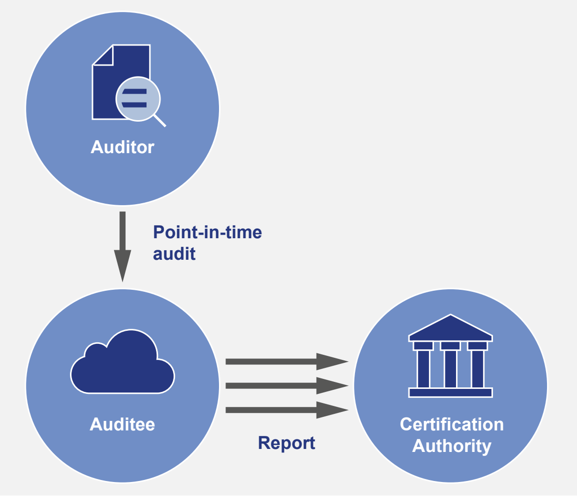

Figure 3: Extended Certification with Continuous Self-assessment

3. **Continuous certification:** Combines a “point-in-time” certification and a continuous assessment that are both performed under the control of an independent third-party auditing body. It gives the strongest level of assurance on the continuous fulfilment of certification goals. This document focuses on this level 3, which is the one that provides the complete continuous certification process. If you want to learn more about levels 1 and 2 please read EU-SEC Deliverable 2.2, which will give you detailed information on the other two levels.

   Let’s see how EU-SEC provided the level 3, “Continuous Certification”.

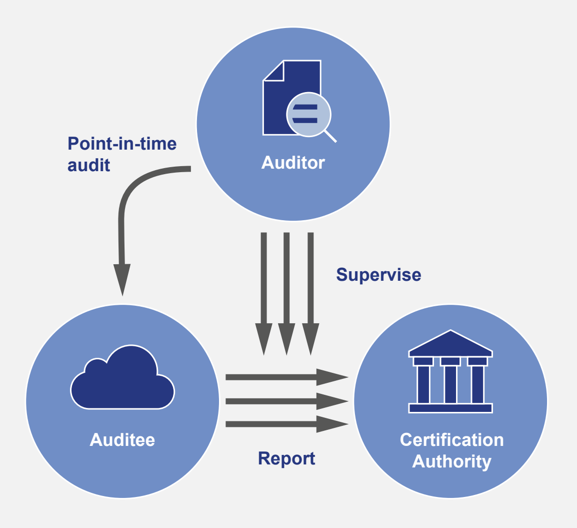

Figure 4: Continuous certification

2 Continuous certification

2.1 Mapping security controls to data

EU-SEC’s continuous auditing-based certification approach is based on normalised data, making assessments unambiguous, repeatable and comparable across different information systems.

How can we do it? We translate the security controls into actionable security “objectives”, which describe constraints on security attributes of an information system. Thanks to this process, we

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

are able to do systematic and more frequent compliance checks.

EU-SEC provides a model that views security controls as a set of objectives (called SLOs or SQOs) similarly to what happens when defining Service Level Agreements. Objectives are essentially constraints defined on the basis of security attributes of an information system. To verify that a certain security control is in place, a company should verify that the associated objectives are met.

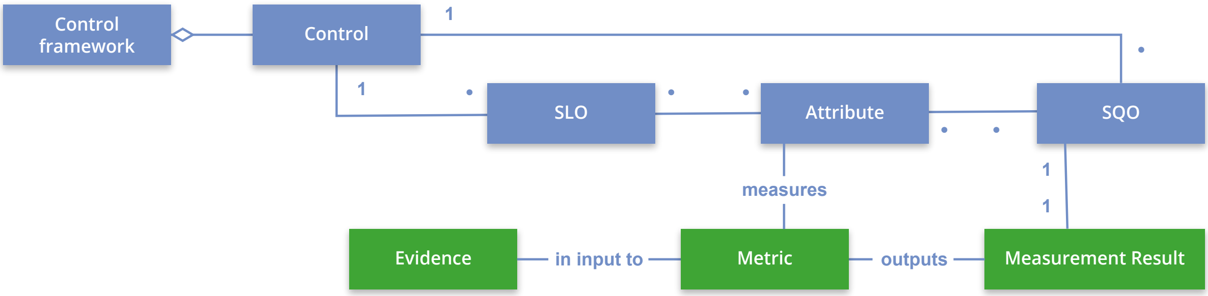

Figure 5: *Conceptual UML model for continuous auditing*

Figure 5 (blue boxes) shows the EU-SEC control framework, in which each control is defined by a set of SLOs and SQOs and related measurable attributes.

