EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D4.5 CONSOLIDATION AND ANALYSIS – THE PILOT RESULTS

VERSION 1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 31.1.2019	DELIVERY DATE: 10.2.2019
AUTHOR: CSA	PARTNERS CONTRIBUTED: SI-MPA, MFSR, SixSQ, Fabasoft, NIXU, PwC
DISSEMINATION LEVEL:* PU	NATURE OF THE DELIVERABLE:** R

INTERNAL REVIEWERS: Fabasoft, Fraunhofer

*PU = Public, CO = Confidential

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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731845

EXECUTIVE SUMMARY

The European Security Certification Framework (EU-SEC) project was formed with the aim of improving the effectiveness and efficiency of the existing certification schemes that cloud providers use to demonstrate their security processes to the market. To do this, it developed a framework for recognising multiple cloud security certifications, known as the Multi-Party Recognition Framework (MPRF).

In order to validate the framework's theoretical model in real-world scenarios, EU-SEC tested and evaluated the core activities of the framework in order to assess its readiness and applicability. As part of work package 4 (WP4), EU-SEC project partners performed four separate pilot exercises, spanning activity in Germany, Slovenia, Slovakia and Switzerland. These activities replicated realistic use cases; the scope each one typically involved an auditee that had already achieved a security certification to ISO 27001, and testing to see how it could make the process of becoming certified to a separate standard or attestation easier and more efficient.

This report, deliverable 4.5, presents the consolidated findings for all four proof-of-concept exercises, including details of each deliverable, and the conclusions and recommendations from each one. The results presented in this report show the theoretical model of the MPRF successfully working in pilots. One pilot participant spoke of an "obvious upside of using the EU-SEC framework and tools", while another was able to reduce security requirements needed for an audit by 80% through using the associated technology tools.

The findings presented here provide strong evidence that the EU-SEC MPRF offers significant benefits for all stakeholders in the cloud computing security and privacy compliance arena.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

ABBREVIATIONS

CCM	Cloud Control Matrix
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
EC	European Commission
EU-SEC	European Security Certification Framework
G-Cloud	Slovak Government Cloud provided by the Ministry of the Interior of the Slovak Republic
ICT	Information and Communication Technology
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commission
IaaS	Infrastructure as a Service
IT	Information Technology
MFSR	Ministry of Finance of the Slovak Republic
MPRF	Multiparty recognition framework
NIXU	NIXU Oy Finland
PaaS	Platform as a Service
PwC	PricewaterhouseCoopers
SaaS	Software as a Service
SI-MPA	Ministry of Public Administration of the Republic of Slovenia
SoA	Statement of Applicability

UPVII	Deputy Prime Minister's Office for Investments and Informatization of the Slovak Republic
WP4	Work Package 4: Pilot 1: Multiparty recognition Scheme
WP2	Work package 2 : Governance Structure and Integration

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TERMINOLOGY AND DEFINITIONS

As in past deliverables, also for this document the terminology and definitions presented in Table 1 will be used.

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
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	https://www.iso.org/certification.html

	or system in question meets specific requirements.	
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 practice often 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 (EU-SEC, 2018)
Cloud Control 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
Delta	Requirements, mandatory for the desired attestation, not covered by already compliant attestations while applying the MPRF. Represent the minimum an audit has to address as its scope for an audit, when applying the MPRF.	
EU-SEC Security Requirements Repository	A repository of all collected requirements mapped against the CSA CCM, making it a native control framework to address the identified requirements	EU-SEC D1.2 v1.2 (EU-SEC, 2017)
Governance Body	A body responsible for governance of the Multi-party recognition framework and for maintenance of its repositories.	
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-	NIST SP 800-57

	based security decisions to adequately protect organization information.	
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
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

Table 1: Terms and definitions

1 INTRODUCTION

To date, the landscape for cloud security services has been characterised by a proliferation of different certification schemes. Currently, a private company that wants or needs to obtain multiple certifications, such as ISO/IEC 27001 or ISAE 3000 for example, or to comply with national standards, must go through multiple certification processes. These processes often duplicate both the requirements needed to reach the standard and the subsequent auditing process. This creates additional expense and labour for the certifying organisation. It also creates uncertainty for customers who typically have no means to easily understand the different meaning and value of each certification and have no easy way of comparing one security certification with another. In turn, the lack of common lens through which to compare certification schemes, and mutually recognise them, has arguably hindered further growth of the digital market in the European Union.

