EUSEC
EU SECURITY CERTIFICATION

WHITEPAPER

Continuous auditing certification

State of the Art in cloud service certification

Cloud computing has emerged as the de-facto-standard when it comes to IT delivery. It comes with many benefits, such as flexibility, cost-efficiency and maintenance reduction. But adoption of cloud computing also means shifting from direct control and governance over security and privacy to an indirect form of control, which is a great concern for many cloud customers. CSPs have addressed this issue by increasing the level of assurance and transparency around the security and privacy capabilities they have implemented, although there remains a need to establish a deeper level of trust between the CSP and the cloud customer.

Third party audits and certifications have become the most effective solution to increase the level of trust in the reliability of security and privacy measures implemented by CSPs. Such audits are traditionally performed annually or bi-annually, which means that whenever interim changes are made to security and privacy practices, the change and effectiveness of these amendments are not evaluated by the assessors until the next official check. This creates gaps in assurance during the periods between surveillance audits. While this may be an acceptable risk for some cloud customers, for others, these assurance gaps remain a strong barrier to cloud adoption.

EU-SEC's contribution

Unified architecture

The EU-SEC project is developing a process that will bring continuous assurance by addressing the lack of regularity and proactivity of traditional "point-in-time" certifications.

The method developed for this is called **continuous auditing based certification**. This process will complete the Level 3 of the Open Certification Framework and builds upon the STAR Level 1 and Level 2.

By 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 a continuous workflow. State of the art security monitoring systems supervise the organization's security status by collecting data from the CSP's information system. This collected data is further assessed and used as the basis for continuous auditing.

EU-SEC's continuous auditing approach is based on normalised data, making assessments unambiguous, repeatable and comparable across different information systems. During the data normalisation process, security controls are translated into actionable security "objectives", which describe constraints on security attributes of an information system. This process enables systematic and more frequent compliance checks.

The EU-SEC project has received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement no 731845.

From Monitoring data to certification.

Assessing controls in a standardised way makes it possible to compare and validate the security characteristics of an information system. 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.

1. **Continuous self-assessment auditing:** 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.

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.

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.

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**. A certification based on more frequent assessment of controls is particularly in demand by cloud customers with sensitive data, such as financial institutions or companies in the health sector. Currently, they cannot obtain an up-to-date verification that their data is subject to good practice by CSPs. By applying continuous certification, the level of trust, transparency and assurance is greatly improved.

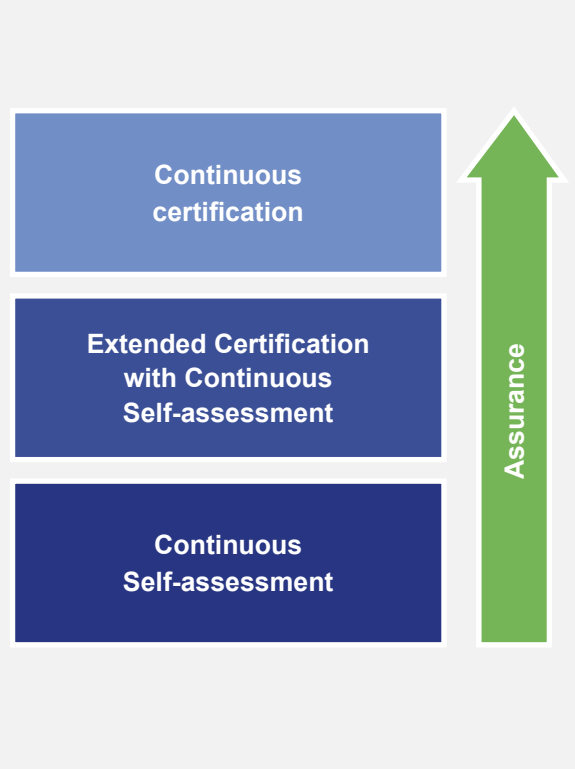

Figure 1: Assurance

The EU-SEC project has received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement no 731845.