Each **control framework** consists of multiple controls, which are designed to give assurance on the fulfilment of a requirement. EU-SEC uses the CSA Cloud Control Matrix (CCM) as a reference control framework.

- When preparing for continuous auditing, each one of those **controls** has to be described via its characterizing objectives namely **Service Level Objective** (SLO), and **Service Qualitative Objective** (SQO).

- Objectives are described as constraints on one or more security or privacy **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.

For instance, consider a security control that establishes the requirement of monitoring network traffic: there are many different ways to define objectives that support this requirement depending on the deployment model and architecture of the cloud service. A IaaS provider will likely monitor inbound and outbound network traffic while a SaaS provider providing a mail service may check incoming and outgoing emails.

Those individual objectives have then to be described by individually chosen attributes. 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, which provides a qualification or quantification of an attribute. In this context, the measurement process consists of three elements (Figure 5 – green boxes):

- **Evidence** can be considered as the input in a measurement. Evidence can be as simple

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

as a plain number or as complex as a large unstructured document. The kind of evidence often defines whether it is suitable for automated reasoning of 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 human interpretation, the number of sources is much broader in a sense that even a screenshot or documentation, for example, can be considered as valid evidence. The level of evidence needed is based on the risk level and classification of that asset.

- **Metric**[1] is a standard for measurement. It defines the function that transforms the evidence into a *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 application of a measurement function (as defined by a metric) to a set of evidence in order to obtain a value that reflects a security attribute of an information system.

And how often do we have to measure and assess each control? Some controls are meant to satisfy policies requirements (e.g. User Policy), others to verify procedures (Incident Management procedures), while others are meant to verify specify technical implementation (patch management). Consequently, the frequency with which each control should be assessed varies. For example, an effective Identity Access Management will demand for short frequency assessment.

2.2 Reference architecture and role of automation

While the “point-in-time” certification is a linear 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.

The reference architecture provided by EU-SEC is divided into five steps, as shown in Figure 6.

- The first part of continuous auditing is the operationalization of the underlying controls. This first necessary step takes place in the **preparation phase**. Key actions in this phase are:
  - ○ Definition of the scope, selecting the controls to put in place in order to fulfil the certification requirements.

[1] As defined in ISO 19086-1

Metric example: Minimum required password length in characters.

Measurement result example: 8 characters.

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

  - Identification of the objectives (SQO, SLO) associated to each control.

  - Determination of the frequencies at which each objective should be checked.

  - Definition of attributes and metrics, as well as the identification of points where the measurements should be taken.

  If this part is supported or carried out by a third party like an auditor, it increases the level of assurance. Any third-party auditor involved in this phase will also need to certify that the tools that will be used in the following collection, measurement and evaluation steps are trustworthy and fit for purpose.

- The actual assessment takes place in the **execution phase**, which is running continuously. It consists of four subparts: Collection, Measurement, Evaluation and Certification (see Figure 6):

  - The **collection step** facilitates the collection of data for automated and non-automated assessment. Collection of data is driven by the metric that has been chosen to provide input about an attribute. Depending on the type of assessment, various tools could be used. Automated assessment is mostly driven by monitoring tools like log analytics, network statistics and monitoring, process statistics or resource utilization. Non-automated assessment requires human intervention to verify the existence and the effectiveness of certain processes, and to read documents or examine records.

  - The **measurement step** describes the processing that transforms the collected raw data into a usable measurement result.