The European Security Certification Framework (EU-SEC) project was formed with the aim of improving the effectiveness and efficiency of the existing certification schemes that cloud providers use to demonstrate the security of the processes and operations. The key component of EU-SEC's work to date has been the Multi-Party Recognition Framework (MPRF) for cloud security certifications. This is described in work package two (WP2) of the EU-SEC project.

MPRF is intended to streamline the process of cloud security compliance by applying a consistent, unified method of activity that allows a Cloud Service Provider (CSP) to minimise the burden of becoming certified to a particular standard "Y", once it has already obtained certification "X". In essence, it takes the common denominators from the leading security standards and compliance schemes, identifies the overlapping components between them, and allows organisations to reuse the work done for one compliance scheme and apply it to another. In this way, the framework helps to eliminate unnecessary duplicated work involved in becoming certified to multiple cloud security standards. Auditors and auditees can focus their efforts most on the deltas where the respective standards do not overlap.

MPRF began as a theoretical model, so in order to validate the approach and observe it in practice, EU-SEC tested and evaluated its core activities (as defined within D2.1) in a series of real-world scenarios in order to assess its readiness and applicability. In working package 4 (WP4), EU-SEC performed four separate pilots together with industry partners. This report

consolidates the input from deliverables D4.1-D4.4 into a single pilot report with findings of all four exercises, including summarised details of each deliverable, along with the conclusions and recommendations from each one.

The objective of this document is to support the work of EU-SEC in advancing the MPRF model. It advances the work carried out so far in developing the theoretical model, bringing it closer to reality by applying it in a series of rigorous real-world tests, by identifying needs of stakeholders and of potential users, by applying valuable feedback from this process and by making the findings public.

The four pilot projects started from a base certification and aimed at achieving another, using the concept of the MPRF to guide the work. The projects were as follows (more detailed descriptions will appear later in this chapter):

Pilots 4.1-4.3 started with auditees having already been certified to ISO 27001 and pursuing a second certification. 4.1 was a table-top exercise and real-life ISO-based audit which aimed to verify if the Slovenian Ministry of Public Administration could effectively and efficiently achieve compliance with the Slovenian National Security requirements for cloud, and with ISO 27017 requirements, starting from an existing ISO 27001 certification.
Pilot 4.2 involved execution of an ISO-based compliance audit of the Slovak Government Cloud infrastructure, working from an existing ISO 27001 certification and using the MPRF to pursue compliance with ISO27017 and the Slovak National Requirements.
4.3 also aimed at validating the MPRF's lifecycle, when used to help a cloud service provider, SixSq to achieve compliance with ISO 27017, having already achieved certification in ISO 27001. In particular, this project aimed to show the validity of MPRF as a way of enabling a provider to comply more easily with multiple certifications or compliance schemes, in turn building greater trust with customers.
4.4 was a use case involving Fabasoft, a cloud service provider and document management service provider. As a European company, Fabasoft must comply with several certifications and attestations. It has a CSA STAR Attestation and was striving for a BSI C5 attestation.

Using the MPRF, any organisation that wants to become certified to multiple security standards may now do so without needing to go through multiple full audits. Instead, they need only focus on the components of each respective standard where there is no overlap. This saves valuable time and resources. In this context, it is to be noted that the MPRF-based pilot works

did not result in providing any official certification (i.e., to the auditees engaged), and that auditees and auditors acted with roles, as defined in the MPRF theoretical model (D2.1).

1.1 BACKGROUND

This section is to familiarise the reader with some of the important concepts and terms in the EU-SEC project and will outline the scope of each of the four pilots that was conducted as part of WP4. It also provides an overview of the concept of multiparty recognition as presented in WP2 and deliverable "D2.1. Multiparty recognition framework". The framework, or MPRF for short, is intended to simplify the comparison between security certification schemes – benefiting cloud service providers and, ultimately, users. Each of the pilots used the MPRF to compare one scheme to which an organisation was already certified, with another to which they wanted to become certified.

