EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D2.1 MULTIPARTY RECOGNITION FRAMEWORK FOR CLOUD SECURITY CERTIFICATIONS

VERSION 1.1

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: September 30th, 2017	DELIVERY DATE: December 19, 2018
AUTHOR: CSA	PARTNERS CONTRIBUTED: NIXU, PwC, SI-MPA
DISSEMINATION LEVEL:* PU	NATURE OF THE DELIVERABLE:** R
INTERNAL REVIEWERS: SI-MPA, MFSR	

*PU = Public, CO = Confidential

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

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

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	22/05/2018	Initial version	Immo Regener (PwC), Jarkko Majava, Mikko Larikka (NIXU), Damir Savanovic, Daniele Catteddu (CSA)
1.1	14/12/2018	Revision of chapters 1, 2 and 3, quality check.	Damir Savanovic, Eleftherios Skoutaris (CSA)

EXECUTIVE SUMMARY

The rapidly changing legal and regulatory landscape has heavily impacted security assurance, governance and compliance. The certification landscape and respective market seem to show signals of inefficiency and lack of effectiveness. Cloud service providers are under considerable pressure, as they are being called to comply with several international, national, and sector specific standards and requirements. Such a proliferation of standards and requirements is dramatically demanding more resources to be spent, increases compliance monetary costs, and potentially also creates room for security vulnerabilities. Cloud users on the other hand, are in need to obtaining clear information on the security and compliance posture of their cloud service providers so to be able to take informed decisions, in contrast to numerous certification and standards which seem to create more confusion rather than clarity.

One of the of the main objectives of the EU-SEC project is to develop a framework for the multi-party recognition between existing cloud security certfication schemes such as: ISO27001, SOC2, CSA STAR Certification and Attestation, BSI C5, and other national schemes or requirements for cloud security. Many of the (mainly national) existing cloud security standards have a considerable amount of overlapping requirements, thus it appears beneficial to identify those common grounds and normalise them under a comprehensive framework. In this document, a framework model for multiparty recognition and its governance structure are presented, as a means to achieve the aforementioned objective.

Motivation to this work has been the challenge and need of achieving cost-effectiveness, increased transparency, awareness and trust with respect to cloud security certification, in aid to the cloud computing organizations and relevant stakeholders within the EU market.

The framework's modeling approach was based on the cornerstone activities for multiparty recognition, that is, the comparison analysis activities of certification/compliance schemes, in adherence to the framework's lifecycle, criteria and requirements already defined in previous works [1]. In this context, information flow diagrams and input/output activity matrices were used to accurately define the framework's operation and governance processes, as well as the roles and responsibilities for the involved stakeholders per activity. Our goal was to develop a model that will allow us to systematically and methodically evaluate, execute and finally govern the multiparty recognition framework, while ensuring its long-term sustainability.

The contributions of the work are two-fold, each including a plethora of advantages. In one hand, the proposed framework architecture is characterized by high scalability and

manageability for all integrated components, allowing its rapid adaption to the evolving cloud security certification landscape. On the other hand, its design ensures the repeatability, consistency and communication of the expected multiparty recognition results, thus promoting awareness and trust towards the multiparty recognition works among the concerned stakeholders (e.g., CSPs, cloud users, scheme owners).

The importance of a multiparty recognition framework and its governance is non-trivial as it constitutes the anteroom of forthcoming works towards its full integration into the EU-SEC framework, anticipated in EU-SEC work package 2 deliverables [2] and [3].

ABBREVIATIONS

Abbreviation	Description
(ISC)²	(ISC)² is an international nonprofit membership association best know for its award-winning Certified Information Systems Security Professional (CISSP®) certification, with additional certification and education programs that holistically address security.
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.
CS	Cloud Service
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)
CSA OCF	Cloud Security Alliance Open Certification Framework
CSA STAR	Cloud Security Alliance Security, Trust and Assurance Registry
CSB	Cloud Service Broker
CSC	Cloud Service Customer
CSCA	Cloud Service Auditor

Abbreviation	Description
CSIRT	Computer Security Incident Response Team, a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. (http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?)
CSP	Cloud Service Provider
D1.2	EU-SEC deliverable of task 1.1 " Security and Privacy Requirements and Controls"
D1.3	EU-SEC deliverable of task 1.2 "Auditing and assessment requirements"
D1.4	EU-SEC deliverable of tasks 1.3 and 1.4 "Principles, criteria and requirements for a multiparty recognition and continuous auditing-based certifications"
D2.4/D2.5	EU-SEC deliverables of task 2.4 "EU-SEC Framework"
DPA	Data Protection Authority as defined in General Data Protection Regulation EU (2016/679)
DPIA or PIA	"Data Protection Impact Assessment" (DPIA) or "Privacy Impact Assessment" (PIA) - the process for building and demonstrating compliance.
EU	European Union
EU MS	European union member state
EU-SEC	European Security Certification Framework (http://www.sec-cert.eu/)
GA	Governing Authority
GDPR	General Data Protection Regulation EU (2016/679) (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)
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.
ISMS	Information Security Management System (See Terminology and Definitions – Management System)

Abbreviation	Description
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)
ITRM	The IT risk management (ITRM) (market) is a part of the growing category of integrated risk management (IRM) solutions. Through common functions, such as an asset inventory, requirements mapping, survey capabilities, workflow functions and data import, IRM automation addresses multiple segments. Within its coverage, Gartner has defined seven primary IRMS segments: • Operational risk management (ORM) • IT risk management • Business continuity management (BCM) planning • IT vendor risk management (VRM) • Corporate compliance and oversight (CCO) • Audit management (AM) • Enterprise legal management (ELM)
MFSR	Ministry of Finance of the Slovak Republic (http://www.finance.gov.sk/en/)

Abbreviation	Description
NIS	Network and Information Security
NPC	National Point of Contact
PA	Public admin
RfC	Request for Change
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)
SIA	Slovenian Institute of Auditors (http://www.si-revizija.si/)
SIEM	Security information and event management products and/or services, which produce an operational view to information security status, enhancing log management and combining it with security event monitoring to enable centralized reporting (https://www.nixu.com/en/service/security-information-and-event-management-siem)
SI-MPA	Republic of Slovenia Ministry of Public Administration (http://www.mju.gov.si/en/)
SMEs	Small and Medium-sized Enterprises
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	SOC for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service. (https:// aicpa.org/soc4so)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

The deliverable D2.1 uses following terminology. Each used term is explained, while existing defined terms have reference to original standard definition.

Table 1. Terms and definitions.

Term	Definition	Source
Accreditation	Accreditation assures users of the competence and impartiality of the body accredited.	http://www.iaf.nu/
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
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 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

Term	Definition	Source
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
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. A certification body is considered as an authorized auditor.	
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)

Term	Definition	Source
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.	
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
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
Governance 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 analyzed 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
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
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

1 INTRODUCTION

The EU-SEC project is devised to improve the effectiveness and efficiency of existing security certification schemes by addressing issues related to compliance and certification, security governance and risk management in the cloud. In particular, one of its objectives, which is also the subject matter of this deliverable, is to address certain side effects caused by the increasing proliferation of certification and compliance schemes, the lack of harmonised rules for bridging the gaps between the different schemes' requirements and lack of transparency with respect to their security-oriented differences. The ultimate goal is the creation of a multiparty recognition framework for security and privacy requirements comparison between different standards and compliance schemes.

Our work uses the theoretical basis established in [1] and extends it by providing a sound modelling architecture towards the development of a structured framework for multiparty recognition. The envisaged model uses a set of well-defined matrices and information flow diagrams as a means to define the theoretical model's key actors with roles and responsibilities and related operational and governance processes along with their integrated activities.

The main objective and contribution of this work involves the realization of a framework that can be used to systematically and methodically achieve multiparty recognition between any given certification schemes. At the core of the framework lie the operational processes that are used to perform the various evaluation and comparison analyses between the compared schemes and the EU-SEC repository of security and privacy requirements, which is updated and maintained to include and provide -upon request- to cloud stakeholders the comparison's output results.

Furthermore, the framework is extended to include a governance structure, which purpose is to continuously manage, extend and finally adapt the framework's organization and its repository of requirements to the changes of the evolving cloud security certification landscape. Currently, the framework's governance is addressed with the introduction of two main processes, those of, change and complaint management.

The defined architectural model with its operational and governance proccesses presented in this document is expected to be further improved and refined in future deliverables, that is, [2] and [3], based on the input collected during the use-case "proof of concept" works of the framework throughout the EU-SEC project's pilot in work package 4.

1.1 CHALLENGES OF CERTIFICATIONS PROLIFERATION AND MULTIPARTY RECOGNITION

Due to the increasing proliferation of compliance schemes at international, national and sectorial levels, several challenges have appeared to the foreground for cloud service providers. Here, we introduce these challenges and caused inefficiencies, and we describe a solution of how these can be tackled in the context of a well-defined framework for multiparty recognition.

In more detail, certifications' proliferation has led to various concerns within the respective community and European digital single market due to certain inefficiencies that it has caused, and which have recently appeared in the foreground. More specifically, these inefficiencies considered are:

- Cloud-based organisations are pushed to invest considerable amount of resources in multiple compliance audits that in most cases are conducted based on an overlapping set of security requirements that exist between the different certification schemes. The former actions have an additional impact to organisations, that is, as in many cases the organisational budget for operational security and security compliance is the same, a disproportional increase of the latter compliance costs generates a lack of resources to invest in operational security. The multiparty recognition framework aims at tackling the former problem by enabling its processes to compare two compliance schemes and output a minimum set of complementary security requirements to be audited, hence reducing the overall auditing effort and costs.
- Potential confusion is created for the cloud users, as they may not understand the differences between the various certification schemes. This generates the opposite effect of what a certification scheme is supposed to bring along as a benefit, i.e., being a vehicle of trust, and not a vehicle of confusion. The multiparty recognition framework is expected to add more transparency to the similiarities and differences that exist between the security requirements of two schemes, hence raising awareness and adding to better understanding and higher trust.
- The existence of several EU national certification schemes, rather than creating the conditions for the flourishing of the Digital Single Market[1], creates instead potential market barriers for Small and Medium-sized Enterprises (SMEs) that cannot afford to invest resources in multiple certifications. The multiparty recognition framework and its

[1] https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market, accessed on 10/12/2018.

EU-SEC repository will constitute a unified repository of integrated cloud certifications' security requirements of national and international levels, aiding small enterprises to understand and achieve more efficiently compliance.

- Multiple third parties that have access to a company's IT service during compliance audits could be considered as a potential vulnerability, as they could be a factor of attack vector multiplication and consequently increase the security risk probability. The framework will generate only a minimum set of requirements which will be additionally required to be assessed for compliance through an external audit, hence reducing organisation's security surface exposure.

In this context, CSPs and cloud users need an organised structure with simple mechanisms and supporting tools for facilitating the security and privacy cost/benefit analysis of required certifications. For instance, they need processes and tools that offer ways to compare cloud services and related security compliance schemes and requirements based on the trust levels they offer as well as the transparency and assurance indicators they provide.

In order to tackle the aforementioned inefficiencies, the solution cannot be based solely on predefined principles, criteria and requirements, since the former act only as foundational prerequisites toward mutual recognition of certification schemes. Instead, the proposed solution aims at using such prerequisites as a baseline to establishing a comprehensive framework for achieving multiparty recognition that is composed of well-defined actors with roles and responsibilities and mechanisms for binding roles and requirements to processes and their respective tools.

1.2 SCOPE AND OBJECTIVES

The scope of this work encompasses the development of a multiparty recognition framework for cloud security certification that is based on the mutual recognition criteria identified between widely known certification schemes in the fields of IT security and cloud computing.

The scope of work for the established framework takes into consideration the following main activities and components such as:

- Existing multiparty recognition principles, criteria and requirements are used as a basis to formulate compliance schemes' eligibility evaluation processes within the framework's architecture. Such processes will allow for mutual recognition to become possible between the different certification schemes.

- Definition and development of a well-defined layered architecture with involved actors, related roles and responsibilities, and integrated input/output processes, which are jointly used to perform the multiparty recognition activities
- Definition and development of a governance structure which shall dictate how the framework is to be managed in the long-term with respect to required changes, updates and maintenance tasks.

Activities within the scope of work involve the enforcement of the criteria and requirements for multiparty recognition (defined in D1.4) into a framework with clear structure, purpose and objectives, that will allow for multiparty recognition between certification schemes.

The framework's processes are defined by having in mind the comparison requirements between a number of known cloud security compliance guidelines and national requirements including: the German BSI, French ANSSI, Ministry of Finance of the Slovak Republic, Slovenian Ministry of Public Administration, international standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, CSA CCM and technical, business oriented schemes (e.g., Financial sector, new laws and regulations). It uses the multiparty recognition criteria to establish and define mutual recognition relationships between different certification schemes as well as the relationship between those and the EU-SEC framework. In addition, a governance structure and related management activities are defined to allow for the practical use and future extension of the framework.

To this end, the specific objective of the work is to define a multiparty recognition framework that will include:

- Components, processes and underlying activities for implementing, operating and managing the framework over time;
- Governance structure which shall include the involved parties, assigned roles and responsibilities, and related processes to assist toward the future management and extension requirements of the established framework.

