EUROPEAN SECURITY CERTIFICATION FRAMEWORK

DELIVERABLE

VERSION: 1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EUSEC

D1.4 PRINCIPLES, CRITERIA AND REQUIREMENTS FOR A MULTI-PARTY RECOGNITION AND CONTINUOUS AUDITING BASED CERTIFICATIONS

DUE DATE:	DELIVERY DATE:
31.12.2017	6.3.2018
AUTHOR:	PARTNERS CONTRIBUTED:
Cloud Security Alliance	MFSR, NIXU, PwC
DISSEMINATION LEVEL:*	NATURE OF THE DELIVERABLE:**
PU	R
INTERNAL REVIEWERS:	
Fabasoft, MFSR, SixSq	

*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

EU-SEC project has the ambition to make the current cloud security and privacy certification landscape more effective and efficient. These objectives will be mainly reached by the creation of a multiparty recognition framework for third party audit-based certification and new approach to cloud assurance based on continuous auditing-based certification. This current document covers the foundation of both by detailing the criteria, principles, and requirements on which the EU-SEC multiparty recognition framework and continuous auditing certification framework are based upon.

In order to define the requirements for the EU-SEC multiparty recognition framework, we initially identified the key components of a generic third-party-audit-based certification and then we defined criteria for comparing them. Subsequently we defined high-level principles, which are applied to the certification scheme components and criteria. On these basis, we were able to identify the requirements that a scheme should fulfil in order to achieve the necessary level of quality, robustness and thoroughness and consequently be part of a mutual recognition framework suitable for the European market.

In total we identified five criteria, four core principles, and total of 31 requirements for mutual recognition between different third-party-audit-based certification schemes. Furthermore, we recommend that the EU-SEC governance framework builds on the process lifecycle defined in this document to ensure the long-term sustainability and exploitability of the EU-SEC framework after the finalisation of the project.

Moreover, this document laid out the foundations for a continuous auditing-based certification framework. We provided a set of definitions, that building on existing literature on continuous monitoring, security parameters and service levels, defines some key concepts for the creation of a continuous-auditing-based certification. We highlighted three certifications models each one based on different certification policies and a variable level of involvement of third parties and of automatic controls verification.

Finally, we provided a list of requirements for the creation of a continuous auditing-based certification framework. Ideally, we would like continuous auditing to be fully automated, thereby reducing costs and increasing the potential frequency of assessment. In practice, we acknowledged that is not realistic given the state of the art in certification today. As a

consequence, our requirements take both into consideration automated and non-automated continuous auditing processes, which together will form the basis of a continuous certification.

EU-SEC aims to pioneer the creation of the very first continuous auditing-based certification framework. As consequence, the issue of mutual recognition does not apply today to continuous certification. Nevertheless, the requirements we defined for mutual recognition can be applied to continuous certification as well, should we see the emergence of a plethora of continuous certification schemes in the future.

ABBREVIATIONS

Table 1. Abbreviations used in this document.

Abbreviation	Description
ANSSI	Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France) (https://www.ssi.gouv.fr/en/)
BSI C5	The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) Cloud Computing Compliance Controls Catalogue. (https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html)
CPA	Certified Public Accountant (CPA) is the title of qualified accountants in numerous countries in the English-speaking world. A CPA is an accountant who has satisfied the educational, experience and examination requirements of his or her jurisdiction necessary to be certified as a public accountant.
CSA	Cloud Security Alliance (https://cloudsecurityalliance.org/)
CSA 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)
CSP	Cloud Service Provider
D1.2	EU-SEC deliverable of task 1.1 "Security and privacy requirements"
D1.3	EU-SEC deliverable of task 1.2 "Auditing and assessment requirements"
D2.1	EU-SEC deliverable of tasks 2.1 "Multiparty recognition framework"

Abbreviation	Description
ISAE	Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000) describes general requirements for the qualification and conduct of an auditor (e. g. professional judgment and skepticism) as well as for accepting, planning and carrying out an audit engagement i.e. it is a high-level auditing standard which provides the required high-level framework.
ISO	International Organization for Standardization (https://www.iso.org/home.html)
ISO/IEC 17021	ISO/IEC 17021-1:2015 Requirements for bodies providing audit and certification of management systems (https://www.https://www.iso.org/standard/61651.html.org/standard/61651.html)
ISO/IEC 17024	ISO/IEC 17024:2012 General requirements for bodies operating certification of persons (https://www.iso.org/standard/52993.html)
ISO/IEC 19011	ISO/IEC 19011:2011 Guidelines for auditing management systems (https://www.iso.org/standard/50675.html)
ISO/IEC 27001	ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements (https://www.iso.org/isoiec-27001-information-security.html)
ISO/IEC 27006	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems (https://www.iso.org/standard/62313.html)
ISO/IEC 27007	ISO/IEC 27007:2011 Guidelines for information security management systems auditing (https://www.iso.org/standard/42506.html)
MFSR	• Ministry of Finance of the Slovak Republic (http://www.finance.gov.sk/en/)
SECNUMCLOUD	Requirements Framework for Cloud Service Providers published by Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France) (https://www.ssi.gouv.fr/en/) (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.0_niveau_essentiel.pdf)
SLA	Service level agreement

Abbreviation	Description
SLO	Service Level Objective - a commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale service (ISO/IEC 19086-1:2016, 3.5).
SOC 2	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (https://www.ssae-16.com/soc-2/)
SQO	Service qualitative objective

Table of Contents

LIST OF TABLES

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

The deliverable D1.4 uses following terminology. Each used term is explained, while existing defined terms have reference to original standard definition.

Table 2. Terms and definitions.

Term	Definition	Source
Accreditation	Accreditation assures users of the competence and impartiality of the body accredited.	http://www.iaf.nu/
Accredited cloud service provider	A cloud service provider that has at least one registered certified cloud service in the Multi-party recognition framework.	
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
Attestation	An issue of a statement that conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees.	ISO 17000:2004, 5.2
Attribute	A property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.	ISO/IEC 27000:2014
Audit	a 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 conclusion	Outcome of an audit, after consideration of the audit objectives and the audit findings.	ISO 9000:2005, definition 3.9.5
Audit criteria	Set of policies, procedures or requirements used as a reference against which *audit evidence* is compared Note 1: Policies, procedures and requirements include any relevant Service Qualitative Objectives (SQOs) or Service Level Objectives (SLOs).	ISO/IEC 19011:2011, 3.2
Audit evidence	Records, statements of fact or other information which are relevant to the *audit criteria* and verifiable. Note: Audit evidence can be qualitative (e.g. a document) or quantitative (e.g. KPIs, thresholds, etc.)	ISO 9000:2005, definition 3.9.4

Term	Definition	Source
Audit programme	Arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose.	ISO 9000:2005, definition 3.9.2
Audit scope	Extent and boundaries of an audit	ISO 9000:2005, definition 3.9.12
Auditee	Organization being audited.	ISO 9000:2005, definition 3.9.8
Auditor	Person who conducts an audit.	ISO/IEC 19011:2011, definition 3.8
Authority	A trusted party that is responsible for the correct organization of a certification scheme, including the accreditation of auditors and keeping a registry of certified cloud services.	
Authorized Auditor	An auditing organization/auditor authorized by the certification authority/scheme owner to conduct assessments against the requirements of the scheme.	
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
Certification scheme	The set of rules, requirements and mechanisms that govern the process of certifying a process or a product. **NOTE**: In this document we use interchangeably "certification scheme" and "compliance scheme" noting that in the real term practise often time the term "certification scheme" is used when referring to ISO-based certification while the term "compliance scheme" is used when referring to ISAE 3000 audits.	EU-SEC D1.4 (this document)
Cloud Controls Matrix	provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains *(CSA, 2016)*. Cloud Control Matrix is used as a central cloud service requirement scheme.	
Cloud service	A software service available in a cloud.	
Cloud service customer	A body that contracted a cloud service.	
Cloud service provider	A third-party company offering a cloud service.	

Term	Definition	Source
Cloud service security ontology	A formalization describing domain of cloud service security and data privacy.	
Competence	Ability to apply knowledge and skills to achieve intended results.	ISO/IEC 19011:2011, definition 3.17
Conformity	Fulfilment of a requirement	ISO 9000:2005, definition 3.6.1
Conformity Assessment	Conformity assessment involves a set of processes that a product, service or system meets the requirements of a standard.	https://www.iso.org/conformity-assessment.html
Continuous auditing	An on-going assessment process that aims to determine the fulfilment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.	EU-SEC D1.4 (this document)
Continuous Certification	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.	EU-SEC D1.4 (this document)
Control	A safeguard or countermeasure requirement prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	CCM mapping methodology
EU-SEC Security Requirements Repository	A repository of all collected requirements mapped against the CSA CCM, making it a native control framework to address the identified requirements	EU-SEC D1.2 v1.2
EU-SEC Security Requirements Repository	EU-SEC Requirements and Controls Repository	EU-SEC D1.4 (this document)
Finding	Results of the evaluation of the collected audit evidence against audit criteria. Note: This notably includes the result of comparing the measurement results with SLOs and SQOs, so as to determine if objectives are met.	ISO 9000:2015, definition 3.13.9
Governing Body	A body responsible for governance of the Multi-party recognition framework and for maintenance of its repositories.	

Term	Definition	Source
Information Security	Maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms “continuous” and “on-going” in this context mean that security and privacy controls and organizational risks are assessed and analysed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.	NIST SP 800-57
Management system	System to establish policy and objectives to achieve those policies.	ISO 9000:2005, definition 3.2.2
Measurement	A set of operations having the object of determining a measurement result	NIST 500-307
Measurement result	A value that expresses a qualitative or quantitative assessment of an attribute of an entity	NIST 500-307
Metric	A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement. Note: The word “metric” is often used colloquially and incorrectly to describe “measurement results”. A metric is not a value but a specified process for obtaining a value.	NIST 500-307
Multi-party recognition	A process for establishing a mutual agreement between certification and compliance scheme owners for recognition of the full or partial equivalence between the certification and/or attestation they govern.	EU-SEC D1.4 (this document)
Nonconformity	Non-fulfilment of a requirement	ISO 9000:2005, definition 3.6.2
Personal data	Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	European Parliament, 2016

Term	Definition	Source
Personal data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or MS law, the controller or the specific criteria for its nomination may be provided for by EU or MS law	European Parliament, 2016
Personal data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a personal data controller	European Parliament, 2016
Requirement	A need or expectation that is stated in a standard, law, regulation or other documented information, generally implied (i.e. it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied), or obligatory (usually stated in laws and regulations)	ISO/IEC 27000:2016
Risk	Effect of uncertainty on objects	ISO Guide 73:2009, definition 3.9.2
Security attribute	An attribute which describes security property or characteristic of a cloud service.	
Service agreement	A documented agreement between the cloud service provider and cloud service customer that governs the covered service.	ISO/IEC 19086-1:2016, 3.3
Service level agreement	A part of the service agreement that includes service level objectives and service qualitative objectives for the covered cloud service(s).	ISO/IEC 19086-1:2016, 3.4
Service Level Objective (SLO)	a commitment a cloud service provider makes for a specific, quantitative attribute of a cloud service, where the value follows the interval scale or ratio scale service	ISO/IEC 19086-1:2016, 3.5
Service Qualitative Objective (SQO)	a commitment a cloud service provider makes for a specific, qualitative attribute of a cloud service, where the value follows the nominal scale or ordinal scale service	ISO/IEC 19086-1:2016, 3.6
Suspended Certification	The production of a statement indicating a failure to report at the expected frequency that an information system meets a predefined SQO and/or SLO.	

1 INTRODUCTION

A few years ago, when the Cloud Computing revolution began, most organizations faced a dilemma. On the one hand, Cloud Computing seemed to offer clear benefits regarding cost and security. On the other hand, Cloud Computing created uncertainty regarding compliance and trust. Since then, this dilemma has often been successfully solved through the use of certification or attestation, based on industry-wide standardized compliance frameworks. Cloud Service Providers (CSPs) have submitted their services to the scrutiny of (1) the community, through self-assessment results published in public registries, such as the CSA STAR Registry[1], and (2) independent external auditors, giving back to their customers a certain degree of assurance and trust. Despite this success, certification or attestation has its shortcomings.