User Stories

Who benefits from continuous auditing certification?

Alice
is an executive in a mid-sized CSP that offers IaaS solutions. Her company has adopted all industry renowned cloud security certifications. In meetings with potential customers, she often witnesses their reluctance towards moving their IT onto her company's services. She recognizes that those concerns are raised more often from people in highly regulated sector such as banking and healthcare who provide critical services and deal with sensitive data. In addition, those customers often complain about the difficulties in satisfying their regulators requests especially when it comes to including the right to perform first party audit in cloud contracts. Her company already monitors all the security and privacy related data and operations within their IT-infrastructure as well as the rest of the organization, but for security reasons cannot allow customers to perform first party audits on her company infrastructure. What Alice needs is a way to use this real-time data as a proof of that they have successfully implemented security and privacy measures in a standardized and verifiable way and that the effectiveness of that system is assessed and confirmed. This would reassure current and potential customers concerned about risk, governance and compliance. The answer is for Alice to adopt continuous certification as the best way to communicate her company's efforts to her customers and represent a suitable alternative to the customers' right to audit. In addition to increased trust and transparency for users, it gives her company a competitive advantage over bigger and less flexible CSPs.

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 to regulations. The majority of the industry already moved to the cloud since it introduced advantages over an in-house-solution like on demand scalability or increased security. But regulators, especially in the banking sector, are demanding 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 occurring in the IT's daily operations, Bob is capable of proving his achieved level of security to the regulators. If necessary even via a third party audit. CSPs usually have certifications that show they comply with industry security standards but other than that they rarely provide information that will help Bob to justify to the regulators the increased level of security of a cloud solution on a frequent basis. Since the certifications are usually performed on an annual bases 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 ensures 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.

The EU-SEC project has received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement no 731845.

Technical Details

Mapping security controls to data

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 controls is in place a company should verify that the associated objectives are met.

For this reason, the key element of continuous auditing is the definition of those measurable attributes and objective that describe a security controls, as show in Figure 2 (Blue):

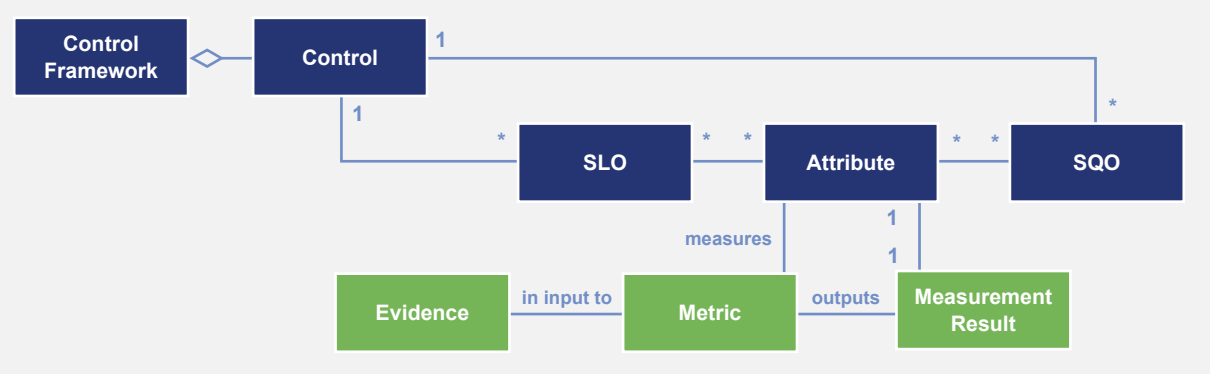

Figure 2: Conceptual UML model for continuous auditing.

- 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 constrains 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.

In this case an objective is specific to the requirements of the CSP. For instance, consider a security control that establishes the requirement of monitoring network traffic: there 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. In this process, information that is either obtained from

The EU-SEC project has received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement no 731845.

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.