Any mapping activities with respect to the collection and comparison analysis of security and privacy controls and auditing requirements of certification schemes, as well as the definition of multiparty recognition criteria took place in [2], [3] and [1] respectively and are not in the scope of this work. However, respective comparison-based processes with an objective to perform a comparison analysis between two schemes are to be developed and integrated into the multiparty recognition life-cycle. The repository of requirements and the multiparty recognition

principles-criteria-requirements, are also to be reused and introduced as foundational construction elements to the multiparty recognition framework and its governance structure.

It is to be noted, that it is in this work's scope and its underlying activities to design a framework, which sole objective is to perform a comparison analysis between the requirements of two certification schemes. Having said that, it is to note that it is not in the scope of this work the definition of a framework which foresees any auditing activities within its underlying processes or outputs any new certification scheme. Instead, the output result of such requirements comparison analysis is used to update the EU-SEC repository of security or privacy requirements that finally become disseminated to the relevant cloud-stakeholders. For instance, an auditor can utilize the EU-SEC repository of requirements to perform an audit against a compliance scheme, however, this activity shall take place independently to the multiparty recognition framework's processes and respective activities.

The target audience for this document includes all interested stakeholders in the area of cloud computing security and certification, such as cloud service providers, certification/compliance scheme owners, auditors and cloud users.

1.3 METHODOLOGY

The realization of the multiparty recognition concept into a framework required the systematic organization and integration of processes and activities for multiparty recognition into a well-defined hierarchical and layered architecture.

Several requirements that add to the modelling complexity include:

- The involvement and necessary collaboration between various stakeholders with distinct roles and responsibilities, such as scheme owners, auditors and the EU-SEC governance body,
- The evaluation of the candidate schemes, if they meet the predefined principles, critera and requirements, in order that they are eligible for multiparty recognition,
- The management of multiparty recognition activties and underlying processes for comparison analysis between certification schemes,
- The execution, sustainability, support and update of requirements for all related activities using a methodical and consistent approach.

To address the above requirements and overcome the inherent complexity of the task, we developed a layered architecture that is based on a comprehensive model comprised of matrices and information flow diagrams, as presented in chapters three and four. The use of matrices allows us to define and describe the required activities and the input/output products of all processes of the framework and its governance structure as well as the corresponding roles and responsibilities of the engaged stakeholders. Similarly, diagrams allow us to visually model the information flow between the framework's predefined activities, hence making each step throughout the multiparty recognition process explicit, from starting to ending points.

1.4 STRUCTURE

The document is organized as follows:

Chapter 2 introduces the preparatory works for multiparty recognition and highlights the importance and contribution of such works toward the realization of the concept.

Chapters 3 and 4 constitute the major contributions of this work. In chapter 3, the actual realization of the multiparty recognition framework is presented, where it is shown how the interrelated parties use the framework's defined activities and underlying processes to achieve multiparty recognition. Chapter 4 presents the governance structure of the framework, comprised of components, governance body with roles and responsibilities and relevant systematic activities in the form of processes. Activities are presented in the form of the framework's change management and complaint management processes.

Finally, Chapter 5 summarizes in brief and concludes the work, and provides additional recommendations for future works and further possibilities for the framework's extension.

1.5 WORK PACKAGE TWO DEPENDENCIES

The work package two (WP2) has both internal and external dependencies as shown in Figure 1. It is to be noted that all dependencies shown use as point of reference WP2 and hence do not reflect any dependencies between the remaining work packages.

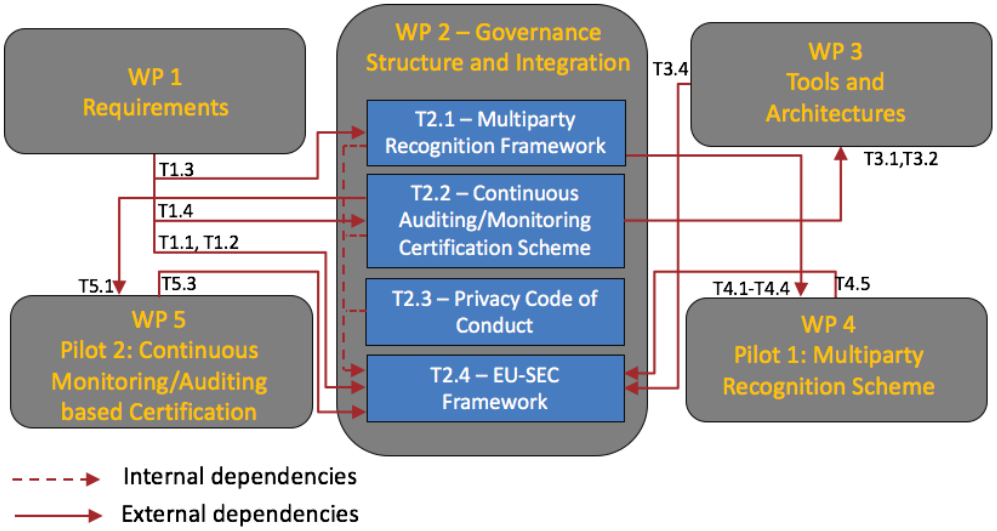

Figure 1: Illustration of the WP2 internal and external dependencies.

More specifically, internally to the work package, T2.1-T2.3 contribute foundational elements of governance structures to the meta-governance framework that is established within T2.4. Externally, there is a bidirectional dependency between work package two and working packages one, three, four and five.

Work package one and tasks T1.1, T1.2 contribute to the EU-SEC framework structure that is realized within T2.4, while T1.3 and T1.4 set the requirements basis for T2.1 and T2.2 respectively.

A bidirectional flow between work packages two and five is also established. Knowledge acquired from the work in T2.2 is used to establish the case study of work package five and in return the results of the study are provided as feedback to T2.4, which integrates the results. By the same means, the multiparty recognition framework established in T2.1 is used as a reference point to supporting the case studies T4.1-4.4 of work package four. Established results are again provided as feedback to T2.4.

2 BACKGROUND TO WORKS TOWARDS MULTIPARTY RECOGNITION

One of the key concepts of the multiparty recognition framework is the comparison analysis of security requirements included in national and International standards, laws and regulations, and the definition of common elements and a common format so to enable the re-usability of requirements, and of security controls. The working assumption that has driven this work was that there is a considerable level of overlap between security requirements included in different standards, laws, regulations and security frameworks. The result of this analysis, consolidation and deduplication exercise is the EU-SEC requirements repository.

The repository was designed to collect the security, privacy and auditing requirements relevant to cloud computing into a single location and based on a standard representation, that is, the CSA Cloud Control Matrix. The basis for the creation of the EU-SEC requirements repository and the process of requirements collection and analysis are described in detail in the EU-SEC project deliverables: D1.2 Security and Privacy Requirements and Controls and D1.3 Auditing and Assessment Requirements.

In the next sections of this chapter we provide a brief overview of the auditing requirements and security controls collection methodology and analysis and denote the importance of these works and their core role in relation to the multiparty recognition concept and the processes' development for the framework presented in this document.

2.1 SECURITY REQUIREMENTS COLLECTION AND ANALYSIS

The security requirements collection and consolidation objective aimed at investigating the means of comparability between cloud security certification schemes, with respect to the included security and privacy requirements. Diverse input sources and reference requirements were analyzed, representing one of the key enablers for the definition of rules and tools for the multiparty recognition framework.

The first step during the requirements collection was the adoption of a common methodology for the requirements identification and evaluation. The use of a common methodology ensured consistency, accuracy, time efficiency and common understanding of the methods and tools

used, as well as being able to use the CSA community for validating the acquired results. The methodology included two phases.

The first phase involved:

- the setting of a common terminology,
- specifying the thematic domains for the selection of input sources for requirements, and
- defining the requirements gathering process, which included the activities of requirements identification and mapping to the controls framework.

The thematic scope for the identification of requirements and controls included standards related to cloud computing and cloud services (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, C5, SecNumCloud), national legislation from Germany, Slovenia and Spain, European and other international legislation (GDPR), good practices (ENISA), trust services principles and criteria (AICPA TSP/TSC) and sector specific sources that focused on banking (standard, EU guidelines, PCI DSS) and public - governmental sector (legislation, recommendations). All together, 23[2] documents were identified as relevant input sources for the selection of requirements.

The second phase included:

- the requirements consolidation process that aimed to converge the identified requirements and strengthen their relevance for the EU-SEC project, and
- proposal and creation of new controls or extension of the existing controls from the CSA CCM.

The outcome of the second phase analysis provided a traceable connection between the originating certification scheme's security requirements to either existing EU-SEC security requirements or to a new security requirement. The process is presented in Figure 2.

[2] For detailed list see D1.2 Table 2.

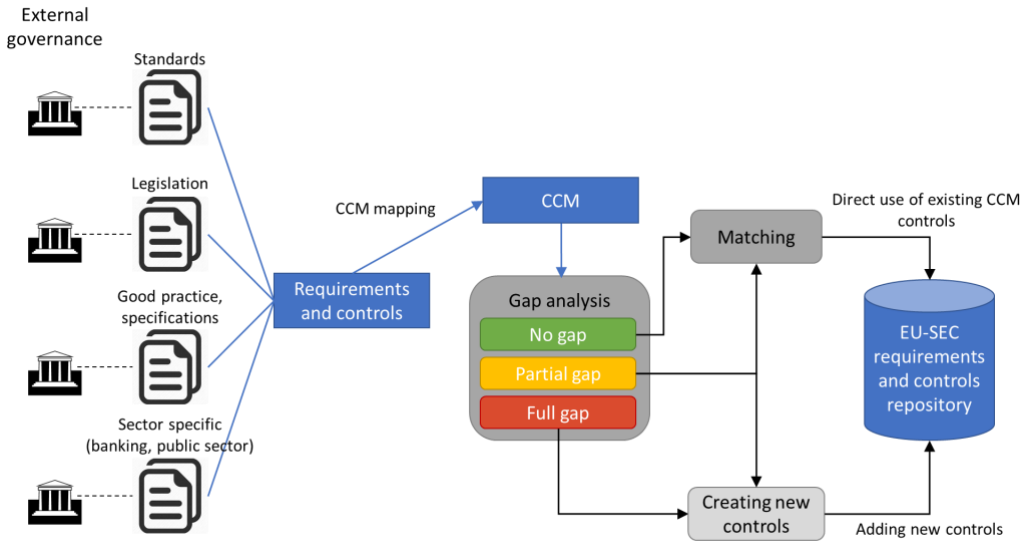

Figure 2: Requirements collection and analysis process to establishing the EU-SEC repository

The requirements collection and analysis was focused mainly on security. Nevertheless, during the process, the requirements related to privacy and personal data protection or regarding auditing, were also identified and analysed. Those requirements were evaluated (by a mapping and gap analysis), but they are addressed in detail in [4] and in [3]. More details can be found in Annex A " Requirements comparison analysis " of this document.

Use case scenario utilizing multiparty recognition

The EU-SEC requirements and controls repository constitutes the basis for the multiparty recognition framework. Figure 3 illustrates a scenario where the EU-SEC repository is utilized to achieve multiparty recognition. The scenario involves a cloud service provider who has already gained a certificate (*Standard 1 / certification scheme*) and thus is compliant with the national law (*National law 1*), and in addition wants to fulfil the compliance requirements based on another certificate (*Standard 2*).

We base our scenario on the hypothesis that all three sources of certification and compliance requirements (i.e., *Standard1, Standard 2 and National law 1*), have already been properly analysed, compared and accepted within the EU-SEC requirements repository. The CSP has implemented several controls to ensure compliance under *Standard 1* (*CCM1, CCM 2 and CCM 3)* and *National Law 1 (CCM3, Control m, other controls developed in addition to CCM)*. In this context, the CSP can demonstrate that the controls that have already been implemented to gain the certificate under the *Standard 1* and compliance to *National law 1,* fulfil also some of the requirements of *Standard 2* (*CCM1* and *CCM3* fulfil *Requirement 3* from *Standard 2)*. Based on that, in order for the CSP to gain a certificate for *Standard 2*, would need to demonstrate

compliance to only that part of the requirements (i.e., *Requirement 4)* that are not covered by previously gained certificate under *Standard 1* or compliance with *National law 1*.

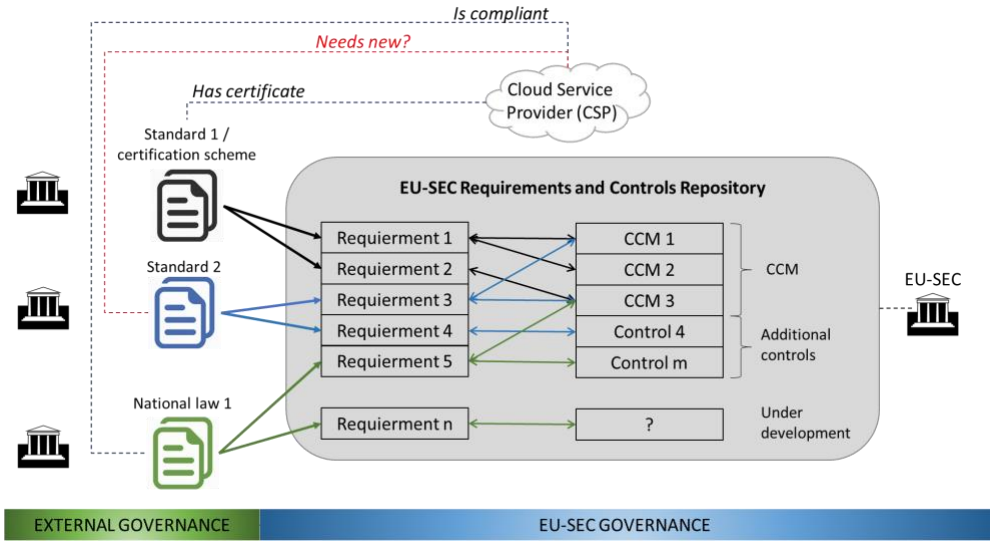

Figure 3: Multiparty recognition scenario of multiparty recognition using the EU-SEC repository

In this scenario, the EU-SEC requirements and controls repository provided reliable relationships to demonstrate a semantic overlap between security controls that fulfilled the requirements from diverse certification schemes or other input sources. It also showed the extendibility of the EU-SEC requirements and controls repository, since *Control 4,* which fulfiled *Requirement 4* defined by *Standard 2,* has been added into the repository. The conceptualization of the mechanism is presented in Figure 4 by using the context of Figure 3.