The first shortcoming is a product of the success of certification or attestation: there are perhaps too many compliance schemes on the market today. Initially, CSPs relied on general information assurance schemes such as ISO 27001 or audit firms applying ISAE 3000 to provide SOC 2 attestation report on selected TSC categories. Soon, Cloud Security Alliance (CSA), a partner in the EU-SEC project[2], created one of the first global cloud-centric certifiable and attestable requirement schemes through the STAR program. Additionally, regional authorities and other industry players also introduced their own compliance standards to address national or sector-specific needs. Today, as a result, there is a plethora of compliance schemes that CSPs need to address to gain market access, to the point of creating a burden, especially for innovative smaller players trying to compete with the leaders in the field.

The second shortcoming of certification or attestation appears for organizations that have above-average assurance requirements such as in the banking or the healthcare sector. These stakeholders consider that currently available certification and attestation schemes do not offer the continuous oversight they need over their cloud computing services. While certification or attestation typically follows a yearly cycle, these organizations require a day-to-day view of their compliance in order to offer an active response to the ever-changing cyber threat landscape.

[1] https://cloudsecurityalliance.org/star/#_overview
[2] http://www.sec-cert.eu

The EU-SEC project aims to address these shortcomings through a comprehensive set of solutions that can be adopted by requirement scheme owners, CSPs, certification bodies and audit firms in the EU and around the globe to:

- Facilitate multiparty recognition of cloud computing security and privacy compliance across regional or technical boundaries.
  Implement continuous auditing, to provide an on-going view of compliance on selected requirements.

1.1 THE NEED FOR MULTIPARTY RECOGNITION

The idea of multiparty recognition framework is not to create yet another cloud certification scheme but rather to provide the means to minimize the burden for a CSP of obtaining certification "Y", once it has already obtained certification "X". The purpose is therefore to promote co-operation between different security frameworks, standards and best practices (referred hereinafter generally as *compliance schemes*).

In our study of different compliance schemes we have observed[3] that many of the individual security requirements and control objectives appearing in different compliance schemes are, in fact, largely the same in the context of cloud computing. As a consequence, when a CSP obtains a certification or attestation under two different schemes, a lot of work is in fact duplicated, unduly increasing costs and complexity. Thus, it seems that, in many cases, the work done under one compliance scheme should be re-usable under another, allowing CSPs to focus instead on the differences between these two compliance schemes.

The EU-SEC multi-party recognition framework is meant to benefit all stakeholders in the cloud computing security and privacy compliance landscape. Firstly, it should guide cloud stakeholders in understanding the relationship between information security and privacy requirements contained in various compliance schemes such as BSI C5, CSA STAR, ISO or ISAE 3000. Secondly, it should support CSPs in selecting and adjusting their security and privacy control objectives and controls in a way that addresses several compliance schemes at the same time. Finally, it should offer certification bodies and audit firms the ability to present a more attractive compliance assessment portfolio through multiparty auditing services. Overall

[3] EU-SEC D1.2 "Security and Privacy Requirements and Controls"

a multi-party recognition framework is meant to streamline the cloud compliance process, bring efficiency, increasing assurance and reducing cost.

For illustrative purposes, consider the following scenario in which the Slovak Government wants to conclude a contract with a foreign CSP:

1. The foreign CSP holds a CSA STAR certification
2. The Slovak Government wants to understand, which of their national requirements are already covered by the CSA STAR certification.
3. The CSP can focus on describing which of the Slovak Government's control objectives are not covered by CSA STAR.

Conversely, consider a CSP seeking to attract new customers by addressing specific regional/sectorial compliance requirements:

1. The CSP holds a SOC 2 attestation on selected TSC categories.
2. The CSP wants to identify the gaps between the TSC requirements provided by the SOC 2 attestation and the (regional/sectorial) requirements of its new target customers.
3. The CSP identifies the gaps and e.g. develops controls or adjusts processes addressing the identified gaps.

The above scenarios are indicative to the contributions, benefits and future perspectives this work aims at offering to all involved parties with respect to multiparty recognition between cloud-based security certification schemes. The next sections present an approach for the definition of criteria and requirements for achieving multiparty recognition, as well as the establishment of a structured and well-governed framework for reaching the goals stated above.

1.2 THE NEED FOR A CONTINUOUS AUDITING

In a traditional "point-in-time" (or "period-of-time") compliance scheme, auditors will examine a cloud computing system during a predefined historical period leading (or not) to the issuance of a certification or attestation. While the focus in largely on the past, the audit report provides limited assurance for the future. Once the audit is finished, cloud users are left to wait until the next certification or attestation cycle, possibly a year later, to obtain assurance over the

assessed information system. For some cloud users this is not enough: it is necessary to provide renewed assurance more often in a world of rapid technology change and with a constantly evolving threat landscape. This renewed assurance would not need to be applied uniformly to the whole system, necessarily: depending on the threat landscape, some control objectives will be more critical than others and should therefore be assessed with a higher frequency ("hourly" vs. "monthly"). This in essence is the main driver for creating a continuous auditing certification framework.

One of the challenges of continuous auditing are the additional cost potentially generated by more frequent assessments. To mitigate this, we highlight the necessity of automation wherever possible, by treating security objectives more like Service Level Agreements as suggested by ISO 19086-1. The framework proposed here is designed for this approach.

As detailed in this work, we propose a three-level approach to continuous auditing-based certification:

- Level 1: Continuous self-assessment, with confirmation of the timely submission of findings to an authority.
- Level 2: An "extended" traditional point-in-time audit leading to a certification or attestation, which serves as a baseline for a continuous self-assessment, with confirmation of the timely submission of findings to an authority.
- Level 3: A continuous certification or attestation

Note here that we refer to "point-in-time" certification in a general sense, covering all frameworks that provide independent assessments of the security of cloud systems, with an audit frequency typically in the 6 to 12 months range. In particular, this means that the scope of our work encompasses both "ISO-style" certification schemes as well as "ISAE 3000 Type 2-style" attestation schemes, which are typically referred to as "over-a-period-of-time" assessments. By contrast, we refer to "continuous auditing" to cover assessments conducted with a frequency ranging from seconds up to one month.

1.3 OBJECTIVES AND SCOPE

The objective of this deliverable is to define the principles and requirements serving as the basis for the development of frameworks for the:

1. **Multiparty Recognition** of requirements contained in today's cloud security-focused, "point-in-time" compliance schemes.

2. **Continuous auditing** of cloud services pursuing reductions of compliance cost for CSPs by audit automation increasing the efficiency of audits strengthening the level of assurance from cloud users' perspective.

This deliverable provides readers with an overview of these two frameworks, presenting the core concepts of the EU-SEC project.

The targets audiences of this document are the governing bodies of certification schemes. It should also be useful to all other EU-SEC's stakeholders, notably cloud users and providers, who can understand what multi-party recognition and continuous certification can offer in order to facilitate compliance and increase assurance.

Please note that the original title of this deliverable used the terms "Continuous Monitoring" in accordance with the description of work of the EU-SEC project. We adjusted it to "Continuous Auditing" as the original terms caused confusion with some stakeholders and could hinder our efforts to communicate our work to the community. We are confident that the terminology "Continuous Monitoring" reflects the technical facts and circumstances better.

1.4 ORGANISATION OF THIS WORK

This deliverable is structured as follows:

- In section 2, we present essential principles of certification, which serve as a guiding light for defining the requirements that follow in sections 3 and 4.
- In section 3, we define requirements for multiparty recognition
- In section 4, we define requirements for continuous auditing.

The bibliographic references are listed in Appendix A. Appendix B shows the checklist for standard scheme evaluation. Appendix C contains a mapping of the requirements to the principles and the criteria for our multiparty recognition framework.

1.5 WORKPACKAGE DEPENDENCIES

The following graphic captures the main dependencies between this work and other deliverables in the project.

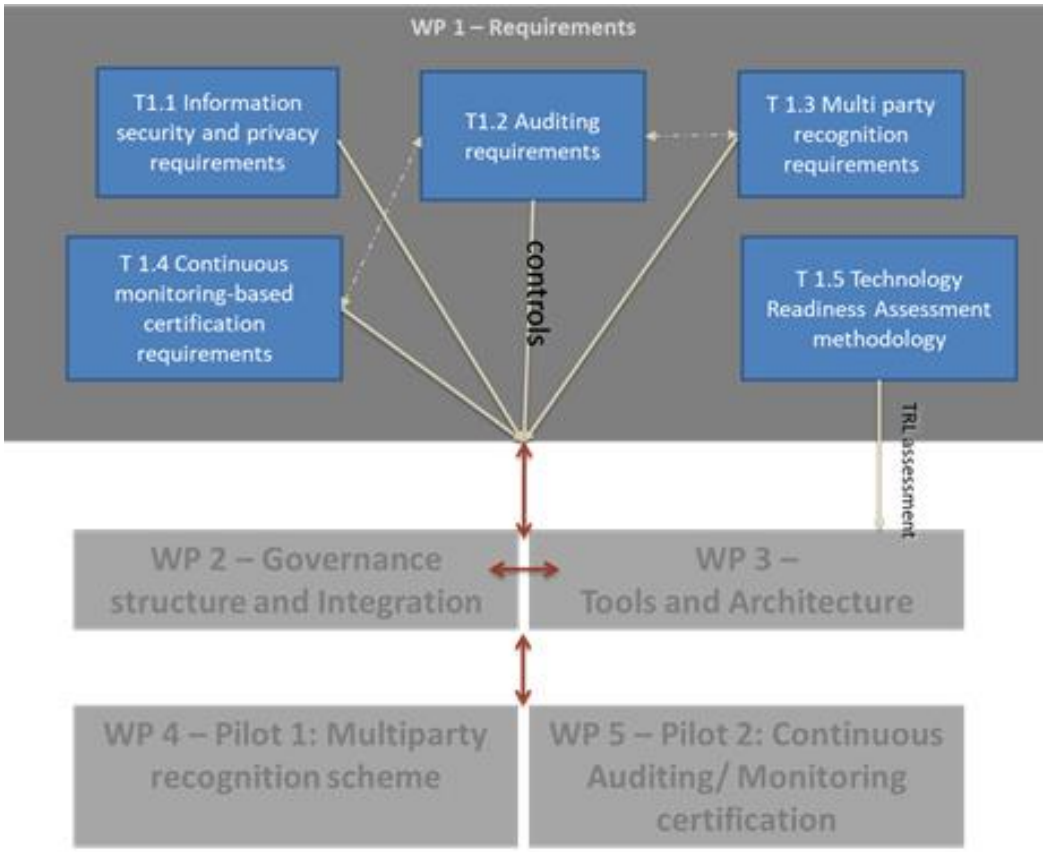

Figure 1. Work package 1 dependencies.

2 MULTI-PARTY RECOGNITION FOR SECURITY CERTIFICATION

2.1 BACKGROUND

Between 2012 and 2015, many new cloud security certification schemes have emerged. In this context, the European Union Agency for Network and Information Security (ENISA), in collaboration with the Cloud Select Industry Group (C-SIG), has produced the Cloud Certification Schemes List[4] (CCSL), which provides an overview of cloud security certification schemes applicable in the European cloud market.

A similar effort has been made by the CloudWatch Consortium, of which CSA was a member. Its published report titled "Cloud Certification Guidelines and Recommendations"[5] analyses currently available security certification schemes for cloud computing. Fifteen options have been identified, including national, regional and global, sector-specific, cloud-specific and generic certification schemes.