  - In the **evaluation step**, the compliance status with the certification goal is determined by evaluating the controls.

  - The result of the evaluation has to be published and affirmed accwording to the targeted level of assurance by a third party. Achievement of the targets results in the issuing of a **certificate**.

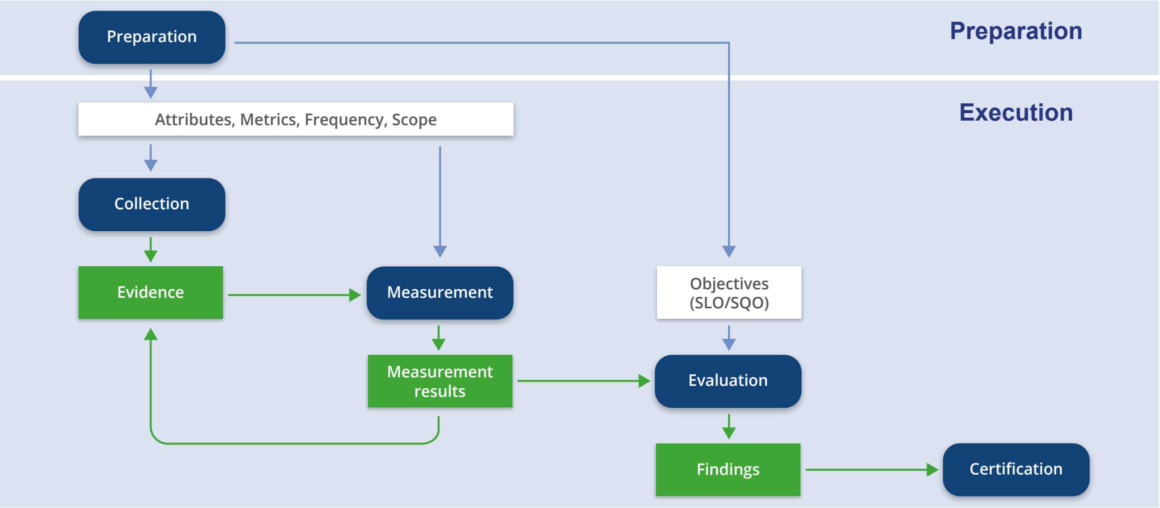

***Figure 6:** Conceptual UML model for continuous auditing*

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

2.3 Overview of the actors

There are several actors that play a significant role in the process of continuous auditing-based certification.

- **Cloud Service Customer**
  The role of the Cloud Service Customer is key, because it is the entity who will need and benefit from the continuously certified service. It is the entity that should establish the security requirements to be achieved by the CSP. It should validate the translation of those requirements into the SLO/SQOs that will be continuously measured.

- **Cloud Service Provider (CSP): Auditee**
  The entity who operates the service, the processes and controls to be audited is normally the CSP. It initiates and finances the continuous auditing process. It should be able to continuously provide the data to be leveraged in the audit, and it is responsible for working with the results of the auditing process.

- **Certification Body (CB): Authorized Auditor**
  The CB is a trusted party or organization, normally an auditor, which is recognized and qualified by the Certification Authority. Its main functionality is performing an audit with a view to 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, as a minimum, need to implement and maintain the auditing system.

- **Certification Authority (CA): Governance Body.**
  The EU-SEC Certification Authority (CA) or Governance Body is a trusted party that qualifies external auditors to perform audits and establish rules for recognition of external auditors.
  The CA provides guidelines on the establishment of a suitable scope for the creation of the Certification Target, defines acceptable Reporting Policies and monitors the transition of certificates through various states. Within continuous auditing, the CA publishes recommendations on data formats and data exchanges to enable measurability through external auditors and is also responsible for definition of interoperability guidelines.

What are the key roles and responsibilities to be carried out by the three main players (Auditee, Auditor and Certification Authority) in the continuous auditing-based certification process?

3 The Cloud Service Provider: Auditee

This section describes the key processes that are the responsibility of the auditee (in some cases in cooperation with the auditor). These are mainly:

- **Selection of controls to be audited.** This information will feed into a Statement of Applicability. This first step is the same as for a traditional audit.