1.1.1 OVERVIEW OF MULTIPARTY RECOGNITION

Certification proliferation has caused organisations such as CSPs to invest considerable resources in compliance audits. Such a plethora of certification schemes introduces additional and often prohibitive re-assessment costs to CSPs, especially for small and medium-sized enterprises (SMEs) that cannot afford to invest resources in multiple certifications. Moreover, this adds confusion among cloud service users, because they may not understand the differences between the level of assurance offered by the various certification schemes. The existence of several EU national certification schemes, rather than creating the conditions for the flourishing of the Digital Single Market, instead create potential market barriers.

These issues gave birth to the idea of multiparty recognition, which enables the comparison-making process and the identification of the common security denominators that are found between the various certification schemes. Multiparty recognition enables an already certified CSP to acquire an additional cloud security certification by proving compliance only to that new certification's difference, or delta, of security requirements – that is, those new requirements not covered by certification[s] it has already acquired.

The expected benefits to cloud service providers and relevant stakeholders within the EU market are potentially significant. For providers, it allows them to invest time and resources more effectively; and for the end user it increases transparency, awareness and trust about cloud security certifications.

It is possible to deduce the "delta" of security requirements between two certification schemes after performing a comparison analysis (known as a methodical mapping and gap analysis) between them. This analysis is thoroughly described in previous works (see D1.2). This analysis also includes other comparison activities of certification-based elements, such as evidence collection and audit criteria and requirements.

The work presented in D2.1 "Multiparty Recognition Framework" aimed at organising and developing the multiparty recognition concept into a well-defined layered architecture. The framework allows for multiparty recognition activities to be performed in an unambiguous, organised and systematic manner.

In brief, the multiparty recognition framework, as thoroughly presented in D2.1, comprises several distinct components:

- The operational and governance processes for multiparty recognition
- The governance and bodies, with roles and responsibilities
- The principles, criteria, requirements for multiparty recognition
- The repository of security, privacy, evidence and audit requirements.

These components are organised and multilaterally interact within a 3-step lifecycle "Evaluate-Execute-Govern", which defines the starting and ending points of the multiparty recognition activities (see D1.4 and D2.1).

The "evaluate" step of the lifecycle includes the framework's assessment activities that take place before any execution activity. In this step, a request for multiparty recognition between two certification schemes will be assessed for eligibility against the framework's established principles, criteria and requirements.

The actual multiparty recognition comparison activities take place within the operational context of the framework; that is, the "execute" step of the lifecycle. The operational phase is defined by five ordered activities as shown below in Figure *1*.

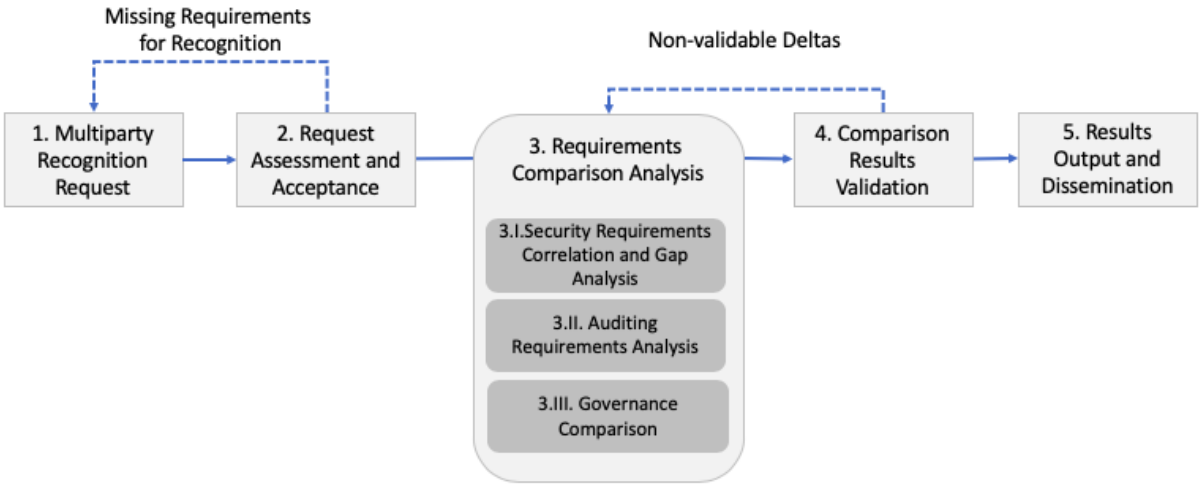

Figure 1: MPRF Operational Phase's Process Diagram

Finally, the "govern" step is dedicated to the governance of the multiparty recognition framework. It defines the organisational, managerial and maintenance activities for all incorporated components, based on which all activities taking place within the other two lifecycle steps become possible. Two main processes have been defined in governance; the change and complaint management processes.