In the meantime both ISO 27018 and 27017 were published, driving many market players to show interest in complying with these codes of practice and already having cases of early adopters. Moreover, several countries have decided to develop their own national certification schemes, with the purpose of creating a system for the accreditation of CSPs that want to provide cloud services to their public administrations. First was the US with its Federal Risk and Authorization Management (FedRAMP) standard[6], followed by the UK's Government G-Cloud[7], then Singapore's Multi-Tier Cloud Security (MTCS). More recently the German Federal Office for Information Security[8] (BSI) and the French Network and Information Security Agency[9] (ANSSI) have developed schemes with the intention of creating a French-German Label for

[4] https://resilience.enisa.europa.eu/cloud-computing-certification
[5] http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH_Cloud_certification_guidelines_and_recommendations_March2015.pdf
[6] https://www.fedramp.gov
[7] https://www.gov.uk/government/publications/g-cloud-security-accreditation-application
[8] https://www.pwc.de/de/pressemitteilungen/2015/cloud-computing-bsi-anforderungskatalog-fuer-cloud-anbieter-angekuendigt.html
[9] https://www.ssi.gouv.fr

cloud security. Other countries including Canada, Hong Kong, Australia, Israel, Turkey and Romania are working on their own national schemes.

The aforementioned landscape for cloud security certification, clearly indicates a vast proliferation of cloud security certification schemes over the recent years. While at first sight, all these new certification schemes seem to be uniquely heterogeneous, as they are targeting wider or specific application areas (e.g., national, sectorial, regulatory domains and requirements), this might not be the case. In fact, cloud-based certification schemes are based on world-wide acceptable and widely used standards (e.g., ISO 27000 series of standards), and hence their very core security domains and requirements are rather homogeneous from a perspective of security semantics equivalency.

This work aims at highlighting and in the long-term countering the challenges and corresponding impacts that respectively arise from the proliferation of cloud-based certification schemes. In addition, by utilising certifications' common security characteristics, it will show that by terms of comparability and interoperability and under certain principles, criteria and requirements, mutual recognition between certifications can be achieved.

2.1.1 *CHALLENGES IN CURRENT CERTIFICATION LANDSCAPE*

The maturity of cloud adoption in EU countries varies quite a lot, creating a very heterogeneous environment. The European market currently includes a wide range of CSPs, from international (often headquartered outside the EU, for instance in USA or China) providers with a global footprint, to multi-region European providers, down to national providers, operating in a single region or country. In such a context, being able to compare, switch, mix and match these services requires to be able to have interoperable certification.

In this contextual landscape of CSPs and security certification requirements, the main challenges that must be tackled are to:

- Limit the proliferation of compliance schemes, while ensuring that each relevant party is able to express and enforce their cloud security and data protection requirements
- Ensure comparability and interoperability between existing certification schemes
- Provide simple tools to streamline the compliance process and reduce cost

Compliance is becoming an increasing cost for CSPs, and as a consequence of that, and increased cost for cloud users. One of reason of such an increase in costs is certainly the proliferation of the national and sectorial standards and certifications as well as the actual costs

of performing assessments and re-assessments. This becomes particularly challenging for SMEs since they might neither have the resources to comply with many different security requirements nor to pursue several different certifications. Furthermore, the costs of maintaining several certifications once obtained can become a deal breaker for many SMEs.

Moreover, from the security standpoint, the fact that several auditing teams are having access to a CSP infrastructure is a risk.

Looking at the issue from the cloud users' standpoint, it is clear that a better understanding is needed with respect to what extent a particular cloud service can be trusted and certainly that certifications and attestations are a good proxy of trust. In fact, due to their increasing number and diversity of certifications, cloud users often struggle understanding the level of assurance provided by these. Therefore, instead of creating more trust, this overabundance of certification is paradoxically leading to diminished trust due to confusion and lack of comparability.

The proposed solution to tackle the above-mentioned challenges is to defining principles, criteria and requirements for the mutual recognition between multiple certification schemes.

2.1.2 *SCOPE AND OBJECTIVES TOWARD MULTI-PARTY RECOGNITION*

The scope of this chapter on multiparty recognition framework includes the definition of a set of principles, criteria and requirements. With these, a clear direction towards comparison, analysis, mapping and finally mutual recognition between cloud security compliance schemes becomes possible. The implementation of such criteria into a well-defined mutual recognition framework is not part of this work. The mutual recognition concept is realised in task 2.1. "The multiparty recognition framework" of the EU-SEC project and documented in the homonymous deliverable D2.1.

While having in mind the fundamental elements that compose all known compliance schemes (e.g. requirements or criteria, security controls implementation and system description etc.) and rules for auditing (e.g. test procedures, evidence collection and inspection, etc.), we have set objectives. These need to be satisfied in order to make compliance schemes comparable and allow for the mutual recognition of the requirements contained within those. The objectives we have set and are targeting are:

- Definition of the principles, which serve as foundational propositions for multiparty recognition to be possible,

- Establishment of criteria, which constitute prerequisites that if satisfied in full or partial allow for multiparty recognition, and finally the,
- Identification of the requirements, which act as key elements toward mutual recognition between two compliance schemes.

The target audience of this chapter includes all interested parties with respect to cloud-based infrastructures and services certification, such as certification scheme owners/governing bodies, CSPs, cloud users and auditors of the related certification schemes. Those stakeholders are expected to obtain awareness of how to compare and assess certifications and thus on acquiring a greater understanding of the assurance provided.

2.1.3 *METHODOLOGY*

The methodology that was followed for satisfying the objectives defined in the previous section was based on a comparison analysis and identification of common characteristics found in widely established cloud-based security certifications, such as the ISO 27K series, SOC 2 and the CSA STAR certification schemes but also on EU national certification schemes (e.g., ANSSI SecNumCloud, BSI C5).

Through the analysis we have identified four (4) main stakeholders in the multiparty recognition approach:

1. Governing Body (A body responsible for governance of the Multi-party recognition framework and for maintenance of its repositories.)
2. Authorities/scheme owners (A trusted party that is responsible for the correct organization of a certification scheme, including the accreditation of auditors and keeping a registry of certified cloud services.)
3. CSPs (Cloud Service Provider)
4. Authorized auditors (An auditing organization/auditor authorized by the certification authority/scheme owner to conduct assessments against the requirements of the scheme.)

Five (5) common key certification scheme components are used as criteria for comparing security certifications:

1. Security controls and requirements
2. Audit mechanisms

3. Evidence collection and suitability
4. Auditors qualifications
5. Governance models

The foundation generated by this work enabled for hypothesis supporting the further, more detailed work: "when the above criteria are found in certain compliance schemes, then similarities will exist between them". Such a hypothesis was verified by our comparison analysis made in the content of these compliance schemes and related standards and was also strongly supported by auditors that were engaged in the project and were also interviewed.

Secondly, we defined principles serving as foundational propositions for mutual recognition. These need to be supported by the compliance schemes in scope and were leveraged from previous work, as described in the respective chapter.

Thirdly, the reference compliance scheme CSA CCM gave us the opportunity to identify the basic requirements that a scheme should contain in order to be part of the mutual recognition framework. In order to add more granularity to the required semantics (see Figure 2) we have mapped requirements to principles based on the applicable criteria.

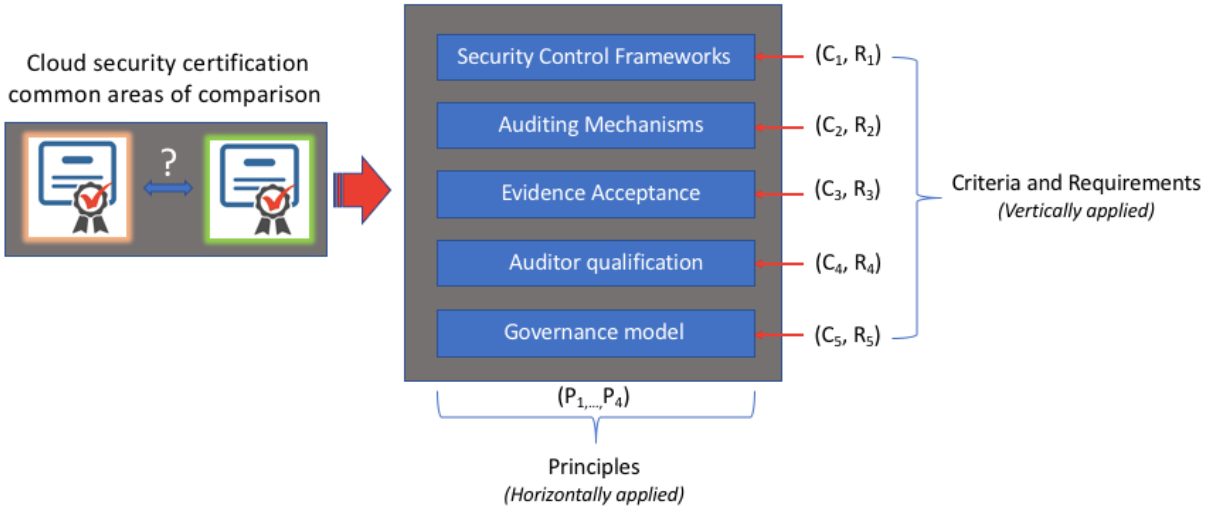

Figure 2: Diagram of principles, criteria and requirements organization for mutual recognition

2.2 DEFINING MULTI-PARTY RECOGNITION CRITERIA

Multi-party recognition criteria enable for comparing different certification schemes and serve as first filter. By applying these criteria, it becomes apparent which schemes can be compared

and might contain requirements which are candidates for mutually recognition. The criteria are:

C.1.Comparability of requirements

Comparability of requirements contained in the schemes is a key element of multi-party recognition. Only when requirements in different schemes are comparable, these can be mapped to each other and any gaps can be identified. As such, comparability of requirements is a prerequisite for their mutual recognition.

C.2.Comparability of auditing mechanisms

Test procedures executed and metrics used in an audit are comparable and are resulting in the same level of assurance / audit comfort. Audits refer to or require compliance to a named code of practice(s), as e.g. BSI C5 requires the auditor to apply the ISAE 3000.

C.3.Suitability of evidence

Due to the extreme importance of collecting evidence during audits, we are calling this out as a separate element. It includes the criteria for defining a "suitable evidence", which is an evidence that is accurate, reliable and suitable to support the audit conclusions.

C.4.Auditor qualification

Criteria for qualifying the auditor are transparent and well defined. Auditors must demonstrate knowledge of the cloud sector and be qualified to perform assessments in line with relevant auditing standards. Such criteria would include relevant formal education and personal certifications, minimum work experience, adherence to Code of Professional Ethics as well as training and continued professional education.

C.5.Governance model

Certification scheme has a transparent and a well-defined governance model with an independent standard setting body which is free of any possible conflict of interest. The governance model uses a change management process to ensure that the standard stays fit for purpose and fit for use.

2.3 PRINCIPLES

In this section we propose some core principles that seem necessary to conduct any form of assessment in order to support certification, be it point-in time or continuous. The principles are derived from prior research work (see notably [CUMULUS D2.1] and [HogbenP13]) as well as internal consultations within the EU-SEC consortium. The table below describes the four core principles both from the perspective of certification schemes and the EU-SEC multiparty recognition framework:

PRINCIPLE	CERTIFICATION SCHEME	EU-SEC FRAMEWORK
P1. The repeatability principle	If two different entities each conduct an independent audit of the same security/privacy requirements of an information system, under the same scope and conditions, then the results should be the same.	If two different entities each conduct a comparison analysis and mapping of requirements of two different certification schemes, under the same conditions, then the results should be the same.
P2. The equivalence principle	If a security/privacy requirement is assessed in two independent information systems and if the evidences collected or the measurement results are the same, then the security/privacy level provided should be equivalent in both information systems.	If a certification scheme requirement is compared with requirements of another scheme and the measurement results are the same, then the provided security/privacy level should be equivalent in both certification schemes respectively.
P3. The relevancy principle	The security/privacy requirements and the associated processes used for	NOT APPLICABLE

	assessing an information system should be selected so as to provide actionable information to the auditee.	
P4. Trustworthiness principle	The process of collecting, verifying and evaluating evidence against audit criteria should be transparent, unbiased, complete and unambiguous in order to provide a trustworthy representation of the security/privacy level provided by an information system.	The process of comparing two certification schemes should be transparent, unbiased, complete and unambiguous in order to provide trustworthy results.