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

- **Collection of technical evidence and objective evaluation.** This includes formalising as many requirements from the Statement of Applicability as possible. This step is what really distinguishes the continuous approach from the traditional audit method. The formalised requirements are the core of the Continuous Audit Based Certification approach; these controls can be automatically monitored to collect evidence on a continuous basis, to map the results to the compliance level of the scheme. This can, for instance, be done with the use of external tools proposed by the EU-SEC project.

- **Verification of integration.** This is carried out by a (technically advanced) auditor.

3.1 Selection of controls to be audited

Similar to preparations for a traditional audit, the CSP selects a set of controls that must be put in place in order to fulfil the requirements of the required certification. This results in a Statement of Applicability.

In most cases, the CSP will have already undertaken a traditional audit for the particular certification and there are therefore existing procedures to build upon.

In addition to the traditional audit procedures, the CSP has to select a set of SLOs and SQOs that can provide technical evidence to the fulfilment of a particular control, which we refer to as the "operationalization" of controls. The example of the EU-SEC pilot can be used as a guide for how to derive objectives from a (limited) set of CCM controls. Most importantly, the CSP has to keep in mind that not all controls can be formally operationalized and thus have to be kept as manually audited. This is an adaption and expansion of the Statement of Applicability.

3.2 Collection of technical evidence and objective evaluation

Once the operationalization of the controls is done, technical means have to be put in place to collect evidence to support the measurement of an objective. While in theory, numerous technical implementations are possible, the EU-SEC project aims to streamline this process by proposing two main components:

- The definition of an Audit API and evidence formats, available in an industry standard format.
- The use of an auditing tool to collect said evidences and evaluate it against a defined set of objectives, mapped to controls. A reference implementation of such an auditing tool exists in the form of the tool *Clouditor*.

The Audit API needs to provide auditing tools like *Clouditor* with the required evidence for assessing the effectiveness of the security efforts. In a nutshell, the Audit API collects the evidence from the (virtual) IT infrastructure, normalizes the data according to its rules and provides them to the audit tool for further assessment. As security efforts are mainly driven by securing the assets, the Audit API is also asset-driven.

The common element among most services is a multi-layered architecture, i.e. a web application running on top of a platform which then runs on top of an infrastructure. The Audit API addresses this by allowing multiple scopes for one service, referring to a single layer in the overall architecture. For example, “encryption” can be provided on multiple layers, meaning that evidence on encryption can provided for the infrastructure level, i.e. through use of encryption (virtual) hard disks, as well as the application level, i.e. through the use of Transport Layer Security (TLS).

The specification of the Audit API was made available as open source within the EU-SEC project[2]. It reflects a starting point for discussion and contributions are welcome by the community. Key to the individual implementation of the audit API is to map REST Endpoints to the correct data sources. Data sources in this sense are log files, configuration files, databases, or even third party APIs, i.e. from the underlying IaaS Cloud provider, if the CSP itself has only a Software-as-a-Service offering.

Afterwards, the fulfillment of a specified objective can be continuously and automatically evaluated. The EU-SEC project proposes a class of auditing tools to assume this role and specifies a blueprint in the EU-SEC deliverable D3.5. Additionally, in order to accelerate the market adoption of continuous certification, a reference implementation of the *Clouditor* tool was made available during the course of the project. Clouditor’s Community Edition is open source and can be retrieved freely from GitHub[3]. It is a standalone application which can be run, e.g., as part of the infrastructure to be audited. Integration guides of Clouditor are included in the GitHub repository.

However, it should explicitly be noted that the project welcomes the adoption of the framework through other existing or upcoming commercial or freely available tools or even a custom toolchain put in place by the CSP itself. The latter however, will probably result in a bigger effort of tool integration verification through an auditor, since it is safe to expect that any serious commercial tool vendor already can provide a certified development process.