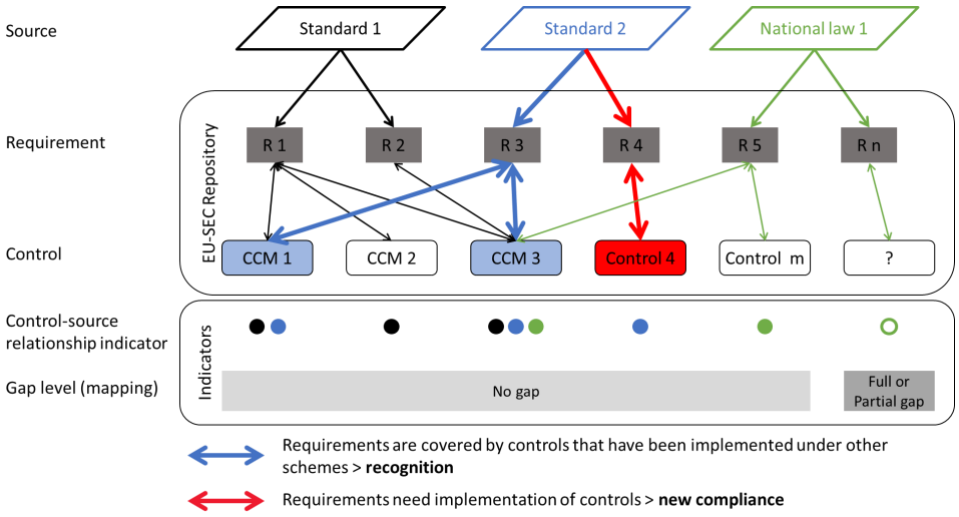

Figure 4: Mechanism of multiparty recognition between security controls

The mechanism used three types of information: the input sources (e.g., standards, certification

schemes, legislation, guidelines), the requirements that originated from those sources, and a common set of security controls within the EU-SEC framework. The requirements mapping to a common set of security controls and gap analysis formed the basic relationships. The relationships from the requirements to controls and vice versa provided traceability to sources, and identification of the controls that could be mutually recognised and used.

With the creation of new or updated controls, the EU-SEC requirements and controls repository has increased its wider applicability (e.g. to industry, public administration, CSP companies, banking specific sector etc.) and has provided rich content and information that will be useful for cloud service providers (i.e., by expanding to new markets and achieving compliance extensibility to new certifications) and cloud service customers (raising awareness through transparency of the multiparty recognition process between security certifications).

2.2 AUDITING REQUIREMENTS

The auditing requirements were analyzed in the EU-SEC D1.3 "*Auditing and assessment requirements*". They were collected from the following compliance schemes:

- ISO standards for organizations certifying information management systems (ISO/IEC 17021 and ISO/IEC 27006)
- ISO standards for auditing information management systems (ISO/IEC 19011 and ISO/IEC 27007)
- International Auditing and Assurance Standards Board proposed International Standards for Assurance Engagements ISAE 3000 and ISAE 3402

ISO/IEC 27007 is a subdomain of ISO/IEC 19011 "Guidelines for auditing management systems".

The auditing requirements that were identified and collected are specific to the auditing process, non-/conformities, auditors' competence, evidence suitability and were shown to be comparable between the listed auditing standards. For these requirements, respective comparison processes were developed and integrated into the multiparty recognition framework's architecture, as presented in chapter 3. More details on such auditing requirements can be found in Annex B of this document " General Audit Requirements".

3 MULTIPARTY RECOGNITION FRAMEWORK REALIZATION

3.1 OVERVIEW OF STRUCTURE AND UNDERLYING COMPONENTS

The purpose of this section is to introduce the modeling components used to define the framework's main processes, related activities and the involved stakeholders. These components are then used and applied toward the framework's realization.

3.1.1 FRAMEWORK LIFECYCLE

The framework is realized in accordance to a lifecycle process composed of three main phases, as shown in Figure 5 (see also D1.4. Continuous Monitoring Certification Requirements).

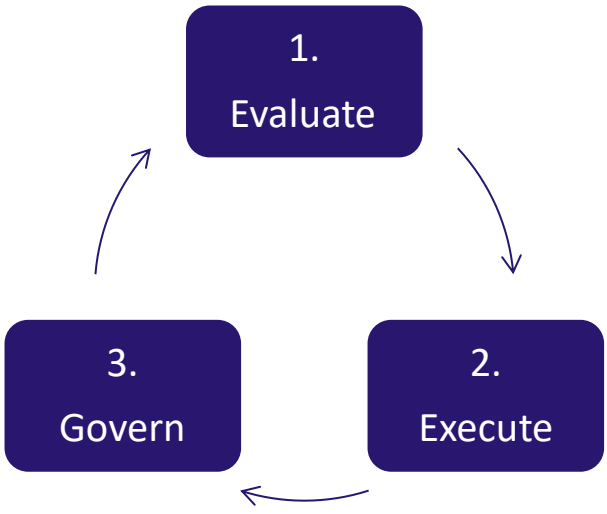

Figure 5: Process lifecycle of the multiparty recognition approach

These steps provide a guidance on how to achieve and maintain multiparty recognition within the context of continuous improvement and following changes in the environment as well as feedback based on real life implementations of the framework:

1. **Evaluate:** 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. Furthermore, throughout the framework's validation processes, the requirements comparison results are also validated for their soundness and consistency.

2. **Execute:** Within the execution step the governance body and consulting entities (e.g., scheme owners, auditors, or cloud service providers) are assuring the execution of the multiparty recognition activities, from the point of requirements' collection, comparison processing and results output and dissemination.

3. **Govern:** To ensure that the multiparty recognition framework reflects the current state of the cloud certifications and standards, a governance framework is to be implemented. Governance is applied throughout all activities of the framework in order to ensure its long term management, maintainance and its synchronization to the evolving cloud-certification landscape.

Steps one and two of the lifecycle are implemented and presented as a well-defined process in section 3.2 of the document, while step three is thoroughly presented in section 4.

3.1.2 PROCESSES AND ACTIVITIES STRUCTURE DEFINITIONS

Complementary to the framework's lifecycle high-level process are also the underlying processes and diagrams that are used to define the respective activities of the involved stakeholders. Below the relative structural templates of these activities are presented.

Introduction to the table template used for defining a process:

< Process Name>	
Inputs	List of inputs required to initialize the process and its underlying activities
Activities	List of process's underlying activities
Outputs	List of outputs resulting from the process's activities

Table 2: Input/output activities template format

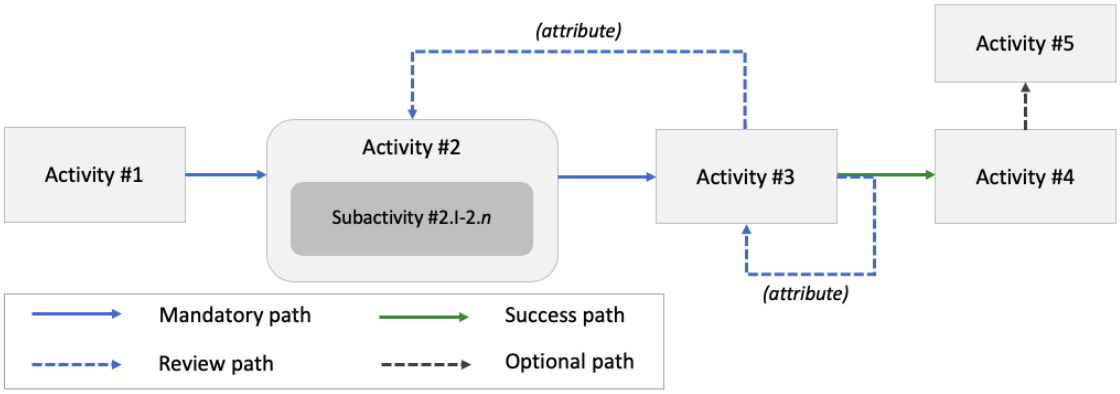

Figure 6: Process activity diagram template format

Framework's processes and underlying activities are mapped to roles and responsibilities of the involved stakeholders using the following table template:

<Process Name>		**Activities**		
		#1	**#2**	**#*n***
Roles	Role #1	*(RACI)*	…	…
	Role #2	…	…	…
	Role #*n*	…	…	…

Table 3: Process and activities mapped to roles and responsibilities template format

Introduction to table template used for defining an activity with actors, assigned responsibilities and input/output functionality:

Responsibilities	
- Person/Group #1: *(RACI)* - Person/Group #2: *(RACI)*	
Input	**Output**
- Input document/Accomplished task <xyz>	- Activity output <xyz>

Table 4: Activity input/output with mapped roles and responsibilities template format

3.1.3 STAKEHOLDERS, ROLES AND RESPONSIBILITIES

The Multi-party recognition framework is supported by four main stakeholders:

- EU-SEC governance body
- Scheme Owners
- Authorized Auditors

- Cloud Service Providers

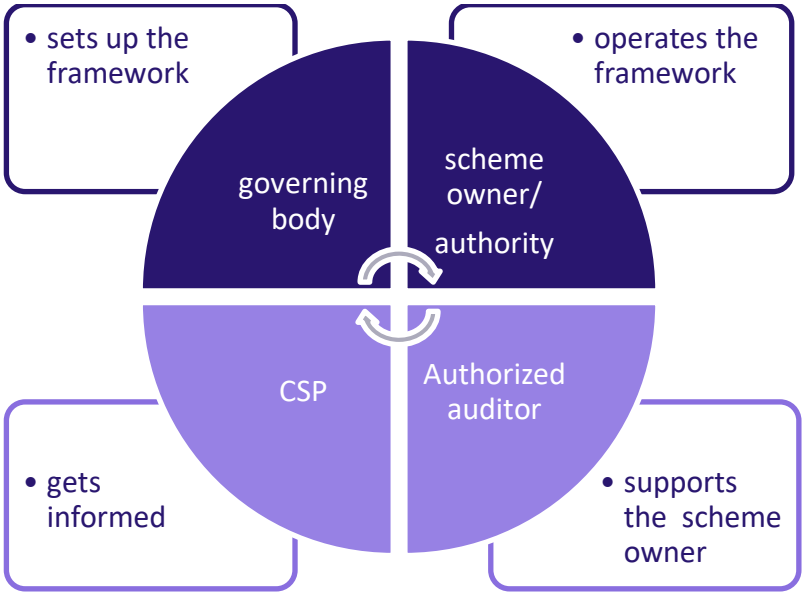

Figure 7: Stakeholders of the multiparty recognition framework

The roles of the above stakeholders are summarized as follows:

EU-SEC Governance Body: is the main stakeholder in the multi-party recognition framework. It is responsible for managing the main operational and governance activities of the framework, including the management of the EU-SEC repository of security requirements, the registered cloud security compliance schemes and maintenance of the requirements' comparison status between them.

Scheme Owners: A trusted party that is responsible for the correct organization of a certification or compliance scheme, including the accreditation of auditors and keeping a registry of certified cloud services. Scheme owners take over a significant consulting role within various processes and respective activities of the framework.

Authorized Auditors: Are qualified external auditors that constitute a trusted party or organization, which are recognized as such by the EU-SEC governance body, to provide consultation and feedback over multiparty recognition activities performed between the compared security compliance schemes.

In addition to the four aforementioned stakeholders, the following are also considered to have some form of interaction with the framework's activities and governance processes:

Cloud Service Providers: Are directly impacted from the multiparty framework's recognition results derived after the required compliance schemes' comparison analysis. In this context, CSPs maintain an open communication channel with the EU-SEC governance body in order to either access to the existing mutually recognized certifications within the EU-SEC requirements repository or be informed of certifications' undergoing mutual recognition activities and expected results.

Besides the four main stakeholders, **Cloud Service Users** (CSU) require having trust, transparency and security with respect to their data that is entrusted to CSPs. To address these requirements CSPs are acting on behalf of CSUs by reaching out to achieve multiple security certifications. Having said that, it becomes evident that CSUs are indirect stakeholders regarding the multiparty recognition framework. As indirect stakeholders, they are a driving force behind the need for multi-certification but do not have an imminent interest in how this is achieved. Therefore, CSUs and their requirements are not mentioned in other parts of this document, but instead are embedded to the role of CSPs.