Table 3 Principles for certification schemes and multiparty recognition.

2.4 REQUIREMENTS

This section describes requirements for the Multi-party recognition framework. Those requirements are linked to the above-mentioned principles and criteria. Here, we present the requirements organized by the criteria. For complete overview of requirements mapped both to principles and criteria, see Appendix C .

The requirements are formulated as "shall" and "should" clauses. "Shall" clauses are used for requirements that are required to fulfil the framework's principles and criteria. "Should" clauses are used for requirements that do not have to be necessarily implemented in the framework for its basic operation, but their implementation can enhance the framework and are desirable.

2.4.1 *COMPARABILITY OF CONTROL FRAMEWORK (R1)*

R1.1 The EU-SEC Governing Body shall perform the mapping and gap analysis of requirements of different certification schemes.

R1.2 The EU-SEC Governing Body shall determine the nature of the gaps between the requirements of different certification schemes.

R1.3 The EU-SEC Governing Body should suggest the compensating requirements to bridge the identified gaps between the requirements of different certification schemes.

R.1.4. The EU-SEC Governing Body should adopt a clear, well documented and transparent approach for performing a comparison and gap analysis between requirements of different security frameworks.

R1.5 The Authority should accept the requirements mapping, gap analysis and potential compensating requirements of the EU-SEC framework.

2.4.2 *COMPARABILITY OF AUDITING MECHANISMS (R2)*

R2.1 The Authority shall require from Authorized Auditor to use control procedures and metrics that are comparable and are resulting in the same level of assurance.

R2.2. The Authority shall require from Authorized Auditor to perform audits which refer to or require compliance to a named code of practice(s).

R2.3 The Authority shall require that the Authorized Auditor accepts to perform an audit on a scope that is considered as relevant.

2.4.3 *SUITABILITY OF EVIDENCE (R3)*

R3.1 The Authority shall require from Authorized Auditor to collect evidence that needs to be appropriate, sufficient, selective and persuasive, providing an extent of information and guidance of procedure for a reasonable audit.

R3.2 The Authority shall require from Authorized Auditor to determine the timeframe of collected evidence.

R3.3 The Authority shall require from Authorized Auditor to identify the criteria against which evidence is needed to be audited in order to secure understandability and correctness of conclusions.

R3.4 The Authority shall require from Authorized Auditor to record audit findings to enable informed decision on compliance with the requirements.

R3.5 The Authority shall require from Authorized Auditor to record nonconformities with specific requirements and contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based.

R3.6 The Authority shall require from Authorized Auditor to follow a consistent and relevant sampling approach in the collection of evidence.

2.4.4 *AUDITOR QUALIFICATION (R4)*

R4.1 The EU-SEC Governing Body shall initiate the process for mutual recognition only between certification schemes that impose clear, transparent, comparable and relevant auditor qualifications.

R4.2 The Authority shall require from Authorized Auditor to lead the auditing or assessment engagement as required by standards and schemes in the scope of the engagement.

R4.3 The Authority shall require from Authorized Auditor to have sufficient subject matter expertise and knowledge to allow professional judgement. The relevant expertise shall be supported by relevant professional certifications.

R4.4 The Authority shall require from Authorized Auditor to have sufficient number of personnel with adequate professional experience to conduct the audit or assessment engagement.

R4.5 The Authority shall require from Authorized Auditor to adhere to the Code of Professional Ethics.

2.4.5 *GOVERNANCE MODEL (R5)*

R5.1 The EU-SEC Governing Body shall allow mutual recognition only between schemes that have a well-defined, transparent and documented governance structures.

R5.2 The EU-SEC Governing Body shall allow mutual recognition only between schemes that have a governance structure that guarantee independency and prevent any possible conflict of interest.

R5.3 The governance structure of the certification scheme under comparison shall envisage mechanisms for the collection of complains.

R5.4 The governance structure of the certification scheme under comparison shall envisage internal audit mechanisms, i.e. the scheme owner should be entitled to periodically audit the certification bodies / auditing partners.

R5.5 The governance structure of the certification scheme under comparison shall clearly identify their governing body and shall define its roles and responsibilities.

R5.6 The governance structure of the certification scheme under comparison shall include a clear change management process.

R5.7 The governance structure of the certification scheme under comparison shall transparently define what the rules of participation into the governing bodies and their decision-making mechanisms are.

R5.8 EU-SEC Security Requirements Repository should be audited by accredited auditors.

R5.9 The Authority should maintain a publicly available register of Authorized Auditors

R5.10 The Authority shall maintain a register of Certified CSPs; such a registry should be preferably made publicly available.

R5.11 The EU-SEC Framework Governance Body shall maintain a repository of standards, best practices and control frameworks that are covered under the mutual recognition framework and provide reference to the specific requirements/controls in each standard.

R5.12 The Authority shall periodically audit the Authorized Auditors to maintain acceptable level of quality.

3 IMPLEMENTING THE MULTIPARTY RECOGNITION FRAMEWORK

The degree of acceptance of the multiparty party recognition framework is largely dependent on the number and relevance of the certification schemes in scope. To achieve this, it is important to involve the scheme owners into the multiparty party recognition management process. At this purpose we have defined requirements and processes that are meant to ensure a continuous and targeted involvement of scheme owners into the framework management.

A prerequisite for scheme owners for being able to be recognised as a part of the multiparty recognition framework is that they operate the multiparty recognition lifecycle and follow its precepts. The lifecycle is defined and controlled by the governance body and ensures that the certification schemes which are part of or are supposed to be included in the multiparty party recognition framework fulfil certain requirements. This will ensure that the framework will comprehend only certification schemes with an equivalent level of quality and maturity and will keep up with changes and developments of the schemes and cloud ecosystem. Ultimately the requirements and processes included in the lifecycle will guarantee transparency, consistency and manageability of the framework.

3.1 LIFECYCLE-BASED MAINTENANCE AND ENHANCEMENT

The multiparty recognition mechanism needs to evolve as the external environment in which it lives and operates changes. Hence, all of its technical contents are going through a lifecycle covering all essential requirements proposed in Chapter 2. This lifecycle provides both:

1. Transparency for external parties: e.g. scheme owners are able to assess the soundness of the multiparty recognition framework and understand how to operate within it.
2. Ensure governance effectiveness: The clear process definitions within the lifecycle ensure that the technical contents of the multiparty recognition framework are equally subjected to the framework's governance

The steps of the lifecycle provide a guidance on how to achieve and maintain a multiparty recognition. In addition, the lifecycle suggests a path for continuous improvement based on changes in the environment as well as feedback based on real life implementations of the framework.

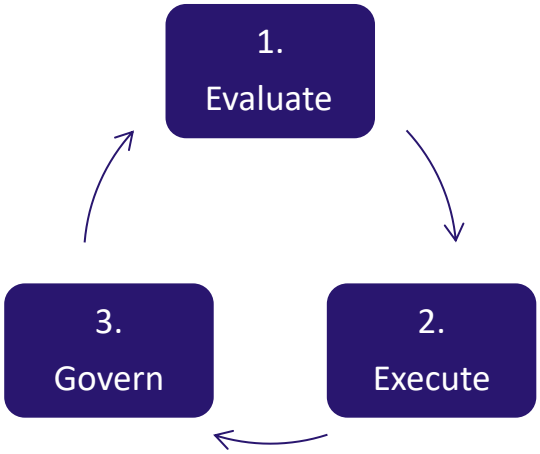

Figure 3 Process lifecycle of the multiparty recognition approach

It shall be noted that the basic process lifecycle defined in this document, will be further refined in future EU-SEC deliverables, and more specifically in D2.1, D2.4 and D2.5. At this purpose the feedback from the EU-SEC pilots will be the most relevant input.

3.1.1 *EVALUATE*

As described in Chapter 2, based on the five basic components of a generic certification scheme (see 2.1.3), the governing body sets up criteria (see 2.2) and principles (see 2.3) according to which basic requirements (see 2.4) are established.

Within this phase the scheme owner is requested to provide the necessary information in order for the governing body to evaluate if the candidate scheme meets the necessary criteria and principles to be eligible to participate in the multiparty recognition process.

If a scheme owner likes to apply for the multiparty recognition framework, the governing body assesses at high level whether the candidates' scheme includes in its structure a reference of the five basic criteria, described in 2.2 and the four core principles described in 2.3:

CRITERIA	CORE PRINCIPLE
1. Comparability of requirements	1. Repeatability
2. Comparability of audit mechanisms	2. Equivalency
3. Suitability of evidence	3. Relevancy
4. Auditor qualifications	4. Trustworthiness
5. Governance models	

If the referencing applies, it will be evaluated, whether the candidates' scheme has the potential to provide improvements to the multiparty recognition framework.
Moreover if the candidates' scheme proposes a potential innovative or complementary approach, which might lead to the revision of the multiparty recognition framework, the information is considered as input for the change management process included in the "Govern" step.

3.1.2 *EXECUTE*

Within the execution step the governing body is assuring that every certification scheme is satisfying the "shall" and "should" clauses defined in 2.4. The scheme owner is required to provide documentation for their scheme. The contained information will be assessed by the governing body (or other bodies appointed by the governing body) in order to determine whether and to what extent the certification scheme under consideration is suitable to be added to (or to be kept as part of) the multiparty recognition framework. The outcome of this assessment will be made available to the scheme owner for alignment.

To streamline the execution step, the governing body provides a guidance to assuring that the necessary requirements to allow participation into the recognition framework are met. This guidance focuses on two of the main pillars of the multiparty recognition framework, i.e. the mapping methodology (which was developed within the D1.2) and the audit criteria composition (developed within the D1.3).

Mapping Methodology

The Mapping Methodology process follows a four-step approach, which is shown in the following diagram and elaborated in more detail below.

Figure 4 Steps toward a successful mapping methodology

1) Preparation phase

Within the preparation phase, the governing body evaluates the certification schemes. The governing body examines, whether the schemes have a well-defined, transparent as well as documented governance structure, ensure independency and prevent any possible conflict of interest.

2) Mapping process

The mapping process relies on the comparability of compliance schemes, addressed in section 2.2 C.1. In order to achieve mapping and inclusion (ergo mutual recognition), the candidate's compliance scheme's requirements have to be mapped to the EU-SEC's requirements repository.

3) Gap analysis

As a further aspect targeted in 2.4.1, requirements have to be revised and existing gaps have to be recognised, defined and eventually closed. Gaps are determined between different certification and compliance schemes by the governing body and should be bridged by compensating requirements. After a review identified gaps or findings have to be timely addressed to ensure the consistency of the multiparty recognition.

4) New requirements integration

If any gaps are identified and closed, requirements need to be revised, mapped and monitored. Successfully recognised new requirements will be integrated into the EU-SEC Framework and provide further guidance into mapping existing certification schemes against new or changed ones.

Audit Criteria Composition

The aim of this step is to guide relevant stakeholder to find an approach to enable comparison and recognition between different auditing standards. Figure 6 illustrates the audit criteria composition which is described more into detail in the project deliverable D1.3.