Regardless of the choice of tooling, the following high-level steps should be considered:[4]

1. Drawing on the general integration strategy, the deployment strategy is determined, that is, the CSP needs to decide where to run the continuous audit tool. This may even mean to leverage third party services, that provide the auditing tool as a service, running outside of the premises of the service under audit. Alternatively, the tool can be deployed within the infrastructure of the provider which is the expected case if evidence as well as measurement results produced by the audit tool must not leave the domain of the provider as by the provider’s general data security policy.

2. Once the continuous auditing tool is deployed, it needs to be configured following the evidence available from the cloud service provider’s

[2] https://github.com/eu-sec/continuous-auditing-api-spec

[3] https://github.com/clouditor/clouditor

[4] An extensive description of central concepts when integrating the entire tool chain to conduct continuous security audits can be found on Working Package 3.4, Section 3.2.

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

Audit API implementation (which will, in turn, determines computable measurements). This implies that a tool provider must be able to perform some form of Audit API discovery, naturally ideally in an automated manner.

3. Having configured the auditing tool according to the available evidence, the tool can be started, collects evidence from the Audit API and computes measurement results.

4 Certification body (CB): Authorized Auditor

Certification bodies and auditors have an important role in the continuous auditing-based certification as independent third-party, conducting the audits and monitoring of automated controls. Traditionally, depending on the target certification, the role of the auditor has been to produce an audit relying on evidence collected from the environment during the audit process. For example, in an ISO 27001-based certification, the surveillance activities of the certification have typically been quite simplified. Certification has only been revoked if an auditor and/or any other party has provided information manually about a breach of certification. There have not been any methods on how a certification body or auditor could automatically follow if requirements are being met between the initial audit and re-certification audit phase.

When looking at the certification levels in the continuous audit-based model, it can be seen that auditors are involved in the two highest levels.

- Level 2 / Extended Certification with Continuous Self-assessment: providing the traditional auditing services and the auditee is responsible for the continuous monitoring
- Level 3 / Continuous Auditing: providing the traditional audits as well as the continuous certification by monitoring pre-defined security controls.

We are only describing the Level 3 in this document because Level 3 is used in third-party certification providing the highest level of assurance.

4.1 Traditional audits still play a key role

Traditional audits are not redundant in a continuous auditing-based certification scheme. They are complemented by the active monitoring of security controls, which provides the assurance of **continuous security** instead of relying on notification-based surveillance processes and predefined certification maintenance checks. For the auditor, the traditional approach for conducting audits can be considered mostly as a project-type assignment, which has a defined start and end point and the process follows a predefined workflow. The approach has its advantages, which is the reason why traditional audits continue to be essential in continuous certification process.

When an organization implements the continuous auditing process, there are still several steps which have to be conducted using traditional auditing methods. Many of the technical controls can be broken down to objectives measurable by technology, but human intervention is still required in the certification process since some

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

requirements cannot be automatically monitored. For example, adequacy of written security policies requires analysis from a competent auditor to determine whether the policy is complying with the audited standard and whether that policy is implemented in the auditee's environment. Secondly, traditional audits allow in-depth analysis of the target environment with multiple methods of verification to ensure that all of the requirements are met. Automated controls are designed to measure the targeted objectives by following predefined sets of rules. Human auditors have the possibility of using multiple and creative ways of verifying information and therefore providing a broader image of the auditee's compliance.

Generally, default rules apply in traditional audits:

- Requirements for auditors are set by the standard owner/certificate authority
- Traditional audits are conducted according to the auditing guidelines for the target certification.
- Standard defined certification lifecycle shall be followed, even when using continuous auditing-based certification.

4.2 Continuous audit monitoring

For auditors, the most significant addition provided by the framework is the responsibility for continuous audit monitoring which on the lower certification levels is done by the auditee but in continuous certification is part of auditor's responsibilities.

- The auditor is provided with access to the monitoring tools so that the auditor has the ability to verify the monitoring tools' evaluation results as well as the configuration of the monitoring tools.
- The auditor is responsible for maintaining the status of the certification.