In the context of the multiparty recognition framework, the main stakeholders are assigned responsibilities per assigned activity, based on the Responsibility Assignment Matrix[3] (RAM), also known as RACI matrix, which is an acronym for:

- **Responsible (R)** is to organize, perform and complete the process activity.
- **Accountable (A)** is to provide resources to perform the process and is ultimately answerable for the correct and thorough completion of the activities.
- **Consulted (C)** are subject matter experts contributing on-demand basis.
- **Informed (I)** are kept up-to-date on progress and process outcomes, at latest by the completion of the activities.

The RACI matrix is used in combination with the respective roles and assigned activities supported by the framework, as a means to achieve a higher level of granularity over the description of the required responsibilities that need to be assigned per actor and a specific activity. In this way, adherence to the framework's predefined principles (e.g., trustworthiness) can be enforced and hence succeed in the overall quality of its output results.

[3] Organization Charts and Position Descriptions". A Guide to the Project Management Body of Knowledge (PMBOK Guide) (5th ed.). Project Management Institute. 2013. p. 262.

3.2 THE DEFINITIONS OF MULTIPARTY RECOGNITION FRAMEWORK ACTIVITIES

The multiparty recognition framework is comprised of five main activities, which are run as part of the "Execute" and "Evaluate" lifecycle phases, illustrated in Figure 8. Activities 1, 2 and 4 correspond to the "Evaluate" lifecycle group of activities, while activity 3 and its underlying sub-activities, as well as activity 5, constitute the core analysis and output process respectively, corresponding to the "Execute" lifecycle group of activities. The "Govern" lifecycle group of activities interact with and run throughout the remaining two "Execute" and "Evaluate" groups, as more elaboratively described in chapter 4.

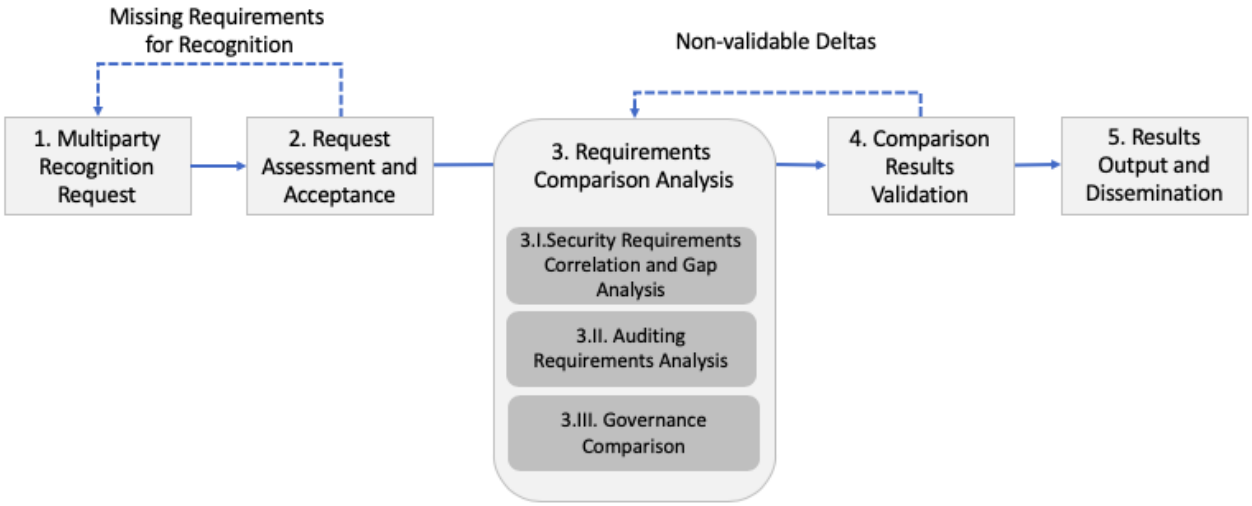

Figure 8: Multiparty Recognition Framework Process Diagram

Activities overview:

1. ***Multiparty Recognition Request*** *is the provision and collection of inputs that will be fed to the framework, involving requests from the compliance schemes to initialize the multiparty recognition framework process.*

2. ***Request Assessment and Acceptance*** *evaluates the request against the multiparty recognition framework's criteria such as comparability of the requirements and governance model, and principles such as relevancy and transparency. Approval of the request is required to initialize the correlation and gap analysis of the submitted compliance scheme.*

3. ***Requirements Comparison Analysis*** *involves the analysis of the submitted compliance scheme and is a critical activity to enable the multiparty recognition. The correlation and analysis is performed in three (3) main categories: security requirements, auditing requirements and governance requirements.*

4. ***Comparison Results Validation*** *receives input from the requirements correlation and gap analysis and assesses the results. Any deltas that are found to be unacceptable by the requesting compliance scheme owner, are fed back to the previous activity for further correlation and gap analysis. This is a feedback cycle that is continued until a satisfactory result is achieved.*

5. ***Results Output and Dissemination*** *releases the final results of the "comparison results validation" process to the EU-SEC (security and auditing) requirements repository and disseminates them to the relevant stakeholders.*

Table 5. The multiparty recognition process card: the inputs, the activities and the outputs.

Multiparty Recognition Framework Process	
Inputs	- Compliance scheme X's security and auditing requirements, and governance model description - MPRF framework criteria, principles and requirements
Activities	1. Multiparty Recognition Request 2. Request Assessment and Acceptance 3. Requirements Comparison Analysis *3.I. Security Requirements Correlation and Gap Analysis* *3.II. Auditing Requirements Analysis* *3.III. Governance Comparison* 4. Comparison Results Validation 5. Results Output and Dissemination
Outputs	- Final results of the comparison activities are archived at the EU-SEC (security and auditing) requirements repository.

Every stakeholder role in the framework has been assigned a set of responsibilities for every respective activity, as illustrated in the table below by using the RACI matrix template.

Table 6. The multiparty recognition framework process activities mapped to roles and responsibilities.

Multiparty Recognition Framework Process	**Activities**

		#1	#2	#3	#4	#5
Roles	EU-SEC Governing Body	R	A R	R	R	A R
	Compliance Scheme Owners	A R	C	A R	A R	R
	Authorized Auditors	(A R)[4]	C	C	C	C I
	Auditees (the Cloud Service Providers)	-	-	C	C	C I

The main processes' activities and the underlying sub-activities of the multiparty recognition framework are described in more detail in the subsections below.

3.2.1 ACTIVITY #1: MULTIPARTY RECOGNITION REQUEST

Process requests from the various cloud stakeholders, e.g., compliance scheme owners, and initialises the multiparty recognition framework process.

Table 7. The activity #1 card to detail sub-activities, inputs and outputs.

Activity #1	
List of the activities: 1# Cloud stakeholder submits a request. 2# EU-SEC governance body generates the Request ID for the submission, with a description of the request and the submitter's (e.g., a compliance scheme owner's representative) contact details and confirms receipt with the submitter. 3# EU-SEC governance body to request from the submitter for the description of the compliance scheme's security requirements, auditing requirements and governance model. 4# Compliance scheme owner to submit the requested documents. 5# Once the initial set of documentation is received and verified for its completeness, the request process results are passed to the activity #2, or are closed in the case of an incomplete request.	
Inputs	**Outputs**
1# A request by a cloud stakeholder is received in written method 2# Request management system	1# Request ID (e.g., Unique identifier) with the description of the request and contact details 2# The submitted compliance scheme's security and auditing requirements, and governance model description.

[4] In case when Authorized Auditors present the Certification Body (e.g. ISO).

3.2.2 ACTIVITY #2: REQUEST ASSESSMENT AND ACCEPTANCE

The outputs of activity #1 are evaluated against the multiparty recognition principles, criteria and corresponding requirements. More specifically, the certification or compliance schemes that are provided as input to the framework are evaluated for eligibility against certain principles, criteria and requirements (PCRs) for multiparty recognition. If the candidate schemes do not satisfy these PCRs then multiparty recognition is not made possible and activity #2 triggers a request back to activity #1, for the resolution of the missing PCRs. A more detail list of the underlying subactivities of #2 are presented in Table 8.

Table 8. The activity #2 card to detail sub-activities, inputs and outputs.

<table>
<tr><th colspan="2">Activity #2</th></tr>
<tr><td colspan="2">List of the activities:
1# EU-SEC governing body to confirm receipt with the submitter that the assessment and acceptance activity have started.
2# EU-SEC governing body evaluates the compliance schemes' governance models, security requirements and auditing requirements in co-operation with the scheme owners that the multiparty recognition framework criteria and principles are met.
3# EU-SEC governing body to make preliminary request acceptance (preliminary Dis-/Approved) decision
4# In case the preliminary approval, jointly with the scheme owner, the EU-SEC governing body defines a scope for the requirements correlations and gap analysis.
5# Scheme owner reviews and accepts the scope's definition.
6# EU-SEC governing body performs a final review and acceptance of the scope definition.
7# EU-SEC governing body makes a final request acceptance (final Dis-/Approved) decision.
8# Approved request is passed to the activity #3, or close the rejected and/or incomplete request.</td></tr>
<tr><th>Inputs</th><th>Outputs</th></tr>
<tr><td>1# Activity #1 outputs
2# Request management system
3# Multiparty recognition framework principles, criteria and requirements</td><td>1# Request acceptance (Dis-/Approved)
2# Reviewed and Approved Scope for Activity #3</td></tr>
</table>

Approval of the input request is required to initialize the "Requirements Comparison Analysis" activity #3, for the submitted compliance scheme(s).

3.2.3 ACTIVITY #3: REQUIREMENTS COMPARISON ANALYSIS

Produces an objective correlation and gap analysis of the submitted compliance scheme's in-scope area. The comparison analysis is performed in parallel by the three (3) main categories, each executed independently from one another: the security requirements, the auditing requirements and the governance model. The final output is sent to formal acceptance by the activity #4, where the parallel streams join as one stream.

Subactivity 3.I: Security Requirements Correlation and Gap Analysis

The submitted compliance scheme's security semantics of the security requirements is analyzed with the method explained in chapter 2.1. The correlation, mapping and gap analysis results and definition of the new requirements is performed using the EU-SEC requirements repository as the reference point. The information flow of the process is depicted in the figure below.

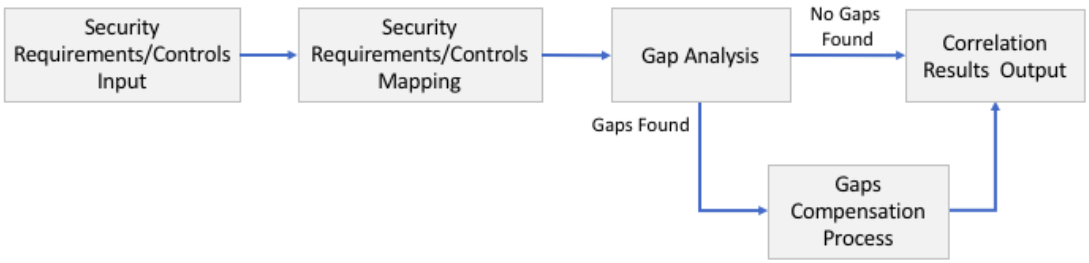

Figure 9. Security requirements correlation and gap analysis activity diagram.

The mapping and gap analysis approaches are (currently) based on an informal, but unified and consistent methodology and related tools, which requires professional judgement for the identification and interpretation of the possible semantic equivalences that are to be found between the submitted compliance scheme [2] and the (EU-SEC requirements repository) reference point. The Compliance Scheme Owner is to review the outcome and if required, additional consultation for the analysis is requested from the subject matter experts, such as the auditors and auditees. The Compliance Scheme Owners is ultimately responsible to liaise and approve the interpretations.

Table 9. The activity #3.I card to detail sub-activities, inputs and outputs.

Activity #3.I	
List of the activities: 1# EU-SEC governing body to confirm receipt with the submitter (within two business days at latest) that the security requirements correlation and gap analysis activity has started. 2# Utilize the method explained in the chapter 2.1.2 3# If required, request additional consultation from the subject matter experts 4# Compliance scheme owner to review, liaise and accept the results. 5# EU-SEC analyst to perform final review and acceptance of the results. 6# Pass the results to the activity #4.	
Inputs	**Outputs**
1# Activity #2 outputs 2# Request management system 3# EU-SEC requirements repository 4# The method explained in the section 2.2.3 "use case scenario utilizing multiparty recognition"	1# The security requirements correlation, mapping and gap analysis results matrix 2# Compensating controls matrix (if required)

Subactivity 3.II: Auditing Requirements Analysis

In this activity the submitted compliance scheme's auditing requirements are to be analyzed. In the case of ISO-series of standards comparison analysis, the ISO standards 27006 and 27007 are used as the reference points. The first "specifies requirements and provides guidance for bodies (audit firms) providing audit and certification of an information security management system (ISMS)" and the latter "provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS (cloud security) auditors".

Earlier EU-SEC research (D1.3) advises to focus on the general auditing requirements comparison, that includes, the evidence suitability, the auditors' qualification and the auditing process requirements.