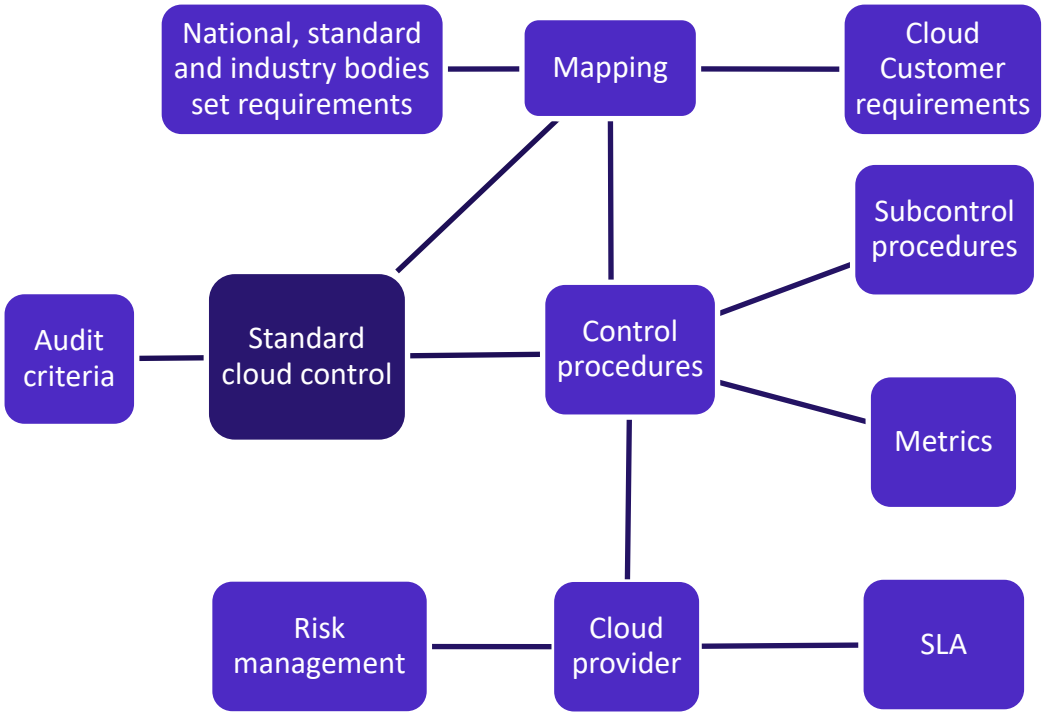

Figure 5: Simple illustration of an audit criteria composition

Additionally, in the execution step, the governing body takes care of the collection of change requests, such as modified requirements or the need to include new requirements to monitor and bridge potential gaps.

3.1.3 *GOVERN*

An essential element of continuous improvement is the permanent monitoring and updating of procedures. With respect to new developments, the governing body needs to inform or be informed about recent changes, the scheme owner needs to restart the evaluation process and auditors/auditees need to comply with their task to support the primary actors. Whenever crucial changes are implemented, event handling measures are triggered.

The scheme owners need to ensure that their certification schemes address the stakeholder's needs and are embedded into and connected with the legal as well as the regulatory landscape. Hence, the scheme owner is required to implement measures which are eligible to safeguard this. For example, the scheme owner needs to review their scheme on a regular basis according to defined requirements as well as processes and update them accordingly, if required.

All these points mentioned in the previous sections are necessary considerations to be able to react appropriately to emerging changes and to be able to incorporate them into the lifecycle model promptly and regularly.

To ensure that the multiparty recognition framework reflects the current state of the cloud certifications and standards, a governance framework shall be implemented. The governance framework also provides guidance on the suitability of evidence and auditors qualifications. The governance framework is introduced in the Deliverable 2.4.

3.2 RESPONSIBILIES OF STAKEHOLDERS

The criteria, principles and requirements described in Chapter 2 affects, in different ways, all the four (4) main stakeholders in the multiparty recognition framework defined in 2.1.3.

We divided the stakeholders in two categories, on the one hand operating, on the other hand informed parties. The following diagram shows the roles of the stakeholders.

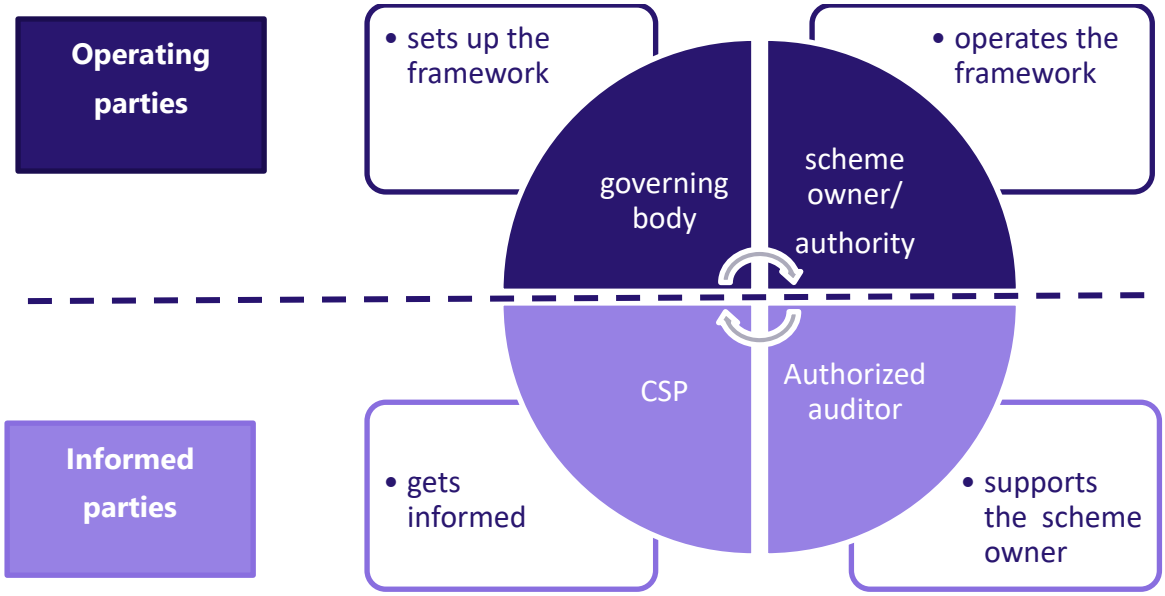

Figure 6 Roles of the stakeholders in the multiparty recognition framework

The operating parties, consisting of the governing body and the scheme owners are the primary stakeholders. With the objective to establish and maintain the multiparty recognition framework, the scheme owner is advised to communicate and address updates, changes and terminations to the auditor/auditee. The informed parties, consisting of the Authorized Auditor and CSP are supporting the process, e.g. Auditors are meant to satisfy the requirements that are imposed by the scheme owners.

The main focus area of the multiparty recognition framework's operations needs to be the inclusion of further certification schemes and their owners. The multiparty recognition framework's operation is actively driven by the operating parties and supported by informed parties.

Both, the operating and the informed parties are active in two streams. The first stream is about informing stakeholders about recent changes to the framework, laws and regulations. The second stream describes required actions to be performed by the specific stakeholder.

	PRIMARY ACTOR	RESPONSIBILITES	
		Information Stream	Activity Stream
Operating parties	Governance Body	→ Inform stakeholders about recent changes	→ Define criteria, principles and requirements. → Evaluate schemes. → Execute the multiparty recognition framework → Evaluate possible effects → Update the framework according to changes in laws, regulations etc.
	Scheme owner/Authority	→ Inform Authorized auditor and CSP about scheme requirements	→ Comply with criteria, principles and requirements → Align with multiparty recognition lifecycle → Govern and guard ability for comparability and interoperability
Informed Parties	Authorized auditor	→ Inform candidates auditee (CSPs) about recent updates	→ Comply with criteria, principles and requirements, in addition to law and regulations of authorities. → Support multiparty recognition by analysing circumstances and

				identifying missing requirements
	CSP	→	Provide auditable information	→ Adjust the internal control framework to meet new requirements

Additional details about the multiparty recognition framework stakeholders and their roles and responsibilities will be provided in the Deliverable 2.1.

4 CONTINUOUS AUDIT-BASED CERTIFICATION

4.1 BACKGROUND

While traditional "point-in-time" and "over a period of time" security and privacy certifications are quite well established, continuous auditing-based certification is still a novelty. As a consequence, it is necessary to step back and review the definitions and concepts that can be adopted for continuous auditing before we can discuss relevant requirements.

The definitions and concepts we present in this introduction were derived from existing standards whenever possible, in particular ISO/IEC 19086, which defines the notions of "SQO" and "SLO". The full rational for these definitions is presented hereafter in the remainder of this section. All the definitions we examine in this section are also collected for reference in the *terminology and definitions* section found at the beginning of this document.

4.1.1 *CONTINUOUS AUDITING*

In traditional compliance lingo, "continuous auditing" describes the evaluation of control implementation by internal auditors while "continuous monitoring" is used to describe the continuous feedback provided to management regarding key processes. While these two concepts overlap, they target clearly different stakeholders in an organization.

In the field of information security management, continuous monitoring is defined as "*as maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions*." [NIST SP800-137].

To make matters more complex, in some cases the terms "continuous monitoring" and "continuous auditing" have been used interchangeably: this is notably the case in the Description of Work that supports the EU-SEC project. Since the EU-SEC project is unambiguously about continuous certification, we have decided to drop the term "continuous monitoring" in favour of "continuous auditing", which we define as follows:

> **Continuous Auditing:** An on-going audit process that aims to assess Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.

The terms Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs) come from [ISO 19086-1] and broadly mean "security and privacy objectives" here. The precise meaning of these terms is described in the following subsection.

Following the definition of Continuous Auditing, we further specify the following terms:

> **Audit**: The systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (SOURCE: ISO19011:2011, 3.1).
>
> **Audit criteria: S**et of policies, procedures or requirements used as a reference against which audit evidence is compared (SOURCE: ISO19011:2011, 3.2).
>
> Note**:** *Policies, procedures and requirements* include any relevant SLOs or SQOs.
>
> **Audit evidence: R**ecords, statements of fact or other information which are relevant to the **audit criteria** and verifiable (SOURCE: ISO 9000:2005, definition 3.9.4)
>
> Note: Audit evidence can be qualitative or quantitative.

4.1.2 *AUTOMATED VS NON-AUTOMATED*

In order to conduct an "on-going" audit process, evidence must be collected and assessed with a frequency that will be expressed in minutes, hours, days or months.

The on-going nature of this auditing process poses several challenges, both from technical and economic point of view.

An organisation may be willing to pay for an audit once a year but might find it disproportionally expensive to maintain this cost on a permanent basis. A solution to this is automation: we should try whenever possible to use tools and automated processes that will evaluate audit criteria automatically, without human intervention (except for initial setup costs). Unfortunately, a fully automated audit is currently an unattainable goal. Current audit frameworks do not lend themselves to automation and we need to consider what can be automated and what still requires human intervention.

In traditional certification, compliance is described with reference to a set of requirements or control objectives: either there is a control able to satisfy a certain minimum requirement/objective or not. Some schemes may also rate the "maturity" of the control

implementation, as done in CSA STAR Certification[10]. The principle remains the same: compliance is expressed as a qualitative objective that is often described with a certain level of abstraction, which requires assessment by a human (e.g. "*business continuity plans shall be documented and tested regularly*").

Does this apply to continuous auditing as we defined it above?

As detailed hereafter, there are two approaches to answer this question:

1. The first approach is to consider that indeed, continuous auditing must apply to a set of controls, as in traditional "point-in-time" certification, often at the expense of possibilities for automation.
2. The second approach is to consider that continuous auditing is better suited to lower level "service attributes" that can be more easily automatically evaluated.

"Continuous auditing", as defined above, is still a relatively new topic. As a consequence, it is not yet framed in a widely recognized standard or set of best practices. However, there are some standardization developments in another very closely related domain: Cloud Service Level Agreements (SLAs) as embodied in the recent ISO/IEC 19086 standard suite[11] titled "Cloud Computing – Service Level Agreement (SLA) Framework" [ISO 19086-1]. SLAs describe an agreement between a cloud service provider and a cloud service customer about the expected quantitative and qualitative characteristics of a service. Typically, when the agreement is not satisfied, the provider compensates the customer in one form of another. In turn, this requires the terms of the SLA to be continuously monitored to determine if the agreement is satisfied or not. As such, the conceptual model introduced in ISO/IEC 19086 is relevant here and we aim to re-use it whenever applicable.