The preparation phase for continuous auditing is critical for successful monitoring. Key action for this preparation phase is the identification and definition of the Service Level Objectives (SLO) and Service Qualitative Objectives (SQO) associated to each control. Each of the SLOs and SQOs selected must be predefined so that they include the frequency at which each of the objectives is checked, the definition of attributes and metrics, as well as the identification of points where the measurements should be taken.

From the auditor perspective, trustworthiness and appropriateness of the defined attributes used in continuous monitoring process is one of the key aspects. The auditor should check if those attributes fulfill the requirements set by the certification scheme and currently this might be difficult. The auditor needs to understand how and based on what these attributes are created. There are some reference points created (e.g. ISO 19086-2/3/4) and there might be some regulation set by local authorities. But nevertheless, the auditor must be aware of required attributes before trusting the continuous auditing process.

In some situations, the auditor could be the one creating these rules; thus, this requires high level of knowledge from the auditor's side.

In addition to the quality of SLOs and SQOs, CABC relies on the quality and expressiveness of the evidence provided for further assessment. Like the evidence provided in a traditional "point-in-time" audit, it should be sound and suit the purpose of an audit. As evidence is gathered in the collection phase it has to be ensured that all data is reasonable and suitable for the assessment in the evaluation phase. Similarly, the measurements and the evaluation have to be performed in way that the compliance status is reflected as precisely as possible. Implementing CABC accordingly is the responsibility of the CSP, but additional trust on the soundness has to be established if a continuous certification is targeted. This means that besides the actual audit, in which compliance to requirements is evaluated, the CABC implementation itself is evaluated by the auditor.

This requires the auditor to perform the following steps:

1. Evaluate the correct implementation of the security requirements inside the scope.
   a. Gather evidence for each control.
   b. Asses if the evidence proves the proper implementation
2. Check the CABC Implementation, if the controls that are subject to CABC are assessed in a similar manner.
   a. Check if the right objectives are addressed
   b. Check if the objectives are described by proper attributes
3. Check if the measurement process is providing suitable results
4. Check if the right evidence is used.

4.3 Trusting the monitoring tools used

The execution phase of the continuous auditing is achieved by using automated monitoring tools to provide the collection, measurement and evaluation of SLOs and SQOs. To gain widespread adoption of the tools among auditors, the monitoring tools need to be trusted.

Trust is achieved by using monitoring tools and architectures which are designed and built securely. As shown in figure 3 the execution phase is divided in four different steps:

1. Collection of the evidence using the SLO/SQO attributes defined in preparation phase. Tools and APIs used to collect the information from audited environment must be designed and implemented securely.

2. Tool used for measurement of the collected raw data to usable measurement result must be designed securely.

3. Tools and methods used for evaluation phase must be designed securely.

4. Tools used for certification phase must be

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

In order for the auditor to trust the information collected and handled during the continuous auditing process, securely designed monitoring tools must be used. During the EU-SEC continuous auditing phase, analysis of the pilot architecture security was conducted and the required level of trust was achieved. However, it should be noted that each implementation of the monitoring tools differs and as such should first be evaluated by a third-party. The most efficient way to gain trust of monitoring architecture is to rely on certified products and platforms.

5 Certification authority (CA): Governance Body

The certification authority must deal with the following processes:

- Accreditation of certification bodies
- Maintenance of public registry of continuously certified cloud services
  - Initiation of a continuous audit/based certification
  - Collection of results from a continuous assessment
- Dealing with complaints from stakeholders
- Maintaining best practices for metrics used in SLO/SQOs.

5.1 Accreditation of certification bodies

A Certification Body (CB) is required to intervene for Extended Certifications or Continuous Certifications. In addition to traditional third-party assessments, the CB must check that the tools are fit for purpose and trustworthy. This requires an additional set of skills (e.g. code analysis, version integrity, etc.).

The CA will specify the relevant requirements for CBs that want to conduct continuous assessments. Accredited CBs will be listed by the CA in a registry.