1.1.2 INTRODUCTION TO PILOTS' SCOPE

The multiparty recognition framework constitutes a theoretical model which has to be tested for "proof of concept" against realistic use cases in order to validate the established concepts, activities and processes as defined by its architecture. Useful feedback and lessons from the exercises will then be used to further enhance the MPRF ahead of its full deployment and operation.

In this context, there were four pilot works that targeted to validating the MPRF "proof of concept" requirement. Here, we briefly introduce the partners and services that were used in each pilot as part of the works in WP4. This introduction will provide an overview of the basic concepts and respective components used in such pilots, allowing the reader to fully comprehend the basic semantics of the works carried out, as presented in later chapters.

The first pilot D4.1, was conducted by EU-SEC project partners SI-MPA and NIXU, as auditee and auditor respectively. The scope of the audited service included the "hosted applications

on the private Slovenian Government Cloud (SGC) infrastructure" (see Figure *2*). SGC is managed by the Ministry of Public Administration, and offers cloud computing services to citizens, businesses entities and government administration. The ministry's SGC has already achieved ISO 27001 certification for the ISMS of the core business process. As well as complying with different standards of information security, it is typical for public administration agencies to ensure trust by adhering strictly to national legal requirements for cyber security and privacy data protection. In addition, compliance to CSA CCM and SI national legislation certification requirements also required examination. In this context, the objective of the pilot was to test the aforementioned certification schemes for multiparty recognition based on the respective theoretical concept and framework model.