4.1.2.1 NON AUTOMATED CONTINUOUS AUDITING

Control objectives are often expressed in an abstract form, with a lot of room for interpretation or context dependency. They contain elements that are impossible to evaluate by automated means without human intervention.

To illustrate this case consider the following simplified control objective: "*business continuity plans shall be documented and tested regularly*". Should we want to fully automate the verification of this control objective, this would immediately raise the following questions:

[10] https://cloudsecurityalliance.org/star/certification/#_overview
[11] ISO/IEC 19086 is a standard that is published in several parts.

- How can an automated process verify that business continuity plans are documented?
- Even if the auditing process knows where the document is, how can it know if the document describes a business continuity plan and not a cake recipe?
- The words "tested regularly" are largely context dependent. We can however verify that some testing has been done once the test is readily specified.

In the future, Advances in Artificial Intelligence and natural language processing techniques might open the door to solutions that answer some of the questions above. Even if these novel solutions are imperfect, they might still appreciably reduce human intervention, which would simply be limited to the validation of machine-generated assertions as opposed to conducting the full assessment themselves. In practice today, this technology is not yet available.

Control objectives are usually translated into a set of controls (i.e. measures mitigating risks), which are more concrete than the control objectives they stem from. Yet, more often than not, they still contain abstractions, context dependencies and other elements that require human intervention.

As a consequence, 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". This can be considered as a subset of what ISO/IEC 19086-1 defines a Service Qualitative Objective (SQO): the *"commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale."*

Given the nature of current cloud certification landscape, based on standards such as ISO 27001, SOC 2 or CSA STAR, it seems inevitable that some aspects of continuous auditing will require human intervention.

4.1.2.2 AUTOMATED CONTINUOUS AUDTING

Another school of thought is to consider that traditional security or privacy controls do not lend themselves to continuous auditing and need to be expressed in a different form that better lends itself to automation.

The alternative is to break down the control into a set of security or privacy attributes of the service that can be evaluated quantitatively and automatically audited (e.g. availability is

evaluated between 0 and 100%). An audit criterion is typically defined with reference to a specific threshold, which defines an objective (e.g. availability must be greater than 99.5%).

This can be considered as equivalent to what ISO/IEC 19086-1 defines a Service Level Objective (SLO): "the *commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale*". More rarely, automated tools may provide results on a qualitative scale, and the use of SQOs we presented in the previous sub-section is valid here as well.

In our example which states that "*business continuity plans shall be documented and tested regularly*", we could define the following "auditable" attributes:

- Number of backup restoration tests performed in the past period (e.g. a month).
- Number of backup restoration failures in the past period.
- Maximum recovery time.
- Recovery point actual.
- …

These attributes can then be used to define corresponding SLOs, respectively:

- The minimum number of restoration tests performed in a period (e.g. a month).
- The maximum number of backup restoration failures in a period.
- The RTO (Recovery Time Objective).
- The RPO (Recovery Point Actual).
- …

The mapping between a control and a set of automatable "SLOs" is almost always incomplete. In our example above, we were not able to define an attribute that measures the fact that business continuity plans have been "documented". Compliance assessment might therefore be based on a hybrid approach:

- A less frequent (or point in time) assessment of some SQOs (e.g. "business continuity documentation").
- A frequent and automated assessment of SLOs (e.g. RTO).

In order to discuss SLOs, the NIST has shown [NIST 500-307] that is useful to define more formally three additional concepts[12]: Measurement, Measurement result and Metrics.

- **Measurement**: Set of operations having the object of determining a Measurement

[12] These definition can also be found in the *terminology and definitions* section found at the beginning of this document

Result. (from [NIST 500-307])

- **Measurement Result**: Value that expresses a qualitative or quantitative assessment of an attribute of an entity. (from [NIST 500-307])
- **Metric:** Standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement. (from ISO/IEC 19086, borrowed from [NIST 500-307]).

As illustrated on Figure 7 unterhalb, when continuous auditing targets an SLO, the following processes take place:

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

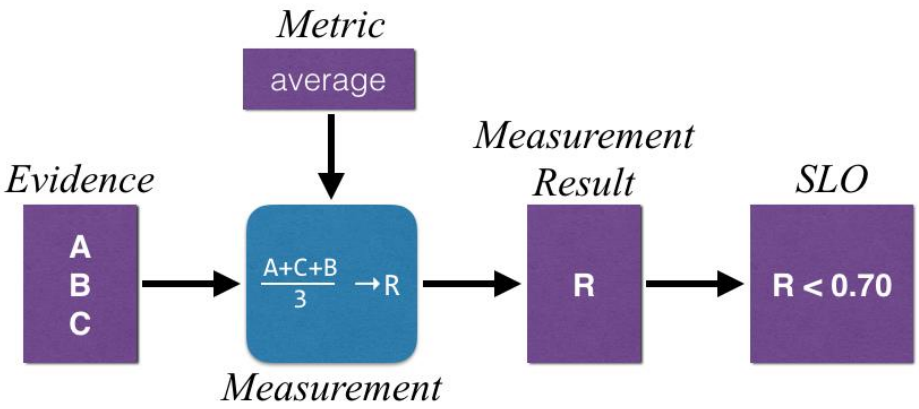

Figure 7. Evaluation of an SLO

4.1.3 *CONTINUOUS AUDIT-BASED CERTIFICATION*

As we have now defined the key concepts related to continuous certification, i.e. continuous auditing, SLOs, SQOs, measurements and metrics, we can finalize this section by defining "continuous audit-based certification" itself:

> **Continuous audit-based certification**: 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.

Given the on-going nature of continuous auditing, an information system may temporarily fail to report that it meets an SLO or SQO at the expected frequency, just like a cloud service provider may temporary fail to match the terms of its SLA. We will say that such an information system is in a state of "suspended certification".

> **Suspended (audit-based) certification**: The production of a statement indicating a failure to report at the expected frequency that an information system meets a predefined SQO and/or SLO.

A governing body or authority will be responsible for the process of producing or suspending certifications, either acting directly or through an accredited intermediate body, as detailed in the certification governance rules presented in the EU-SEC project Work Package 2.

4.2 CONTINUOUS AUDIT-BASED CERTIFICATION ARCHITECTURES

From a high-level perspective, continuous certification can be broken down in 4 phases:

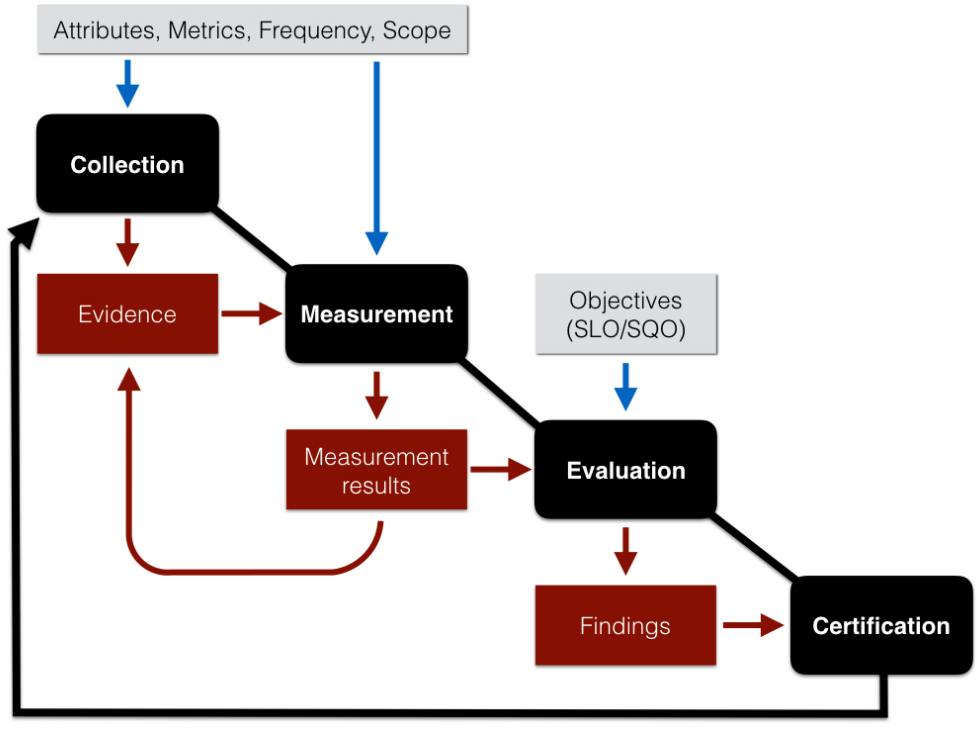

Figure 8: continuous certification process

The **collection phase** describes the collection of data from information systems by auditing tools and humans. Such tools can collect from a wide range of data sources, such as:

- Network and system process statistics,
- Service API success, errors, and response times,
- System logs,
- Process statistics (e.g. backups, migrations)
- Incident related events (e.g. start, end and notifications),
- Documentation,
- Etc.

The data collected will be strongly influenced by the **certification target:** the list of SLOs and SQOs that the information system is assessed against. Some or all of the data collected shall be saved and used later as digital evidence.

The **measurement phase** describes the processing of evidence in order to produce measurement results, which represents a qualitative or quantitative assessment of a security or privacy attributes of an information system. The way a measurement is conducted and how its results are interpreted is typically defined through a metric.

The measurement phase may involve several iterations of measurements: the measurement results obtained as the output of a first measurement become the input of another second measurement producing new more refined measurement results. As a consequence, there may exist some "intermediary" measurement results that can be considered as evidence in their own good, as shown by the arrow on the diagram above.

Measurement results can be specific to a customer (e.g. the availability of the customer's instances) or general (e.g. global backup restoration failure statistics.

The **evaluation phase** describes the evaluation of SLOs and SQOs in regards with the previously obtained measurement results, producing a set of findings describing whether or not the objectives are met. In this context an SLO or an SQO can be seen as "audit criteria" against which we assess.

The **certification phase** describes the publication of a statement confirming or not that an information system fulfils a set of predefined objectives, as verified by an independent party.

The certification phase therefore evaluates whether an information system is in the state of continuous certification or suspended certification.

4.2.1 *APPROACH 1: CONTINUOUS SELF-ASSESSMENT.*

A self-assessment approach involves only two actors:

- An auditee, a CSP that wants to perform continuous audit-based certification.
- An authority or governing body, which keeps track of the timely submission of self-assessments by the CSP.

The CSP collects service data using its own monitoring tools and personnel, makes assessments of security or privacy SLOs/SQOs and produces the results.

- The first 3 phases (collection, measurement and evaluation) are performed by the CSP.
- The certification phase (4th phase) is conducted under the responsibility of the governing body but is limited to the verification that the findings were submitted in a timely manner.
- No elements of the collection, measurement or evaluation (tools and processes) are reviewed by an external auditor.

The governing body maintains a public registry of certified cloud services, which can be consulted freely by cloud customers.

This approach is the simplest but puts al trust in the CSP.

4.2.2 *APPROACH 2: EXTENDED CERTIFICATION WITH CONTINUOUS SELF-ASSESSMENT*

An extended certification with continuous self-assessment involves three actors:

- An auditee, a CSP that wants to perform continuous audit-based certification.
- An external auditor, which performs a point in-time certification.
- An authority or governing body, which keeps track of the timely submission of self-assessments by the CSP, as well as point-in time certifications awarded.

The CSP performs a traditional (non-continuous) certification, followed by a continuous self-assessment. The assessment activities of this traditional certification are extended to include the verification that the tools and processes that will be later used in the self-assessment are "fit for purpose".

During the continuous assessment, the CSP collects data from the tools and makes assessments of security or privacy levels and produces results:

- The tools and processes involved in the first 3 phases (collection, measurement and evaluation) have been audited by an external auditor at a point in time, for compliance to a set of continuous auditing standards or rules.
- The execution of the first 3 phases remains under the control of the CSP.
- The certification phase (4th phase) is conducted under the responsibility of the governing body but is limited to the verification that the findings were submitted in a timely manner.