It is also important to note that security controls are context specific, their implementation will vary depending on the specificity of the risk appetite and technological environment of the CSP. Moreover, some controls are meant to satisfy policies requirements (e.g. User Policy), others to verify procedures (Incident Management procedures) and while others are meant to verify specify technical implementation (patch management). Consequently, the frequency with which each control should be assessed varies. An example for short frequency would be the control for an effective Identity Access Management where constant accesses demand a higher frequency.

A measurement (Green in Figure 2) provides a qualification or quantification of an attribute. In this context, the measurement process consists of three elements:

- **Evidence** can be considered as the input in a measurement. Evidence can be as simple as a plain number or as complex as a large 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 human interpretation the number of sources is much broader in a sense that even a screenshot or documentation can for example be considered as valid evidence. What 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.

Metrics provide knowledge about the attributes of an IT infrastructure, through units, rules and the values from the analysis of the evidence. The evidence is processed into a result via a metric.

[1] As defined in ISO 19086-1.

Metric example:
Minimum required password length in characters.

Measurement result example:
8 characters.

The EU-SEC project has received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement no 731845.

Technical Details

Mapping security controls to data

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.

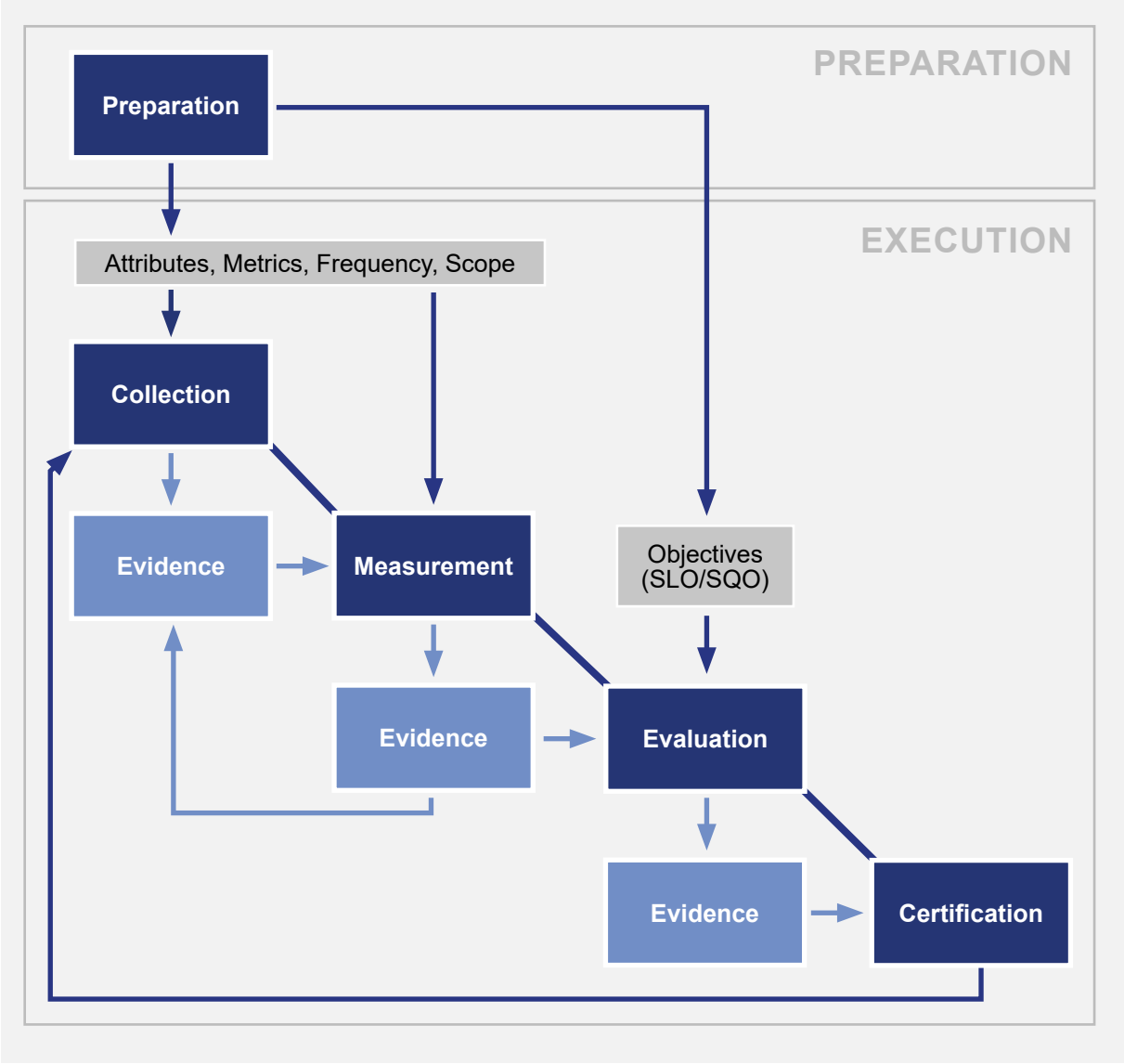

Figure 3: Model of continuous auditing phases

The EU-SEC project has received funding from the European Union’s HORIZON 2020 research and innovation programme under grant agreement no 731845.

The reference architecture provided by EU-SEC is divided in five phases, as shown in Figure 3.

1. The first part of continuous auditing, as developed in the EU-SEC Framework, is the operationalization of the underlying controls. This first necessary step takes place in the **preparation phase**. 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. If this part is supported or even realized by a third party like an auditor, it increases the level of assurance. Any third auditor involved in this phase will also need to certify that the tools that will be used in the following collection, measurement and evaluation phases are trustworthy and fit for purpose.

2. The actual assessment takes place in the **execution phase**, which in running continuously. It consists of four subparts: Collection, Measurement, Evaluation and Certification. See Figure 2.

- The **collection phase** facilitates the collection of data for automated assessment 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. While non-automated assessment requires human intervention to verify on the existence and the effectiveness of certain processes, and to read documents or examine records.