The purpose of this activity is the comparison of audit-based requirements, such as the audit mechanisms, auditor's qualifications and evidence suitability, as defined by the certification or compliance schemes' that are placed under comparison. The comparison results represent useful guidelines for the auditors, and more importantly when it comes to the additional auditing requirements they will need to adhere to for the target certification (i.e., the additional

certification a CSP aims at proving compliance with) that is to be acquired, when placing the corresponding EU-SEC repository requirements under compliance assessment.

Figure 10: Auditor competence analysis activity diagram.

For example the auditors' qualifications comparison activities are illustrated in Figure 10. Certain requirements such as the auditors' "professional experience" and the respective "code of ethics" requirements as defined by of the two schemes are placed under the "miscroscope" and are compared.

Table 10. The activity #3.II card to detail sub-activities, inputs and outputs.

Activity #3.II	
List of the activities: 1# EU-SEC governing body to confirm receipt with the submitter (within two business days at latest) that the auditing requirements correlation and gap analysis activity has started. 2# Utilise the auditing requirements comparison. 3# If required, request additional consultation from the subject matter experts 4# Scheme owner to review, liaise and accept the results. 5# EU-SEC governing body to perform final review and acceptance of the results. 6# Pass the results to the Activity #4.	
Inputs	**Outputs**
1# Activity #2 outputs 2# Request management system 3# ISO standards 27006 and 27007	1# The auditor and auditing process and requirements comparison matrix 2# Compensating auditing procedures matrix (if required)

In the scope of this activity #3 resides also the evidence's suitability comparison. This activity's results represent useful guidance for auditors against additional evidence suitability requirements (if any) that are derived based on the requirements comparison between the reference and target certification schemes respectively. For instance, if the target certification scheme introduces additional requirements to the reference scheme with respect to how

suitable evidence are defined, then an auditor has to consider these differences while performing an audit when using the EU-SEC repository.

Subactivity 3.III: Governance Comparison

The objective is to assess and compare the submitted compliance schemes' governance models. The activity can be broken down into several granular sub-activities as depicted in Figure 11.

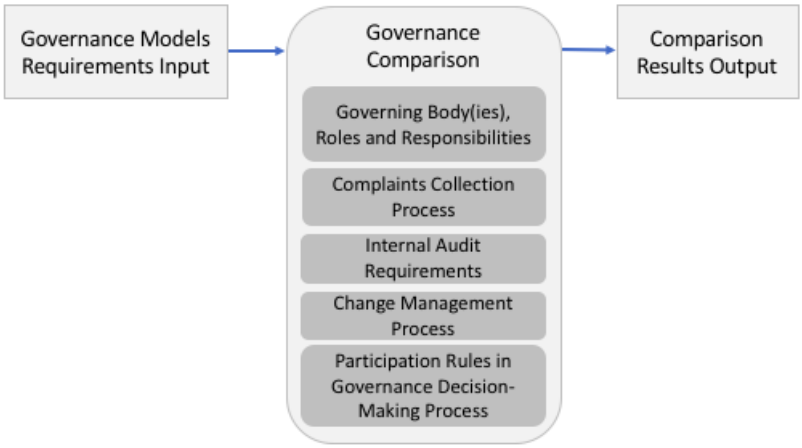

Figure 11: Governance model analysis activity diagram.

The outcome of this comparison activity is the formulation of differences that the compared schemes have with respect to their governance structures. This comparison could provide information with respect to how the requirements of a scheme are managed in short or long term periods, for instance, their estimated requirements update period.

Table 11. The activity #3.III card to detail sub-activities, inputs and outputs.

Activity #3.III	
List of the activities: 1# EU-SEC governing body to confirm receipt with the submitter that the governance model analysis activity has started. 2# If required, request additional consultation from the subject matter experts 3# Scheme Owner to review, liaise and accept how the identified deficiencies have been addressed. 4# EU-SEC governing body to perform final review and acceptance of the outputs. 5# Pass the results to the activity #4.	
Inputs	**Outputs**
1# Activity #2 outputs 2# Request management system	1# Compliance schemes' governance requirements comparison results 2# Compensating governance procedures matrix (if required)

3.2.4 ACTIVITY #4: COMPARISON RESULTS VALIDATION

EU-SEC Governance Body is informed about the three Activity #3 streams' results and will review them as one "package":

1# The security requirements correlation, mapping and gap analysis results matrix
2# Compensating controls matrix (if required)
3# The definition of new security requirements
4# The preconditions for the audit firm, auditor and auditing process to conduct an "authorized" audit in comparison to the requirements explained in chapter 2.
5# Compensating auditing procedures matrix (if required)
6# Report of all invalidation outcomes and comparison results deficiencies and how they are processed to reach a consensus between the evaluating parties.

This process enables the framework to validate the previously acquired results from the activity #4:"Requirements Comparison Analysis". The respective stakeholders will collectively work in this direction based on their assigned responsibilities. Any inconsistencies that are identified during the validation assessment activities are to be fed back to activity #3, if deemed necessary.

Table 12. The activity #4 card to detail sub-activities, inputs and outputs.

<table>
<tr><th colspan="2">Activity #4</th></tr>
<tr><td colspan="2">List of the activities:
1# EU-SEC governing body to confirm receipt with the submitter that the results validation activity has started.
2# Consulted entities review Activity #3 output results and will review them as one "package"
3# EU-SEC governing body reviews and makes final decision to go-no-go with the comparison results
4# EU-SEC governance body approves the validation output results and prepares the final output of the multiparty recognition framework to pass to actvitity #5
5# Pass the final multiparty recognition results to activity #5.</td></tr>
<tr><th>Inputs</th><th>Outputs</th></tr>
<tr><td>1# Activity #3.I, #3.II and #3.III outputs
2# Request management system</td><td>6# Final results of the validation activities
7# Comparison results matrices are finalised based on #3.I-3.III outputs</td></tr>
</table>

3.2.5 ACTIVITY #5: RESULTS OUTPUT AND DISSEMINATION

The purpose objective of this activity is to output the multiparty recognition results and to disseminate them to the corresponding EU-SEC stakeholders. Throughout this activity, the EU-SEC (security and auditing) requirements repository is updated and the requirements comparison results are archived. The activity aims at increasing awareness with respect to the purpose and importance of the framework's results by organizing webinars and workshops, create blueprints and help CSPs to design, build, operate and support their control environment in-scope of the multiparty recognition framework.

Table 13. The activity #5 card to detail sub-activities, inputs and outputs.

<table>
<tr><th colspan="2">Activity #5</th></tr>
<tr><td colspan="2">List of the activities:
1# EU-SEC governing body to confirm receipt with the submitter that the dissemination activity has started
2# EU-SEC governing body to update EU-SEC (security and auditing) requirements repository
3# EU-SEC governing body to organize webinars and workshops on the newly included compliance scheme
4# EU-SEC governing body to create blueprints on applying the multiparty recognition framework for the submitted compliance scheme together with
5# EU-SEC governing body to invite, include and promote the compliance scheme owner, auditors and auditees the slack channel to request and receive support.
6# Enroll the compliance scheme for the designated operational role specified in the governance structure
7# Complete and archive the request.</td></tr>
<tr><th>Inputs</th><th>Outputs</th></tr>
<tr><td>1# Activity #3.I, #3.II and #3.III outputs
2# Activity #4 outputs
3# EU-SEC requirements repository
4# Request management system
5# Webinar system</td><td>1# Updated EU-SEC (security and auditing) requirements repository
2# Awareness delivered with webinars and workshops
3# Blueprints for applying multiparty recognition framework on the submitted compliance scheme
4# Support channel for the CSPs and cloud users</td></tr>
</table>

4 GOVERNANCE STRUCTURE

The cloud security certification landscape is not static and is likely to change at a rapid pace. New security threats, laws, regulations and compliance requirements must be addressed promptly. In this context, the multiparty recognition framework and its components must adapt in order to ensure that the framework's objectives and requirements are continuously met.

This chapter focuses on defining the governance processes of the framework, as part of the "Govern" step in the framework's lifecycle as described in chapter 3.1.1, and aims at regulating the operation and required changes to the framework and its components. In order to ensure an efficient and effective operation and change management of the framework, the governance processes presented hereby, depend on and integrate with the multiparty recognition process defined in chapter 3.2.

The multiparty recognition framework is built over a set of security requirements deriving from national, international and sectorial cloud security certification or compliance schemes. However, these requirements are expected to evolve and change over time, hence new requirements for compliance will be introduced. For instance, the EU-SEC requirements repository is one of the main components of the multiparty recognition framework that will be significantly influenced by the evolving cloud-based security certification landscape. In order for the multiparty recognition framework and its relevant activities to be effective, the EU-SEC repository must remain up-to-date and relevant to the state-of-the-art of widely used certification/compliance schemes. In addition, the same maintenance approach is also expected with respect to the multi-party recognition criteria and requirements defined in D1.4.

To address the previous challenges and, overall, the operations management of the EU-SEC multiparty recognition framework, a governance structure needs to be defined. The governance structure shall ensure consistency and control over the framework's operation, processes and required changes.

The governance structure defines the "how" and by "whom" the framework is operated and the "if", "when", "how" and by "whom" changes should be applied to the framework and its components through its integrated processes.

The components of the governance structure that will be presented in this chapter are:

- **Assets:** The framework's *assets* affected by the governance processes and required changes

- **Stakeholders**: The *stakeholders* along with their roles and responsibilities
- **Processes:** The *governance processes* and related activities

Every activity described in the framework's lifecycle and corresponding operational and governance processes influence on one or more framework assets. The assets that will be potentially affected by maintainance activities and processes are part of the governance structure.

Furthermore, every stakeholder must understand their role within each governance process and what they are expected to accomplish in order to more effectively manage the framework's operation. Defined roles and responsibilities that are already introduced in chapter 3, are hereby tailored to the governance requirements of the framework. More detailed information about the requirements for managing all governance bodies will be presented as part of deliverables D2.4 and D2.5, "The EU-SEC Framework".

The governance processes presented in the next sections are the change management and the complaint management processes. The change management process is used for the management of any changes that may be required and which will potentially affect the framework's assets. On the other hand, the complaints management process aims at managing and resolving complaints that are issued about the framework and which are handled by the corresponding governance bodies. Both processes are defined and take place as part of the "Govern" step of the framework's lifecycle.

4.1 GOVERNANCE ASSETS

The assets of the multi-party recognition framework that are to be governed are:

- the "Multi-party recognition principles, criteria and requirements", that are preconditions that different certification and compliance schemes need to fulfil to be considered for recognition (see Deliverable D1.4),
- the "EU-SEC requirements repository", that stores the security, privacy and auditing requirements from international standards, national/regional laws and regulations that are mapped against the CSA CCM (see Deliverable D1.2),
- The "governance body", that set the rules and requirements for developing, maintaining and operating the EU-SEC recognition framework.
- The "framework's realization activities" and roles and responsibilities of the stakeholders (see Chapter 3) that define the operation of the overall framework

The former assets are considered in the governance structure as they constitute core elements that are placed under evaluation, comparison and processing from the framework's mutual recognition activities. Hence, any change management or notification activities required in accordance to respective changes and updates in the cloud security certification landscape will influence these assets. The following figure shows the overview of governance structure of the multiparty recognition framework with main assets, key roles involved and main governance processes addressed in this chapter.

Figure 12: Governance structure graphical illustration

4.2 ROLES AND RESPONSIBILITIES

The four main stakeholders introduced in Chapter 3.1.2 are also the key stakeholders for governance of the multi-party recognition framework. In this chapter, the description of the roles and responsibilities of these four stakeholders focus on their activities in the governance processes:

- EU-SEC governance body
- Scheme Owners / Authority

- Authorized Auditors
- Cloud Service Providers

The **EU-SEC governance body** operates and maintains the multi-party recognition framework (see 3.1.2), and it is responsible for the implementation, management and update of all defined governance processes and assets. It coordinates with all relevant stakeholders, to identify and collect input to improve the framework, as for instance, changes in cloud certification/compliance schemes, laws, regulations and standards relevant to cloud computing.

In more detail, main responsibilities of the governance body are to:

- Identify new standards or certification schemes that are relevant to the governance framework (e.g. through a dedicated monitoring expert group)

The governance body is responsible for regular identification and collection of new cloud certification / compliance schemes, laws, regulations and standards from the scheme owners or governments. Therefore, regular contact with scheme owners is desired to understand the current state of art cloud certification / compliance schemes, standards, regulations and laws and future market trends of cloud certification / compliance schemes.

- Request expert opinions

The EU-SEC governance body can request opinion on technical matters from a subject matter advisory group. For instance, to decide on the incorporatation of a new compliance schemes into the framework, the EU-SEC governance body can request consultation from the authorized auditors.

- Publish and communicate framework changes to relevant stakeholder

The EU-SEC governance body shall publish and inform the relevant stakeholder of any changes/updates in the framework.

- Receive new requests to add a compliance scheme to the framework

If scheme owners or other authorities want to add their compliance scheme to the framework, the EU-SEC governance body is the single point of contact that receives such a request. The EU-SEC governance body is responsible to triggering the framework's evaluation processes in order to assess the integration of the new scheme into the framework.

The **scheme owner** or **authority** is either the stakeholder that owns the certification or compliance schemes (e.g. AICPA, BSI, etc.) or the authority that dictates the national/sectorial requirements. It publishes new and updates existing security and privacy requirements and/or certification/compliance schemes or, laws, regulations and standards. The scheme owner/authority can initiate the process for having its scheme included under the EU-SEC framework umbrella. The scheme owner as one of the operating parties (see 3.1.2) represents an essential actor to the success of the EU-SEC framework.