The governing body maintains a public registry of certified cloud services, which can be consulted freely by cloud customers.

This approach is still relatively simple, but provides a higher level of assurance compared to a full self-assessment.

4.2.3 *APPROACH 3: CONTINUOUS CERTIFICATION*

Continuous certification involves three actors:

- An auditee, a CSP that wants to perform continuous audit-based certification.
- An external auditor, which performs a point in-time certification as well as a continuous audit-based certification.
- An authority or governing body, which keeps track of the timely submission of self-assessments by the CSP, as well as point-in time certifications awarded.

The CSP performs a traditional (non-continuous) certification, followed by a continuous self-assessment. The CSP uses auditing tools and processes that have been "vetted" by an external auditor, and continuously provides measurement results to the governing body. Evaluation results are stored on a platform that is independent from the CSP.

- The tools and processes involved in the first 2 phases (collection and measurement) have been audited by an external auditor as part of a point in time certification, for compliance to a set of monitoring standards or rules.
- An external auditor performs the evaluation (3rd phase), based on measurement results provided by the CSP.
- Results may be collected and stored by the external auditor outside of the CSP's infrastructure.
- The certification phase (4th phase) is conducted under the responsibility of the governing body and includes verification that the findings meet the predefined objectives and that they were submitted in a timely manner.

The governing body maintains a public registry of certified cloud services, which can be consulted freely by cloud customers.

This approach is the most complex, but provides the highest level of assurance.

4.3 CONTINUOUS CERTIFICATION PRINCIPLES AND REQUIREMENTS

4.3.1 *BASE PRINCIPLES*

Before stepping into specific requirements for continuous certification, we propose to recall and adapt the principles defined in section 2 to the context of continuous monitoring as follows:

- **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.

While the repeatability principle is not too difficult to apply, the two next principles are more challenging to implement in the context of continuous certification. For example, it's easy to show that all IaaS providers evaluate the attribute "availability" in a different way [HogbenP13], massively falling short of any form of equivalence. Similarly, expressing attributes as averages (e.g. "average incident response time") without additional information is typically of low relevancy, since it tends to hide critical issues.

The trustworthiness principle is key to certification: if the audit process is not trusted, impartial or largely free of significant interference by the auditee, then the resulting certificate will have lower value. In traditional certification, trustworthiness is achieved by a combination of mechanisms, notably the use of independent auditors that are formally accredited by an

independent authority, and the use of formally defined processes. Trustworthiness also needs to apply to continuous certification.

4.3.2 *CONTINUOUS AUDITING-BASED CERTIFICATION BASE REQUIREMENTS*

As detailed in section 1, *continuous certification* relies on *continuous auditing* which itself *aims to assess Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit*. While the evaluation of automatable and non-automatable objectives will each entail a distinct set of requirements, this section will explore common ground requirements that underpin continuous auditing-based certification, both taking into account the 4 principles above and the continuous nature of this new form of certification.

Base continuous auditing-based certification requirements:

R-1.1. An information system SHALL only be certified if meets a certification target defined as a set of SLOs and/or SQOs, each verified at a predefined frequency through a continuous auditing process. Conversely, a failure to meet an SLO and/or SQO or a failure to verify it within the predefined frequency SHALL prevent an information system from being certified.

Note: The certification target is specific to the information system under scrutiny.

R-1.2. Processes and procedures used for continuous auditing SHALL be designed to be as fully automated as possible, so as to eliminate or reduce human intervention.

R-1.3. The evaluation of an SLO or SQO SHALL be conducted at a predetermined interval. This interval SHOULD be chosen to reconcile the relevancy principle and feasibility, and SHOULD be standardized across all audits.

Note: While the set of applicable SLO/SQO is specific to each information system, the applicable frequencies of evaluation should be standardized so as to avoid discrepancies across audited information systems.

R-1.4. Controls MUST be implemented so as to assure that the collection and evaluation of audit evidence is trustworthy.

R-1.5. Any SLO or SQO used in a continuous audit-based certification scheme SHALL be mapped to an existing control framework, either directly or through the definition of audit criteria that are used to compute SLO/SQO.

Note: It is expected that continuous certification will rely on both SLOs and SQOs.

R-1.6. Sufficient evidence SHALL be collected and assessed in order to reliably support compliance findings.

R-1.7. Sufficient evidence SHALL be collected and stored in order to enable independent re-assessments or validations, notably to address any dispute regarding the validity of findings.

R-1.8. The integrity of the tools/application collecting and storing evidence SHALL be protected by appropriate measures, such as:

- prior certification: the deployment of third party-tools that have been verified to satisfactorily implement relevant process, metrics and security measures,
- independent audit: independent review of source code and processes by a trusted party.
- cryptographic checks: the use of software or hardware (TPM) cryptographic checks of tools to assure that they have not been altered.

Note: The exact measures should be chosen in relation with the target certification model and assurance level required.

R-1.9. Appropriate measures SHALL protect evidence and findings against modification or destruction once they have been collected, except when such elements are no longer needed (see R-1.12).

R-1.10. Note: The exact measures will be chosen in relation with the target certification model and assurance level required. It is generally not possible to provide an absolute guarantee that data will not be altered in an information system. In addition to R-1.9, we therefore introduce the following additional requirement to ensure at least the detection of alterations.

R-1.11. Appropriate measures SHALL ensure the detection of any modification or destruction of evidence and findings after collection.

Note: The exact measures will be chosen in relation with the target certification model and assurance level required.

R-1.12. Appropriate measures SHALL ensure that only authorized parties have (read-only) access to evidence or findings.

Note: The exact measures will be chosen in relation with the target certification model and assurance level required.

R-1.13. Evidence SHALL be stored for as long as needed for the potential verification of findings, as specified in contractual terms and relevant legislation where applicable.

4.3.3 *AUTOMATABLE AUDITING REQUIREMENTS*

This sub-section addresses the specifics of automatable continuous auditing.

Automatable auditing requirements:

R-2.1. Metrics SHALL be specified in an unambiguous way, so as to assure the greatest possible uniformity in the implementation of measurements across systems of various vendors and technologies.

A metric definition SHALL at least include:

- The security/privacy attribute(s) it applies to.
- A definition of the evidence needed to conduct an assessment of the attribute.
- A description of the possible ways in which relevant evidence must be collected.
- A specification of the measurement method, as a process that takes as input evidence and produces as output a measurement result.
- The period over which the measurement is conducted (e.g. a minute, a week, a month).
- The required format and applicable units of the measurement result.

R-2.2. The specification or a measurement method as part of a metric SHOULD be formulated to be applicable to the broadest possible range of information systems and vendors.

R-2.3. A metric definition SHOULD include guidance on the interpretation of measurement results and objectives.

R-2.4. The definition of an SLO/SQO SHALL reference the metric that is used for the assessment of any applicable attribute.

Note: Since an SLO or SQO is expressed as a commitment regarding an attribute of an information system it is not possible to evaluate an SLO/SQO without knowing the metric that is used to assess the corresponding attribute.

R-2.5. Findings, SLOs, SQOs and measurement results SHALL be expressible in a machine-readable format for the purpose of automation and interoperability.

R-2.6. Metrics SHALL be designed to have the following properties. Given a security (or privacy) attribute A that is evaluated on 2 distinct information systems S1 and S2, producing two corresponding measurement results R1 and R2, then:

- If R1=R2, the level of security of S1 and S2 SHALL be considered as equivalent for A.
- If R1<R2, the level of security of S1 SHALL be considered as lower as the level of security of S2 for A.
- If R1>R2, the level of security of S1 SHALL be considered as higher as the level of security of S2 for A.

Note: (b) and (c) only apply in cases where measurement results are in an ordered set.

R-2.7. Metrics SHALL be designed to maximize relevancy for the stakeholders that rely on certification for assurance.

This notably means that metrics SHOULD:

- Avoid expressing an "average" or a "mean", which alone hides information.
- Prefer maximums or minimums.
- Prefer totals to percentages.

R-2.8. The integrity of the automated tools assessing evidence and producing findings about an information system SHALL be protected in similar terms to the ones defined in R-1.8.

4.3.4 *NON-AUTOMATABLE AUDITING REQUIREMENTS*

This sub-section addresses the specifics of non-automatable continuous auditing.

Non-automatable auditing requirements:

R-3.1. In the context of non-automatable continuous auditing SLOs/SQOs SHALL be associated with an "evaluation policy".

R-3.2. An evaluation policy SHALL specify:

- A reference to the control or property that the SQO/SLO expresses.
- A maximum evaluation interval: failure to re-evaluate an SQO/SLO within the maximum interval will result in the SQO/SLO to be considered as failed.

R-3.3. An evaluation policy MAY specify:

- Additional criteria for the evaluation of the SQO/SLO if necessary to clarify the underlying control or property that the SQO/SLO expresses, in a specific context.
- A recommended evaluation interval: this interval is used as a best-practice indication.

R-3.4. Controls which must be audited by a human auditor SHALL be marked as such in the control set / controls repository used for the audit

R-3.5. Results of a non-automatable audit SHALL be consolidated and integrated with results of the automated audit allowing a human auditor to derive an overall audit result which is fed into the certification process, subsequently

R-3.6. Principles applicable to the profession SHALL apply, such as Documentation Requirements, Ethic Requirements and Professional Scepticism or Professional Judgment.

Note: Refer for example to corresponding sections in ISAE 3000.

R-3.7. The audit and the audit results, especially SHOULD be documented in a standardised way to maximise efficiency and enable for timely further use of gained information

5 CONCLUSIONS AND RECOMMENDATIONS

The multiparty recognition requirements proposed in this document were defined following a two steps approach; first we identified key certification scheme components and then we built criteria for comparing security certifications. As a part of the second step we defined high-level principles, which are applied to the certification scheme components and criteria. On these basis, we were able to identify the requirements that a scheme should fulfil in order to achieve the necessary level of quality, robustness and thoroughness and consequently be part of a mutual recognition framework suitable for the European market.

The proposed criteria, principles, and requirements we identified are the building blocks of the EU-SEC multiparty recognition framework; we believe those can be acceptable by authorities/scheme owners and help Cloud Service Providers and Cloud Users and will improve the effectiveness and efficiency of the cloud market and more in general of the ICT market as whole, through a set of harmonised rules for bridging the gap between the plethora of existing certification schemes.

We suggest a process lifecycle of the multiparty recognition approach to ensure the multiparty recognition framework reflects the up-to-date security certifications and standards as it is necessary to appropriately react to dynamic security certification landscape and changes of requirements.

We recommend five criteria, four core principles, and total of 31 requirements for mutual recognition between different third-party-audit-based certification schemes. Furthermore, we recommend that the EU-SEC governance framework builds on the process lifecycle defined in this document to ensure the long term sustainability and exploitability of the EU-SEC framework after the finalisation of the project.

Moreover, this document laid out the foundations for a continuous auditing-based certification framework.

Firstly, we provided a set of definitions, that building on existing literature on continuous monitoring, security parameters and service levels, defines some key concepts for the creation of a continuous-auditing-based certification.

Secondly, we highlighted 3 certifications models ranging from a continuous self-assessment to a full continuous certification. Each model is based on different certification policies and a variable level of involvement of third parties and of automatic controls verification. The key

common denominators are the need to establish viable way to operationalise security controls and the need to verify and report the audit results in a timely manner.

Finally, we provided a list of requirements for the creation of a continuous auditing-based certification framework. These requirements are designed to be applicable to existing certification schemes, enabling them to be extended to build a continuous certification offering. Ideally, we would like continuous auditing to be fully automated, thereby reducing costs and increasing the potential frequency of assessment. In practice, we acknowledge that is not realistic given the state of the art in certification today. As a consequence, our requirements take both into consideration automated and non-automated continuous auditing processes, which together will form the basis of a continuous certification.