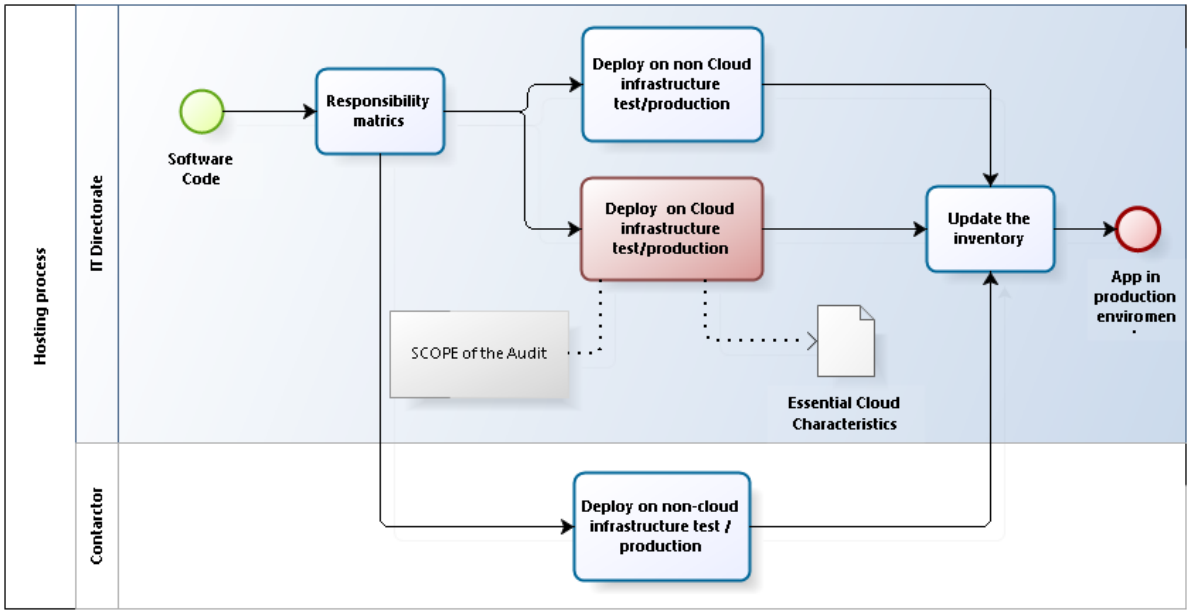

Figure 2: Service scope of the ISO-based pilot 4.1

The second pilot, D4.2, involved two partners: The Ministry of Finance of the Slovak Republic as auditee, and NIXU as auditor. The scope of pilot reflects a service based on the G-Cloud in Slovakia, which is a government-wide cloud computing platform which creates a more efficient and accessible means for dynamically releasing and sharing technical resources such as servers, storage, databases and applications. Currently only IaaS is running in the cloud for the service selected for this pilot, the "Computing power" (Virtual PC), as shown in Figure *3*. The pilot's main task was to use the G-Cloud service's test bed as a use case in order to test the MPRF against ISO 27001 and CSA CCM security requirements.

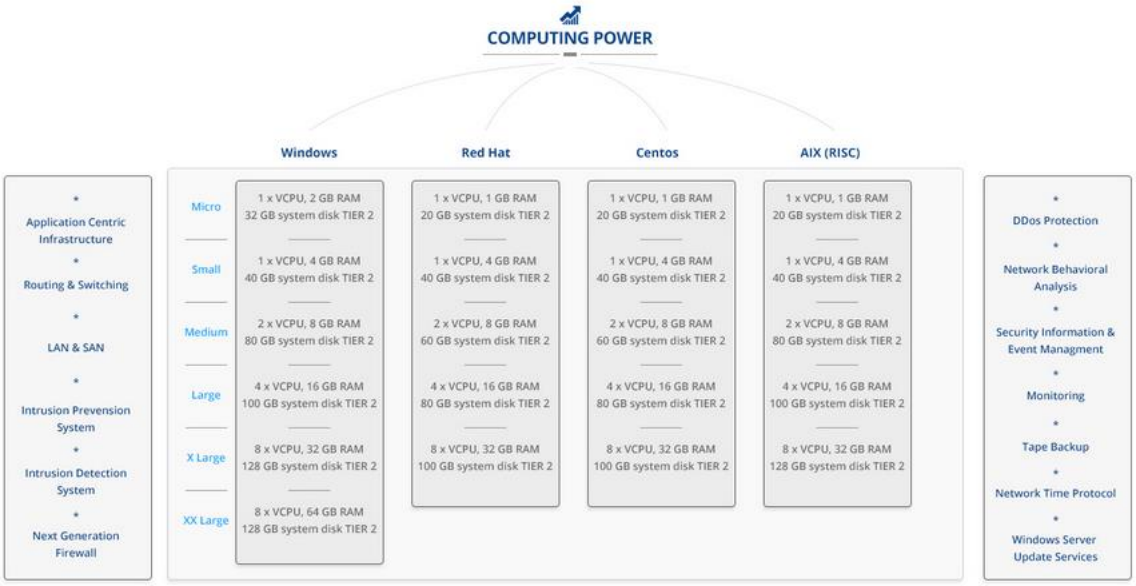

Figure 3: Service scope of the ISO-based 4.2 pilot

For pilot D4.3, SixSq and NIXU were the auditee and auditor respectively. SixSq is a Swiss company that provides "smart" edge and cloud software. The creation of this audit's ISMS (and consequent SoA) was based on existing company policies and best practices which translated into ISO 27001 and ISO 27017 controls. These were later optimised using the CCM mappings methodology [6] and the EU-SEC repository of requirements and controls (sometimes also referred to as simply EU-SEC repository) to identify the minimum set of controls needed for achieving compliance with both specifications. In this use case, unlike the other audits in WP4, the auditee is not to be seen as a CSP actor in the auditing process, as its core business activities are better described as a Cloud Service Broker (CSB). The pilot used MPRF and EU-SEC repository of security requirements to connect and analyse how the ISO-based (ISO27001 and ISO27017) audit and multiparty recognition analysis could be used with respect to the requirements set in CSA CCM.