Although the **authorized auditors** are not directly participating in the governance activities, they provide consultation and feedback over any activities within governance that are operated by the EU-SEC governance body. Furthermore, the authorized auditors keep themselves informed about the latest updates on the multi-party recognition framework.

Cloud Service Provider might be affected by changes of the EU-SEC framework, and thus should be informed about the latest updates. In this context, CSPs maintain an open communication channel with the EU-SEC governance body in order to either access the mutually recognized certifications in the existing EU-SEC repository or be informed about certifications undergoing mutual recognition activities and expected results.

4.3 CHANGE MANAGEMENT PROCESS

The change management process covers the procedure for the implementation of changes to the framework and its components. The objective of the change management process is to formulate and regulate the proper assessment, implementation and communication of changes.

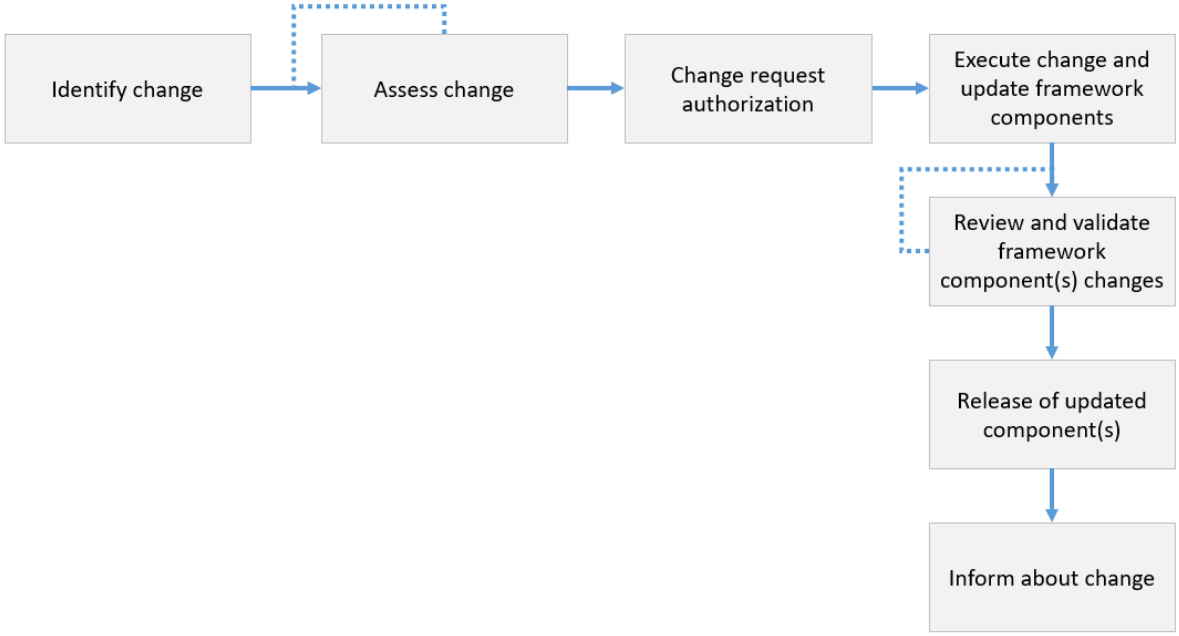

Figure 13: Multiparty recognition framework change management process activity diagram

Activities overview:

1. ***Identify change***

   The dynamic certification landscape shall be continuously monitored by the EU-SEC governance body (e.g., by a dedicated working group) and will provide any relevant input for a necessary change to the change management process. New certifications and compliance schemes and changes to laws, regulations, standards and certifications and compliance schemes are identified. When changes are identified, the governance body is responsible to trigger the change management process. All stakeholders of the EU-SEC framework can also identify and report changes in the requirements of certification and compliance schemes, laws, regulations and standards to the governance body or the working group in charge.

2. ***Assess the impact and value of changes and their effects on the whole framework***

Upon identification of a potential change, an assessment shall be conducted to identify as precisely as possible the parts/sections of the designated component(s) (e.g. domains, requirements of EU-SEC requirements repository) that are impacted by the new input.

After the assessment of the change, a decision is made whether the change is implemented or not. For the desired change, the governance body is responsible to request the change in order to initiate the approval for the implementation.

3. Change request authorization

A Request for Change (RfC) is created and documented along with assessment results and justified with the rationale of the proposed change. The RfC is approved by the change management group before it is executed.

4. Execute change and update framework components

The EU-SEC governance body is responsible for updating (addition, suppression, modification) the framework's components based on the change request and with respect to the identified changes at the underlying certification schemes and their corresponding security, privacy or auditing requirements. After a change is approved, the EU-SEC governance body identifies the relevant resources to implement it. In addition to the EU-SEC governance body, dedicated expert groups may be involved in the updating process. Support and consultation from other stakeholders can be requested.

5. Review and validation of component(s) changes

During this activity, changes to updated framework components and related elements are reviewed and validated after the requested change has been implemented. The EU-SEC governance body compares the updated framework components with the previous version to determine and confirm whether the changes are successfully implemented as planned. Additionally, the governance body is responsible for the validation of the change, with support by subject matter experts (e.g., a dedicated working group), the scheme owners or other stakeholders.

6. Release of updated component(s)

The output of the update process will involve an updated documentation of the frameworks' components.

7. Inform about changes

After the change has been implemented the governance body is obligated to inform the stakeholders about the updated framework and details about the change. Such action may lead to the activation of the execution process of the framework, that is, to trigger a transition from the "Govern" to "Execute" step of the multiparty recognition lifecycle (e.g., if the change affects the EU-SEC repository of compliance schemes' requirements).

Table 14. The multiparty recognition process card: the inputs, the activities and the outputs.

Change Management Process	
Inputs	- New compliance or certification schemes or changes to laws, regulations, standards or compliance and certification schemes, that are part of the framework - Other change requests triggered based on provided input from MPRF internal or external to the MPRF cloud-based stakeholders
Activities	1. Identify change 2. Assess the impact, effects and value of changes to the multiparty recognition framework 3. Change request authorization 4. Execute change and update framework component(s) 5. Review and validate component(s) changes (e.g., by change management committee) 6. Release of updated component(s) 7. Inform about the changes
Outputs	- Result of the change assessment and corresponding updates of the framework

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 15. The Change management process activities' mapped to roles and responsibilities.

Change Management Process		**Activities**						
		#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**
Roles	EU-SEC Governing Body	A R	A R	A R	A R	A R	A R	A R
	Compliance Scheme Owners	R	C	-	C	C	I	-
	Authorized Auditors	R	C	C	C	C	I	-
	Auditees (the Cloud Service Providers)	R	C	-	-	-	I	-

The Change management process activities and the underlying sub-activities are described in more detail in the subsections below.

4.3.1 ACTIVITY #1: IDENTIFY CHANGE

Process change and initialize the change management process.

Table 16. The activity #1 card to detail sub-activities, inputs and outputs.

Activity #1	
List of the activities: *1# Stakeholder to submit an identified change, e.g., new compliance or certification schemes or changes to laws, regulations, standards or compliance and certification schemes, that are relevant for the framework.* *2# EU-SEC governance body generates the Request ID for the submission, with a description of the request and the submitter's (the stakeholders' representative) contact details and confirms receipt with the submitter (within two business days at latest).* *3# When the request is a new compliance scheme that shall be added to the framework the EU-SEC governance body is responsible to trigger the Multiparty Recognition Framework Process (see chapter 3.2) – in this case the change management process ends here.* *4# EU-SEC governance body to gather the relevant documents from the submitter or any other relevant party (within one week).* *5# If relevant: Change requestor to submit the requested documents (within one week).* *6# Once the initial set of documentation is received and verified for its completeness, pass the request to the activity #2 (within two business days at latest), or close the incomplete request.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# A change by a stakeholder in any verbal method 2# Change management system 3# EU-SEC governance body	1# Request ID (e.g., Unique identifier) with the description of the request and contact details 2# The submitted change (e.g. changes in the compliance scheme's security and auditing requirements, and governance model description)

4.3.2 ACTIVITY #2: ASSESS THE IMPACT, EFFECTS AND VALUE OF CHANGES TO THE MULTIPARTY RECOGNITION FRAMEWORK

The change is assessed in the impact, effect and value to the multiparty recognition framework.

Table 17. The activity #2 card to detail sub-activities, inputs and outputs.

Activity #2	
List of the activities: 1# *EU-SEC analyst to confirm receipt with the submitter (within two business days at latest after receiving the Activity #1 input) that the assessment activity has started.* 2# *EU-SEC analyst identifies what specific components of the framework are affected by the change.* 3# *EU-SEC analyst analyses the documents describing the change in co-operation with the relevant parties that the MPRF framework criteria and principles are met on a "high-level".* 4# *EU-SEC analyst to make preliminary request acceptance (preliminary Dis-/Approved) decision* 5# *Pass the request to the activity #3 to request approval, or close the rejected and/or incomplete request.*	
Inputs	**Outputs**
1# Activity #1 outputs 2# Change management system	1# Preliminary request acceptance and respective documentation

4.3.3 ACTIVITY #3: CHANGE REQUEST AUTHORIZATION

The change is submitted for authorization and approval by the change approval group

Table 18. The activity #3 card to detail sub-activities, inputs and outputs.

Activity #3	
List of the activities: 1# *EU-SEC analyst files a request for change (RfC) with the respective documentation of the change assessment and rationale for the preliminary approval.* 2# *EU-SEC change management group evaluates the request for change with the respective documentation.* 3# *EU-SEC change management group can request further information from the subject matter experts.* 4# *EU-SEC change management group to make final change approval (final Dis-/Approved) decision.* 5# *Pass the request to the activity #4*	
Inputs	**Outputs**
1# Activity #2 outputs 2# Change management system	1# Final change approval

4.3.4 ACTIVITY #4: EXECUTE CHANGE AND UPDATE FRAMEWORK COMPONENT(S)

The change is executed and the changes are applied to all the relevant framework components.

Table 19. The activity #4 card to detail sub-activities, inputs and outputs.

Activity #4	
List of the activities: 1# *EU-SEC analyst receives the final change approval.* *2# EU-SEC analyst to apply changes to the relevant areas or MPRF components* *3# EU-SEC analyst to prepare an updated version of the affected framework components.* *4# Pass the change results as well as the updated component(s) version to the activity #5 for review.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #2 and #3 outputs 2# Change management system	1# Documented results of applied changes 2# Updated version of the affected framework components

4.3.5 ACTIVITY #5: REVIEW AND VALIDATE COMPONENT(S) CHANGES

EU-SEC Governance Body reviews and validates the updates of the framework components

Table 20. The activity #5 card to detail sub-activities, inputs and outputs.

Activity #5	
List of the activities: 1# *EU-SEC analyst to send the change results as well as the updated version of the framework to the EU-SEC change management group for review.* *2# EU-SEC change management group to compare the results and the updated version of the framework with the previous version to validate the change.* *3# EU-SEC change management group to consult other stakeholders for the validation.* *4# EU-SEC change management group to approve the updated version of the framework components.* *5# Pass the updated version to the activity #6 for the release.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #4 output 2# Change management system	1# Final version of updated framework components

4.3.6 ACTIVITY #6: RELEASE OF UPDATED COMPONENT(S)

EU-SEC Governance Body releases the updated version of the framework components and makes it available for all stakeholders.

Table 21. The activity #6 card to detail sub-activities, inputs and outputs.

Activity #6	
List of the activities: *1# EU-SEC governance body to prepare external documentation about the updated version of the framework components.* *2# Pass the external documentation about the updated version of the framework components to the activity #7 for the communication to the stakeholders.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #5 output 2# Change management system	1# External documentation of the updated documentation of the framework components

4.3.7 ACTIVITY #7: INFORM ABOUT THE CHANGES

EU-SEC governance body communicates the updated version of the framework components to the relevant stakeholders.

Table 22. The activity #7 card to detail sub-activities, inputs and outputs.

Activity #7	
List of the activities: *1# EU-SEC governance body to release notification about the change and the updated framework components on the EU-SEC website.* *2# EU-SEC governance body to send an email to the stakeholders that are on the stakeholder list to inform about the change and the updated framework components.* *3# Complete and archive the change.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #6 output 2# Change management system	1# Awareness for the change and the updated version of the framework components

4.4 COMPLAINT MANAGEMENT PROCESS

The complaint management process aims at structuring and organising the constructive processing of requests and complaints about the framework or the overall process. All stakeholders involved in the multiparty recognition framework need a channel to send requests or complaints about the framework or the process.