EU-SEC aims to pioneer the creation of the very first continuous auditing-based certification framework. As consequence, the issue of mutual recognition does not apply today to continuous certification. Nevertheless, the requirements we defined for mutual recognition can be applied to continuous certification as well, should we see the emergence of a plethora of continuous certification schemes in the future.

APPENDIX A BIBLIOGRAPHY

Androcec, D., Vrcek, N., & Seva, J. (2012). Cloud Computing Ontologies: A Systematic Review. In *MOPAS 2012 : The Third International Conference on Models and Ontology-based Design of Protocols, Architectures and Services Cloud* (pp. 9–14). IARIA. Retrieved from https://pdfs.semanticscholar.org/cd5f/e6edb6284fcbcb470239464bb0c8e3ee2d50.pdf

CSA. (2016). Cloud Controls Matrix Working Group. Retrieved September 26, 2017, from https://cloudsecurityalliance.org/group/cloud-controls-matrix

European Parliament. General Data Protection Regulation, Pub. L. No. 2016/679, 88 (2016). Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

European Parliament. The Directive on Security of Network and Information Systems, Pub. L. No. 2016/1148, 30 (2016). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Garcia, J. M., Fernandez, P., Pedrinaci, C., Resinas, M., Cardoso, J., & Ruiz-Cortes, A. (2017). Modeling Service Level Agreements with Linked USDL Agreement. *IEEE Transactions on Services Computing*, *10*(1), 52–65. https://doi.org/10.1109/TSC.2016.2593925

Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 11. https://doi.org/10.1186/2192-113X-1-11

Grant Agreement Number 731845 - EU-SEC. (2016). European Commission.

Hooi, Y. K., Hassan, M. F., & Shariff, A. M. (2014). A Survey on Ontology Mapping Techniques. In H. Y. Jeong, M. S. Obaidat, N. Y. Yen, & J. J. Park (Eds.), *Advances in Computer Science and its Applications* (Vol. 279, pp. 829–836). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-41674-3

Pedrinaci, C., Cardoso, J., & Leidig, T. (2014). Linked USDL: A Vocabulary for Web-scale Service Trading. In V. Presutti, C. d'Amato, F. Gandon, M. d'Aquin, S. Staab, & A. Tordai (Eds.), *11th Extended Semantic Web Conference (ESWC 2014)* (pp. 68–82). Cham: Springer. https://doi.org/10.1007/978-3-319-07443-6_6

Singh, V., & Pandey, S. K. (2014). A Comparative Study of Cloud Security Ontologies. In *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization* (pp. 1–6). IEEE. https://doi.org/10.1109/ICRITO.2014.7014763

Takahashi, T., Kadobayashi, Y., & Fujiwara, H. (2010). Ontological approach toward cybersecurity in cloud computing. In *Proceedings of the 3rd international conference on Security of information and networks - SIN '10* (pp. 100–109). New York, New York, USA:

ACM Press. https://doi.org/10.1145/1854099.1854121

Veloudis, S., & Paraskakis, I. (2016). Ontological Templates for Modelling Security Policies in Cloud Environments. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics - PCI '16* (pp. 1–6). New York, New York, USA: ACM Press. https://doi.org/10.1145/3003733.3003796

Wong, W., Liu, W., & Bennamoun, M. (2011). Ontology Learning from Text: A Look back and into the Future. *ACM Computing Surveys*, *44*(4), 36.

Zhang, M., Ranjan, R., Haller, A., Dimitrios, G., Menzel, M., & Nepal, S. (2012). An ontology-based system for Cloud infrastructure services' discovery. In *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (Vol. 7714, pp. 524–530). Pittsburgh, PA, USA: IEEE. Retrieved from http://ieeexplore.ieee.org/document/6450944/

Zhu, J. (2012). Survey on Ontology Mapping. *Physics Procedia*, *24*, 1857–1862. https://doi.org/10.1016/j.phpro.2012.02.273

[CSA-2016] Daniele Catteddu, Alain Pannetrat, Jim Reavis „CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND", Whitepaper, Cloud Secuirty Alliance. https://downloads.cloudsecurityalliance.org/star/csa-star-program-cert-prep.pdf

[NIST SP800-137] Kelley Dempsey Nirali Shah Chawla Arnold Johnson Ronald Johnston Alicia Clay Jones Angela Orebaugh Matthew Scholl Kevin Stine, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", NIST Special Publication 800-137.

[HogbenP13] Giles Hogben, Alain Pannetrat, "Mutant Apples: A Critical Examination of Cloud SLA Availability Definitions." IEEE 5th International Conference on Cloud Computing Technology and Science, CloudCom 2013, Bristol, United Kingdom, December 2-5, 2013, Volume 1.

[NIST 500-307] NIST Cloud Computing Reference Architecture and Taxonomy Working Group, "Cloud Computing Service Metrics Description", DRAFT NIST Special Publication 500-307.

[ISO 19086-1] ISO/IEC JTC 1/SC 38, "ISO/IEC 19086-1:2016, Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts", International Organization for Standardization, September 2016.

[CUMULUS D2.1] Alain Pannetrat, Giles Hogben, Spyros Katopodis, George Spanoudakis, Carlos Sánchez Cazorla, "D2.1 Security-aware SLA specification language and cloud security dependency model", CUMULUS project, September 2013.

APPENDIX B STANDARD SCHEME EVALUATION CHECKLIST

Principle	*No.*	*Description*	*Notes*
Standard setting body independence	1.	The standard setting body is independent of the organisation(s) undertaking assessment and awarding certification	
	2.	The standard setting committee has an independent chair	
	3.	The standard setting committee may include representatives of:	
	3a.	Consumers	
	3b.	Regulators	
	3c.	Cloud Service Providers	
	3d.	Cloud Service Customers	
	4.	The standards setting body is financially independent	
	5.	Standard development and maintenance is self-funded by SSO/SDO	
Quality Assurance & Relevance	6.	A regular check of whether the standard needs to be updated to match changes in regulations is performed (e.g. annualy)	
	7.	Scope of the standard is fit for purpose	
	8.	Satisfaction survey with Assurance Scheme stakeholders is performed regularly (e.g. annually) to identify potential changes to the standard and associated approval processes	
	9.	The scheme ensures that standards are achieved	
	10.	Scheme has defined arrangements for monitoring the of standards	
The standard adherence	11.	The standard refers to or require compliance with a named code of practice(s) (e.g. ISO27002)	delivery

Certification Bodies qualification	12.	Certification Bodies are required by requirement scheme owner to have national/international accreditation (e.g. ISO17021/ISAE3000)	
	13.	The requirement scheme owner requires from certification bodies to have a quality management system	
	14.	The requirement scheme requires that the assessors adhere to certain qualification requirements:	
	14a.	Relevant formal education	
	14b.	Minimum number of years' work experience	
	14c.	Completion of a certified course/training	
	14d.	Adhere to Code of Professional Ethics	
	14e.	Commit to abide to a Continuing Professional Education Policy	
Assessment quality	15.	Frequency of assessments is risk based and the maximum period does not exceed 12 months	
	16.	Assessments include the compliance against all aspects of the standard	
	17.	Assessments include observation of activities, such as customer care, security, record keeping	
	18.	Evidence collected during the assessment is of suitable quality	

APPENDIX C MAPPING REQUIREMENTS TO PRINCIPLES AND CRITERIA

Requirement	Criteria	Principle
Comparability of Control Framework (R1)		
R1.1 The EU-SEC Governing Body shall perform the mapping and gap analysis of requirements of different certification schemes.	C.1.	P1, P2, P4
R1.2 The EU-SEC Governing Body shall determine the nature of the gaps between the requirements of different certification schemes.	C.1.	P2, P4
R1.3 The EU-SEC Governing Body should suggest the compensating requirements to bridge the identified gaps between the requirements of different certification schemes.	C.1.	P2, P4
R.1.4. The EU-SEC Governing Body should adopt a clear, well documented and transparent approach for performing a comparison and gap analysis between requirements of different security frameworks.	C.1.	P4
R1.5 The Authority should accept the requirements mapping, gap analysis and potential compensating requirements of the EU-SEC framework.	C.1.	P4
Comparability of Auditing Mechanisms (R2)		
R2.1 The Authority shall require from Authorized Auditor to use control procedures and metrics that are comparable and are resulting in the same level of assurance.	C.2.	P2
R2.2. The Authority shall require from Authorized Auditor to perform audits which refer to or require compliance to a named code of practice(s).	C.2.	P1, P3, P4
R2.3 The Authority shall require that the Authorized Auditor accepts to perform an audit on a scope that is considered as relevant.	C.2.	P3
Suitability of Evidence (R3)		
R3.1 The Authority shall require from Authorized Auditor to collect evidence that needs to be appropriate, sufficient, selective and persuasive, providing an extent of information and guidance of procedure for a reasonable audit.	C.3.	P4

R3.2 The Authority shall require from Authorized Auditor to determine the timeframe of collected evidence.	C.3.	P3, P4
R3.3 The Authority shall require from Authorized Auditor to identify the criteria against which evidence is needed to be audited in order to secure understandability and correctness of his conclusions.	C.3.	P3
R3.4 The Authority shall require from Authorized Auditor to record audit findings to enable informed decision on compliance with the requirements.	C.3.	P1, P2
R3.5 The Authority shall require from Authorized Auditor to record nonconformities with specific requirements and contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based.	C.3.	P3, P4
R3.6 The Authority shall require from Authorized Auditor to follow a consistent and relevant sampling approach in the collection of evidence.	C.3.	P1, P2, P3, P4
Auditor Qualification (R4)		
R4.1 The EU-SEC Governing Body shall initiate the process for mutual recognition only between certification schemes that impose clear, transparent, comparable and relevant auditor qualifications.	C.4.	P4
R4.2 The Authority shall require from Authorized Auditor to lead the auditing or assessment engagement as required by standards and schemes in the scope of the engagement.	C.4.	P3, P4
R4.3 The Authority shall require from Authorized Auditor to have sufficient subject matter expertise and knowledge to allow professional judgement. The relevant expertise shall be supported by relevant professional certifications.	C.4.	P1, P2, P3, P4
R4.4 The Authority shall require from Authorized Auditor to have sufficient number of personnel with adequate professional experience to conduct the audit.	C.4.	P4
R4.5 The Authority shall require from Authorized Auditor to adhere to the Code of Professional Ethics.	C.4.	P4
Governance Model (R5)		
R5.1 The EU-SEC Governing Body shall allow mutual recognition only between schemes that have a well-defined, transparent and documented governance structures.	C.5.	P4

R5.2 The EU-SEC Governing Body shall allow mutual recognition only between schemes that have a governance structure that guarantee independency and prevent any possible conflict of interest.	C.5.	P4
R5.3 The governance structure of the certification scheme under comparison shall envisage mechanisms for the collection of complaints.	C.5.	P1, P2, P3, P4
R5.4 The governance structure of the certification scheme under comparison shall envisage internal audit mechanisms, i.e. the scheme owner should be entitled to periodically audit the certification bodies / auditing partners.	C.5.	P1, P2, P3, P4
R5.5 The governance structure of the certification scheme under comparison shall clearly identify their governing body and shall define its roles and responsibilities.	C.5.	P4
R5.6 The governance structure of the certification scheme under comparison shall include a clear change management process.	C.5.	P4
R5.7 The governance structure of the certification scheme under comparison shall transparently define what the rules of participation into the governing bodies and their decision-making mechanisms are.	C.5.	P4
R5.8 EU-SEC Security Requirements Repository should be audited by accredited auditors.	C.5.	P4
R5.9 The Authority should maintain a publicly available register of Authorized Auditors	C.5.	P4
R5.10 The Authority shall maintain a register of Certified CSPs; such a registry should be preferably made publicly available.	C.5.	P4
R5.11 The EU-SEC Framework Governance Body shall maintain a repository of standards, best practices and control frameworks that are covered under the mutual recognition framework and provide reference to the specific requirements/controls in each standard.	C.5.	P1, P2, P4
R5.12 The Authority shall periodically audit the Authorized Auditors.	C.5.	P1, P3, P4