5.2 Initiation of a continuous audit-based certification

The auditee, namely the CSP, submits a certification target to the CA, as a file that contains:

- The identity and a description of the scope of the audited information system,
- The SLOs/SQOs that describe the security guarantees of the target information system,
- The assessment period defined for each SLO/SQO,
- The start date and end[5] date for the continuous audit.

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

In addition to the certification target, the submitter will specify the target continuous assurance level: (1) Continuous Self-Assessment, (2) Extended Certification or (3) Continuous Certification.

The CA must verify the identity of the submitter and that the target information system is owned by the submitter. The CA also applies a consistency check on the submitted target certification (e.g. the start date should not be in the past).

In the case of a Continuous Self-Assessment, no other steps are needed.

In the case of an Extended Certification or a Continuous Certification, the CA will also confirm[6] with the designated CB that the certification target was approved.

The Auditee will receive an API key that will be used to authenticate the submission of assessment results during the continuous auditing process, as described in the next section.

Once all verifications are completed an entry is created in the CA's public registry of continuous certification. This publicly accessible entry contains the following information:

- The identity and a description of the scope of the audited information system,
- The target assurance level (Continuous Self-Assessment, Extended Certification or Continuous Certification).
- The start and end date of the continuous assessment
- The last verification date: the date and time when the target information system was last considered as valid.
- The state of the assessment:
  - Pending: if the start date has not been reached yet.
  - Ended: if the end date has been reached.
  - Running: if
    - The start date has been reached.
    - The end date has not been reached.
    - The assessment has not been revoked.

Revoked assessments are removed from the public registry. Until the start date is reached, the last verification date is blank.

In addition to the public entry previously described, a private "view" of the assessment is created for the Auditee. With this private view, the Auditee can access a copy of the submitted certification target and the status of the continuous assessment, including result submission logs. In case of a non-compliance, this view enables the Auditee to identify the SLO/SQOs that were not met, giving information that is otherwise not publicly available.

[5] The end date should correspond to the start date plus one year.

[6] This could be achieved with a cryptographic signature applied to the certification target.

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

5.3 Collection of results from a continuous assessment

A standardized API enables the CA to collect continuous assessment results from the Auditee. An API key that is known only to the Auditee protects the API.

An assessment result must be regularly submitted to the CA with this API for each SLO/SQO defined in the certification target, according to the specified assessment frequency. For example, if an SLO must be assessed every 24 hours, the CA will expect to receive one result for every period of 24 hours, beginning from the start date defined in the certification target. The CA will consider a SLO/SQO to be met if the submitted assessment result meets all the following criteria:

- The result indicates that the SLO/SQO is met.
- The result is submitted before the expiry of the current assessment period, taking the certification target start date as a reference for the start of the very first period.
- The assessment timestamp provided with the result falls within the current assessment period as well.

If all SLO/SQOs are valid, the CA will update the corresponding entry for the assessed information system in the public registry, setting the last verification date to correspond to the latest submitted result assessment timestamp.

If the Auditee fails to submit a result within the predefined period, or if the submitted result does not meet the criteria defined above, the assessment is considered as “suspended”. The corresponding entry for the assessed information system in the public registry is not updated.

The assessment can leave “suspended” state if the SLO/SQOs become valid again, in a following period.

If the target information system remains in “suspended” state for a duration that exceeds a threshold called the “grace period”, then the continuous assessment is considered as revoked and the corresponding entry is removed from the public registry.

5.4 Dealing with complaints from stakeholders

The CA provides a point of contact to deal with complaints from stakeholders, most notably:

- Cloud users that report a potential non-compliance affecting an information system undergoing a continuous assessment.
- Auditees or CBs that believe that a continuous assessment was unfairly revoked.

The CA must review and address these complaints.

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

5.5 Defining standards and best practices for metrics used in SLO/SQOs

It is strongly desirable to have uniform metrics for SLO/SQOs across the whole industry:

- It gives monitoring tool maker a target
- It facilitates the work of CBs that can build experience accordingly
- It makes information systems more comparable in terms of security.

The CA should maintain an industry-wide working group to work towards the creation and maintenance of a catalogue of standardized metrics for continuous monitoring.

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