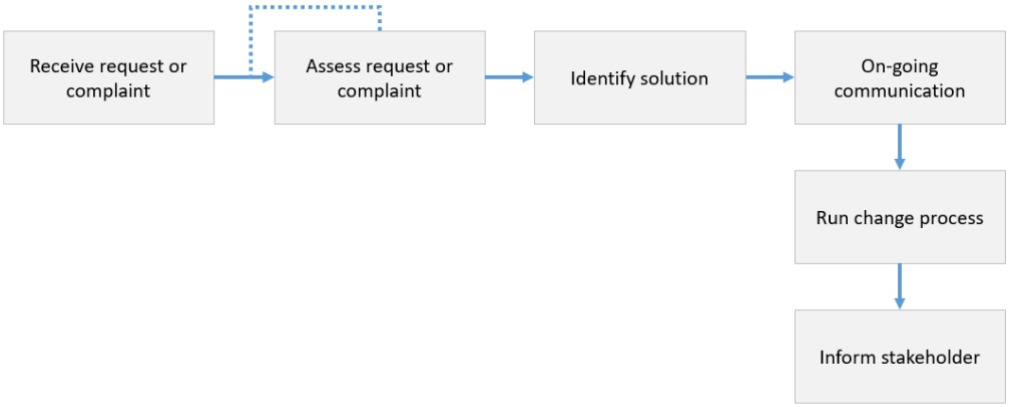

Figure 14: Complaint management process activity diagram

Activities overview:

1. ***Receive request or complaint***

   The complaint management process is triggered by the receipt of a request or a complaint from a stakeholder with respect to the multiparty recognition framework activities. For instance, complaints might be issued in relation to the multi-party recognition criteria and requirements, the security requirements repository and the mapping results, or the qualification of the recognized schemes. The EU-SEC governance body acknowledges the complaints' initiator and that a complaint has been received. Meanwhile, the initiation of the activities predefined in the complaint management process will be triggered.

2. ***Assess validity, relevance and impact for the whole framework***

   The complaint management process assesses the validity of the received complaint statements and their relevance and impact on the multi-party recognition framework's components. The assessment result will support the EU-SEC governance body to make decisions on whether and how further actions shall be taken.

3. ***Identify solution for the request or complaint***

   The EU-SEC governance body is responsible for developing a solution with support by dedicated working groups to address the issued complaints.

4. ***On-going communication***

The EU-SEC governance body shall maintain regular communication with the complaint initiators and inform them on the complaint handling progress, while the necessary assessments and solution implementations takes place.

5. Run change process

When a change is required to be implement the EU-SEC governance body creates an RfC and initiates a solution for implementation into the multiparty recognition framework through the change management process.

6. Inform stakeholder

Upon resolution of the issued request the governance body shall inform the initiator of the complaint about the solution details, and any updates applied to the multi-party recognition framework's assets.

Table 23. The complaint management process card: the inputs, the activities and the outputs.

Complaint Management Process	
Inputs	- Formal request or complaint about the framework or one of the framework components - MPRF framework criteria, principles and requirements
Activities	1. Receive request or complaint 2. Assess validity, relevance and impact for the multiparty recognition framework 3. Identify solution for the request or complaint 4. On-going communication 5. Run change process 6. Inform stakeholder
Outputs	- Result of the complaint assessment and corresponding updates of the framework

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 24. The Complaint management process activities' mapped to roles and responsibilities.

Change Management Process		**Activities**					
		#1	**#2**	**#3**	**#4**	**#5**	**#6**
Roles	EU-SEC Governing Body	A R	A R	A R	A R	A R	A R
	Compliance Scheme Owners	-	C	C	I	I	I
	Authorized Auditors	-	C	C	I	I	I
	Auditees (the Cloud Service Providers)	-	-	-	I	-	I

The Complaint management process activities and the underlying sub-activities are described in more detail in the subsections below.

4.4.1 ACTIVITY #1: RECEIVE REQUEST OR COMPLAINT

Process request or complaint and initialize the complaint management process.

Table 25. The activity #1 card to detail sub-activities, inputs and outputs.

Activity #1	
List of the activities: *1# Stakeholder to submit a request or complaint (e.g., complaints might be issued in relation to the multi-party recognition criteria and requirements, the security requirements repository and the mapping results, or the qualification of the recognized schemes)* *2# EU-SEC governance body generates the Request ID for the request, with a description of the request and the submitter's (the stakeholders' representative) contact details and confirms receipt with the submitter.* *3# EU-SEC governance body to gather the relevant documents from the submitter or any other relevant party to be able to assess the request.* *4# If relevant: requestor to submit the requested documents.* *5# Once the initial set of documentation is received and verified for its completeness, pass the request to the activity #2, or close the incomplete request.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# A request or complaint by a stakeholder in any verbal method 2# Complaint management system 3# EU-SEC governance body	1# Request ID (e.g., Unique identifier) with the description of the request and contact details 2# The request or complaint and the respective documentation

4.4.2 ACTIVITY #2: ASSESS VALIDITY, RELEVANCE AND IMPACT FOR THE WHOLE FRAMEWORK

The request is assessed for validity, relevance and impact to the multiparty recognition framework.

Table 26. The activity #2 card to detail sub-activities, inputs and outputs.

Activity #2	
List of the activities: 1# *EU-SEC analyst to confirm receipt with the submitter that the assessment activity has started.* 2# *EU-SEC analyst identifies what specific components of the framework are affected by the request.* 3# *EU-SEC analyst analyses the documents describing the request in co-operation with the relevant parties to decide whether the complaint is valid and relevant as well as what impact the request has on the framework and the components.* 4# *EU-SEC analyst to file a preliminary request acceptance decision.* 5# *EU-SEC analyst to request for acceptance of the request from the EU-SEC complaint management group.* 6# *EU-SEC complaint management group to accept the complaint.* 7# *Pass the request to the activity #3 to initiate the resolution of the request, or close the rejected and/or incomplete request.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #1 outputs 2# Complaint management system	1# Complaint acceptance and respective documentation

4.4.3 ACTIVITY #3: IDENTIFY SOLUTION FOR THE REQUEST OR COMPLAINT

The EU-SEC governance body finds a solution for the request or complaint.

Table 27. The activity #3 card to detail sub-activities, inputs and outputs.

Activity #3	
List of the activities: 1# *EU-SEC analyst to consult relevant stakeholder to identify whether a improvement is required.* 2# *EU-SEC analyst to identify a solution for the request.* 3# *EU-SEC analyst to document the solution in a complaint resolution plan.* 4# *EU-SEC complaint management group to review and approve the complaint resolution plan.* 5# *Pass the complaint resolution plan to the activity #4.* *Total pass-through time 2 weeks at max.*	
Inputs	**Outputs**
1# Activity #2 outputs 2# Complaint management system	1# Final complaint resolution plan

4.4.4 ACTIVITY #4: ON-GOING COMMUNICATION

The requestor is continuously informed about the progress of the complaint management process.

Table 28. The activity #4 card to detail sub-activities, inputs and outputs.

Activity #4	
List of the activities: 1# *EU-SEC governance body receives final complaint resolution plan.* 2# *EU-SEC governance body to confirm receipt with the submitter that a request resolution plan has been developed and that the change management process will be initiated.* 3# *EU-SEC governancy body to trigger change management process.*	
Inputs	**Outputs**
1# Activity #3 outputs 2# Complaint management system	1# Notification to the requestor that the request has been solved

4.4.5 ACTIVITY #5: RUN CHANGE PROCESS

EU-SEC Governance Body triggers the change management process (see chapter 4.3) to execute the request resolution plan.

Table 29. The activity #5 card to detail sub-activities, inputs and outputs.

Activity #5	
List of the activities: 1# *EU-SEC governance body to trigger the change management process (see chapter 4.3) with the request resolution plan as input.* 2# *EU-SEC governance body to document the successful execution of the change management process.*	
Inputs	**Outputs**
1# Activity #3 output 2# Complaint management system	1# Documentation about the successful execution of the change management process

4.4.6 ACTIVITY #6: INFORM REQUESTOR

EU-SEC Governance Body communicates the resolution of the request or complaint to the submitter.

Table 30. The activity #6 card to detail sub-activities, inputs and outputs.

Activity #6	
List of the activities: *1# EU-SEC governance body to release notification about the successful resolution of the request or complaint to the submitter.* *2# Complete and archive the request.*	
Inputs	**Outputs**
1# Activity #5 output 2# Complaint management system	1# Notification of the resolution of the request or complaint

4.5 INTERDEPENDENCIES OF THE LIFECYCLE PROCESSES

As mentioned before, multiparty recognition is defined via a 3-step lifecycle along with the corresponding processes and activities within each individual step. In this section, we present the interdependencies that exist between the framework's processes in relation to its operation, governance and management of assets.

Based on the lifecycle diagram (Figure 5 in section 3.1.1), a transition between each pair of the lifecycle steps is defined, that is from:

1. "Evaluation" to "Execution",
2. "Execution" to "Governance",
3. "Governance" to "Evaluation".

The dependency between the first pair of steps is illustrated in chapter 3, where activities 2 and 4 of the multiparty recognition process are used to evaluate the respective assets that are to be processed during the framework's operation. If evaluation criteria are met, a transition toward the execution of the remaining operational activities is initialiazed.

The second pair of the lifecycle reflects the execution activities of the multiparty recognition framework, also introduced in chapter 3. These activities and their outputs are continuously controlled during and after their execution has completed. During execution all activities and their respective outputs are monitored and managed by the dedicated governance bodies with defined roles and responsibilities. All activities' output documentation is recorded and archived at the EU-SEC repository, where it is maintained by the governance processes, such as, the change management process.

The transition from the "Govern" step and towards the next steps of "Evaluation" and "Execute" can take place by a triggering event that is initialized by the respective change management process defined within the "Govern" step. The event is provided as input to the framework's execution process (Figure 8 in section 3.2) and represents occurred changes to one of the framework's assets such as the "EU-SEC requirements repository" (and hence the included compliance schemes' requirements) or the "Multi-party recognition principles, criteria and requirements".

In the case of an established change to the "EU-SEC requirements repository", the change management process shall trigger the framework's execution process to initialize. The corresponding compliance schemes' requirements that are affected by the change are re-evaluated, and the established multiparty recognition scheme updated. Re-evaluation requires

that the identified deltas between the affected compliance schemes and their requirements are re-assessed, compared and finally validated for multiparty recognition.

Similarly, an implemented change to the framework's multi-party recognition principles, criteria and requirements is affecting the framework's operation and specifically its activity two "Request Assessment and Acceptance", as part of the lifecycle's "Evaluate" step. In fact, any updates to the multi-party recognition principles, criteria and requirements shall be reflected upon the framework's execution process (i.e., respective evaluation activity two illustrated in chapter3 and Figure 8), since any candidates of compliance schemes submitted for multiparty recognition, have to adhere to the updated criteria and requirements.

Any changes to the remaining assets of the framework, such as the "governance bodies, roles and responsibilities" and the "framework's realization activities" are handled within the "Govern" step of the lifecycle, impacting the relevant documentation. Likewise, within the "Govern" step of the lifecycle, the complaint management process is tightly connected with the change management process, with the former initializing a change request that triggers the latter.

5 CONCLUSIONS

The outcome of this work is the framing into a model of the multiparty recognition concept, which allows for multiparty recognition activities to be performed at an unambiguous, organized and systematic manner.

The suggested model should to able apply the key framework principles, crtieria and requirements (as described in D1.4.) and therefore guarantee:

1. the manageability and scalability of the proposed framework architecture to rapidly adapt to the evolving cloud security certification landscape,
2. the repeatability and consistency of expected multiparty recognition results,
3. the promoted awareness and trust towards the multiparty recognition works among the involved stakeholders.

The framework's scalability is inherited within its structure and modeling components, that is, its well-defined matrices and information flow diagrams. New activities, processes, roles and responsibilities of stakeholders can be defined or existing can be redefined, also with a higher level of granularity -if required-, and can be easily integrated into the existing architecture.

The systematic organization of activities into hierarchical and ordered work flows, supported by the detailed input/output documentation of the underlying processes ensure the consistency, progress tracking and procedural soundness of the expected multiparty recognition activities and content produced.

Clearly, the described interrelationships between the involved stakeholders and the defined association of roles and responsibilities of each stakeholder per required activity, minimises ambiguous interpretations and miscommunication. In addition, transparency and awareness of the framework's activities is increased among stakeholders each step along the multiparty recognition process, hence encouraging trust. This is achieved by the required documentation of the input/output elements per process that become available to the relevant stakeholders, as well as the supporting publication and notification activities that are defined within the framework's governance structure.

From a different standpoint, it is important to note that the current approach for multiparty recognition is based solely on a theoretical model. While this is the case, scheduled pilot exercises, which shall take place in work package four of the project, are expected to provide useful feedback from the empirical exercises and respective derived conclusions and lessons

learnt. Therefore, any invalidities that may be found between the theoretical and real-life requirements for multiparty recognition of certification/compliance schemes, can and will be successfully bridged.

To this end, future enhancements and possibly a better refined version of the multiparty recognition framework and its components is expected to take place within [6], which shall consider the new knowledge and experiences acquired from the pilot works.

BIBLIOGRAPHY

[1] EU-SEC, "D1.4: Principles, criteria and requirements for a multiparty recognition and continuous auditing-based certifications," [Online]. Available: https://cdn0.scrvt.com/fokus/15cde3d2c6267d70/82ed8f0cc69c/D1.4-multiparty-recognition-V-1.0.pdf. [Accessed 10 12 2018].

[2] EU-SEC, "D2.4: EU-SEC Framework," [Online]. Available: https://cdn0.scrvt.com/fokus/c375da367703d004/e78fe75a3771/9EU-SEC-Framework---Draft.pdf. [Accessed 10 12 2018].