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

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

- The result of the evaluation has to be published and affirmed according to the targeted level of assurance by a third party. It can result in the issuing of a **certificate**.

Translating evaluation to certification

The result of each evaluation is continuously collected by a trusted authority and is used to determine whether or not a certificate is awarded to a particular subject. If a non-conformity is reported or if an objective is not reported in due time, the certificate is temporarily “suspended” until the issue is corrected. If the certificate stays in a suspended state beyond a certain “grace period”, the certificate is revoked, and the subject must start the whole certification process again.

There are 3 certification models as previously described in figure 1. The selection of a particular certification model determines the level of assurance provided by the evaluation results:

The EU-SEC project has received funding from the European Union’s HORIZON 2020 research and innovation programme under grant agreement no 731845.

1. In **Continuous self-assessment auditing**, the evaluation is purely based on a self-assessment with not involvement from a trusted third party.

2. In an **Extended Certification with Continuous Self-assessment**, an independent auditor will be expected to evaluate the tools and processes used to collect measure and produce evaluations during a “traditional” point in time initial audit.

3. In a **Continuous certification**, an independent auditor will perform the same work as in the Extended Certification with Continuous Self-assessment, but will also supervise the reporting of evaluations during the continuous audit phase. This means that the auditor will likely have a greater influence on the tools and processes that are put in place by the subject, for interoperability and maintenance purposes.

Conclusion

Continuous Auditing specifies the necessary activities and conditions for the continuous auditing of the cloud service over a defined set of security requirements, covering aspects from governance to infrastructure, and requiring the cloud service to define necessary processes that will be executed during the validation of controls within the scope of assessment. The program promotes trust by ensuring that a cloud service’s necessary activities and conditions are continuously met by through continuous auditing, such as through the operationalization of security and privacy requirements.

This empowers cloud service providers to make precise statements on compliance status of their cloud services covered by the continuous audit process, achieving an “always up-to-date” compliance status.

The EU-SEC project has received funding from the European Union’s HORIZON 2020 research and innovation programme under grant agreement no 731845.