[3] EU-SEC, "D2.5: EU-SEC Framework (Version 2)," 2018. [Online]. [Accessible in Q2 2019].

[4] EU-SEC, "D1.2: Security and Privacy Requirements and Controls," [Online]. Available: https://cdn0.scrvt.com/fokus/ec7f2111f873547b/e2acb6781bc1/D1.2-Security-and-privacy-requirements-and-controls-V1.2.pdf. [Accessed 10 12 2018].

[5] EU-SEC, "D1.3: Auditing and Assessment Requirements V 1.0," [Online]. Available: https://cdn0.scrvt.com/fokus/76bc9febc2cdbd61/9f38925d56b3/D1.3-Auditing-and-assessment-requirements-V1.0.pdf. [Accessed 10 12 2018].

[6] EU-SEC, "D2.3: Privacy Code of Conduct V 1.0," [Online]. Available: https://cdn0.scrvt.com/fokus/1911860fecc21cff/a71af483c4b0/D2.3_Privacy_Code_of_Conduct_v1.0_Final.pdf. [Accessed 10 12 2018].

[7] Cloud Security Alliance, "CCM Mapping Methodology v1.0.," 2018.

APPENDIX A

REQUIREMENTS COMPARISON ANALYSIS

Each requirement was thoroughly analysed and mapped to one or more CSA CCM requirements that are available within each CCM control domain. The mapping produced one-to-one or one-to-many relationships between these requirements and CCM requirements, depending on the identified level of detail, thematic scope and security objectives of the compared semantics.

The gap analysis resulted in three types of relationships:

- No gap: the requirement was adequately covered by the CCM requirement(s)
- Full gap: the requirement couldn't be covered by any of the CCM requirement(s)
- Partial gap: the requirement was partially covered by the CCM requirement(s) and left some gaps.

The outcome of the requirements collection provided 509 requirements that were mapped to the CCM controls (as shown in Figure 15).

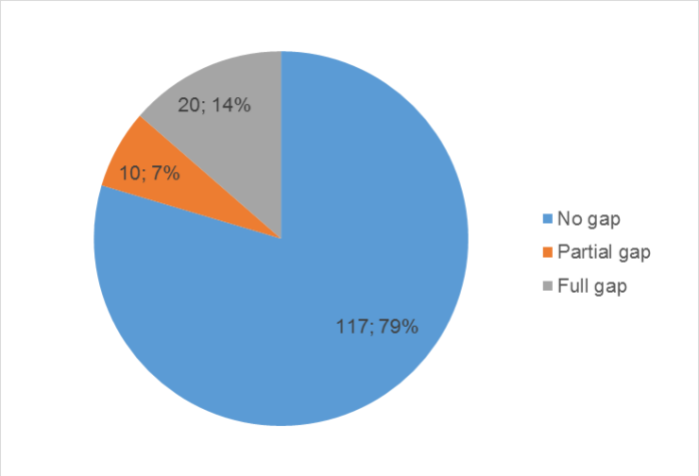

Figure 15: Requirements mapping to CCM gap level

Mapping to CCM: "No gap" cases

The majority of the mapped requirements (79%) resulted in a "No gap" case, which shows that there is considerable level of overlap between different information security frameworks and standards. This is an important empirical validation of our assumption that there are

commonalities between the requirements/controls objectives in these frameworks and standards.

As a result, several cases confirmed that it was possible to map the requirements from diverse input sources to the same CCM control as "No gap". In other words, one requirement from the CCM covered multiple semantically equivalent requirements from diverse sources. This case demonstrated that the CCM could serve as a common comparability tool between diverse input sources or certification schemes and it can be directly used for the EU-SEC requirements and controls repository.

A "No gap" case where the requirements from diverse input sources were successfully covered with the same CCM security control also demonstrated a direct common ground (overlap) between certification/compliance schemes' security controls that could be used for multiparty recognition.

Mapping to CCM: "Full and partial gaps" cases

A "Full gap" case was found in 14% of the requirements, which could not be linked in any way to the CCM controls. It was not possible to determine either the CCM domain nor the control.

7% of requirements were partially mapped to the CCM controls ("Partial gap") indicating that the CCM controls only partially covered the requirements because they provided a lower security level (e.g., CCM was more generic, included broader security objectives or more loose parameters) or that they included diverse semantics than those of the compared requirements.

Both gap cases ("Full gap", "Partial gap") showed a need to establishing a process for creating new controls or amending and updating the existing controls (Figure 2), which would fulfil the missing requirements. By covering the gaps, the common set of controls could better apply to diverse input sources and could increase the possibility that the same control(s) would ensure and contribute to multiparty recognition.

APPENDIX B

GENERAL AUDIT REQUIREMENTS

The deliverable D1.3 collects requirements related to the auditing as applicable to the cloud service security control environment. We focused on the auditing requirements set to third-parties providing certification or attestation services. We also investigated the terms "acceptable / sufficient evidence" and addressed the question on "what is meant to be considered an acceptable evidence during an evaluation?". The analysis had shown that the auditing processes converge to ISO 27006/27007 and ISAE 3000 approaches, which are widely used auditing standards for providing auditing services.

More specifically, the ISO 27000-family of standards focus on and support the auditing of information security management systems (ISMS) based on ISO 27001. In practice, both are suitable to guide the auditing of cloud service security requirements. The most common use of ISO27001 is companies seeking for a certification or compliance assessments, to, e.g., benchmark the current status of their cloud services' security control environments.

The ISAE 3000 standard on the other hand is used by certified public accountants to conduct compliance assessments, to provide an attestation on the control environment, specifically on the suitability of the design (type 1 audit) of controls to meet the selected requirements (e.g. Trust Services Criteria from the SOC 2 scheme) on a specified date or additionally on their operating effectiveness throughout a specified period of time (type 2 audit).

It can be concluded that:

Both ISO 27000-family and the ISAE 3000 standard can be used to provide the compliance assessment for cloud service security requirements.

THE AUDIT FIRM AND AUDITOR REQUIREMENTS

As stated earlier, the ISAE 3000, ISO 27006 and ISO 27007 standards specify the mainstream auditing requirements in the context of cloud service security control environment's compliance assessment. These standards provide both normative requirements and best practices for evaluation processes, for example. The key difference is that:

Companies providing certification services on ISO, shall be accredited as the certification body by a member of the national accreditation organisation[5].

In order to issue Third Party Attestation Reports according to ISAE 3000 the audit firm needs to be registered as an accounting firm according to the respective national provisions.

The above usually enforce that the audit firms have established certain minimum standards regarding, for instance, their quality management system, means for the execution and documentation of engagements as well as processes to conduct risk and independence considerations or the qualification of personnel.

To structure the auditing requirements for an audit firm and auditors, we compared the auditing schemes by using ISO/IEC 27006[6] standard as the baseline requirement. For example, ISO/IEC 27006 chapters from 4 to 7 specify the requirements for an auditor, who is to perform the auditing of the cloud service security control environment. Our evaluation in the D1.3 shows that the stated mainstream auditing standards require competency on the cloud service industry risk and control landscape. In addition, the audit engagement must be led by an accredited auditor by the certification scheme. The statutory requirement for the lead auditor in practise is not interchangeable between different schemes and likely result in situations, where all the schemes must have their representative auditor in charge of the auditing engagement. In the multiparty auditing context, we can summarise the auditor requirements as follows:

The team executing the auditing engagement in the multiparty recognition context shall meet all the auditing competence requirements dictated by each of the compliance scheme(s) in the scope of the engagement.

These requirements may target for instance the qualification of the auditor, the structure and content of the corresponding audit report or other specified provisions. Thus:

The auditing team shall have sufficient knowledge on cloud service industry, risks and control landscape. The knowledge can be demonstrated by holding relevant certifications (e.g. CCSK[7]*, CCSP*[8]*) or other relevant training.*

[5] E.g. FINAS in Finland (www.finas.fi), UKAS (www.ukas.com) in the United Kingdom, ACCREDIA in Italy.
[6] It should be noted that ISO/IEC 27006 is based on ISO/IEC 17021, to which information security management aspects are added.
[7] https://cloudsecurityalliance.org/education/ccsk/#_overview
[8] https://www.isc2.org/Certifications/CCSP

THE AUDITING PROCESS REQUIREMENTS

A comparison of the auditing process between ISAE 3000 and ISO/IEC 27007 was conducted by using an ISO/IEC 19011 standard as the baseline. ISO/IEC 27007 is closely related to ISO/IEC 19011 "Guidelines for auditing management systems". Each of the process steps were analyzed separately.

It was concluded that the audit process at a practical level is fairly similar between the two standards. However, a difference can be found in audit process step 2: Preparing the audit activities where ISAE 3000 type 2 audit amends the ISO auditing requirement:

> *The auditee's control(s) mapped to the security requirement of the EU-SEC requirement repository (for the multiparty recognition), shall be tested against evidence demonstrating the operating effectiveness throughout a specified period of time, whenever possible.*
>
> The audit plans in the multiparty context shall meet the requirements dictated by each of the compliance scheme(s) in the scope of the engagement.

Figure 16: Standard steps of an audit process with mapping to ISO/IEC 27007.

When conducting the review of the documentation, the collection of non-technical evidence and the collection of technical evidence should be done as described in D1.3. It should be

noted, that professional judgement and professional skepticism of the auditor plays a major role during this phase and as such competence of the auditor must be adequate, elaborated earlier in this chapter.

Preparing and distributing the audit report should include the results, quality control and an action plan to handle nonconformities. Report should be constructed using understandable structure.

The content of the audit report shall comply with requirements stated by the relevant scheme (e.g. ISAE 3000, ISO27007, BSI C5 and CSA STAR Certification and Attestation). Quality assurance of the audit report shall be conducted and the compliance scheme owner or other relevant stakeholders (e.g. IAASB for ISAE 3000) shall be consulted, if required.

When conducting the maintenance audit, all the nonconformities should be re-audited according to the action plan to mitigate them.

The non-conformities shall be addressed by maintenance audit according to an action plan set in place at the time of the audit completion, elaborated in more details in chapter 2.2.4.

Completing the audit shall follow the detailed requirements of ISO/IEC 27007 and ISAE 3000 respectively. It was noted that evidence and report retention period vary greatly between studied requirements.

Minimum of three (3) years shall be used as the evidence and report retention period unless otherwise required by the compliance schemes in the scope of the engagement[9].

NONCONFORMITY HANDLING REQUIREMENTS

In order to achieve compliance, ISO-based frameworks require the non-conformities to be addressed by the auditee according to the action plan set in place at the time of the audit completion.

In support of the practitioner's conclusion, ISAE 3000 needs the auditor to show any severe non-conformity (also: "exception", "deviation" or similar) in the attestation report. However, it does not require any specific follow-up activies neither from the auditor nor the auditee, after a completed audit. Furthermore, there are no surveillance (or maintenance) audits but every time the auditor will set up an entirely new audit, including an updated testing strategy.

[9] Please check EU-SEC D1.3 "Auditing and Assessment Requirements" Section 3.4.5 for more details.

However, it is good practice to provide the auditee with a list of minor issues, ideally including recommendations on how to remediate those.

The pass of audit can be used based on qualified auditor's analysis or opinion by both auditing standards, provided the severe non-confirmities have been addressed.

To demonstrate the specifics of handing nonconformities in the context of multiparty recognition, let us assume a case where compliance schemes 1, 2 and 3 have some overlapping security requirements. The diagram below (Figure 17) shows that in the region 1∩2∩3 there is an overlap of all compliance schemes, and a smaller set of overlaps exist also within regions 1∩2, 1∩3 and 2∩3.

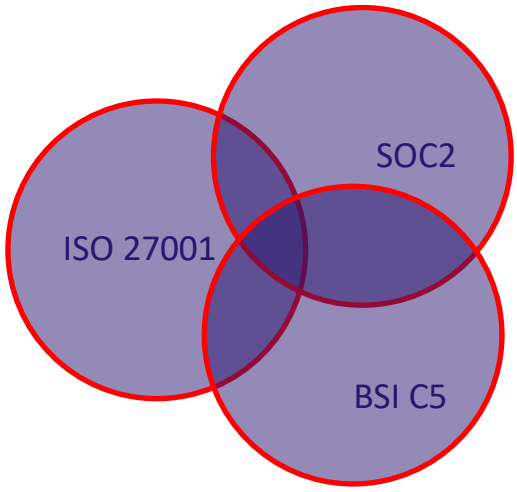

Figure 17: The Venn Diagram to illustrate the intersection of security requirements

The three outer regions above are specific to each compliance scheme. These compliance schemes contain requirements, to which the cloud provider's controls are mapped. During the audit, if controls are found not to be suitably designed/implemented or not operating effectively, non-confomities are to be noted. The non-conformity may lead to the situation where an audit may be considered as failed by one of the compliance schemes. In case the control resides in the overlapping region, all the compliance schemes are affected at the same time, but the actual impact to individual scheme may vary.

Following the logic of the multiparty recognition, a non-conformity in one of the connected schemes may automatically lead to a non-conformity within other scheme. These need to be incorporated into the respective reports, too.

Thus, as a requirement for the multiparty recognition:

Any non-conformities within the connected domain shall be reported by the auditor and shared with the connected compliance schemes (and/or underlying standards), and evaluated for their impacts. The final conclusion of the non-conformity's severity shall be consolidated (feedback loop) and addressed accordingly.