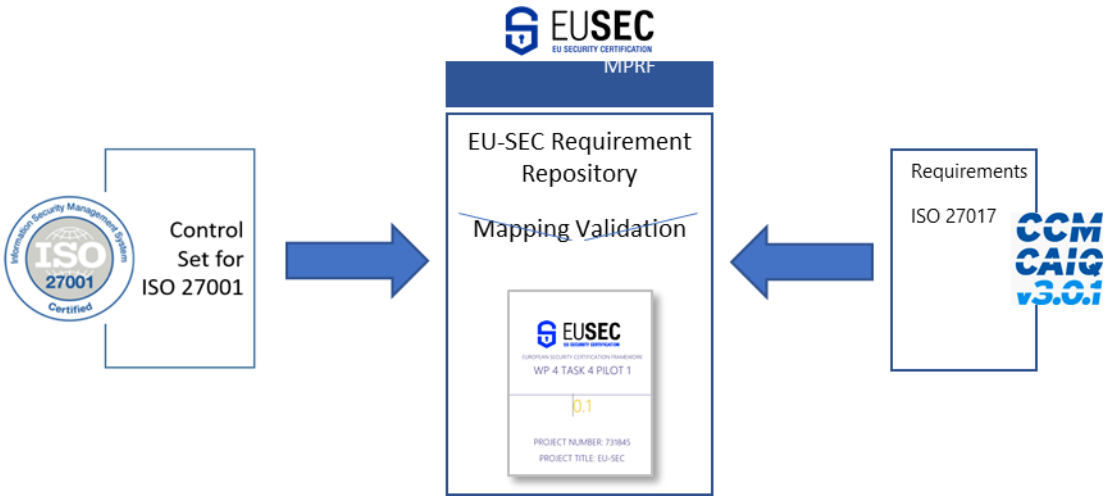

Figure 4*: EU-SEC repository of requirements and controls – validation approach*

For the fourth pilot D4.4, Fabasoft was the auditee and PwC Germany was the auditor. Fabasoft offers services for the digital control of documents as well as electronic document, process and record management. As a European company, Fabasoft is subject to strict data protection laws, but meeting all these compliance requirements carries a significant and increasing cost. For the purposes of the pilot, Fabasoft was assumed to hold a CSA STAR attestation and AICPA TSC 2016 (SOC2) and wanted to achieve BSI C5. It requested an MPRF-based audit with the aim of reducing the effort needed for this. The pilot aimed to test the principles and mechanisms of MPRF within the scope of the pilot's ability to show whether PwC could issue a BSI C5 attestation report and what challenges exist. This involved testing the readiness of the EU-SEC repository to show where the Cloud Controls Matrix (CCM) does not yet fully cover the BSI C5 and AICPA TSC 2016 requirements. It also covered assessing the compliance of Fabasoft's ISMS to the selected requirements included in BSI C5 and CSA STAR Attestation (with a focus on AICPA TSC 2016 (SOC2) related requirements) to show the benefits of using the multiparty recognition concept for auditee and auditor.

Having presented a high-level overview of the context of work so far, the reader will be able to easier comprehend the next steps, including the objectives of this deliverable and the methodology used to achieving them.

1.2 SCOPE AND OBJECTIVES

The scope of work involves collecting and analysing the results from all four pilot exercises D4.1-D4.4 of WP4. These results are expected to shed light on the validity of the theoretical model and framework for multiparty recognition as defined in D2.1. Equally importantly, the results will contribute to our knowledge based on the lessons learned and challenges met from real-world use cases when applying the concept of multiparty recognition for certification, especially from an auditor's perspective.

The objectives of this work can be summarised as follows:

- Identify and present the validation results from each pilot with respect to the multiparty recognition framework and per corresponding life-cycle phase (evaluate, execute, govern).
- Collect and present the auditors' recommendations and conclusions on the feasibility and soundness of multiparty recognition activities.
- Determine what is useful feedback that is to be shared with D2.5 and used to enhance the multiparty recognition framework, defined as part of the EU-SEC framework.
- Consolidate the pilots' assessment results with respect to the Technology Readiness Level (TRL) of the tools used within the pilots exercises (e.g., the EU-SEC repository of evidences and security controls readiness) and establish if such tools are fit for purpose.

The target audience of this deliverable involves all stakeholders that are interested in or benefit from the framework of multiparty recognition, such as: CSPs, cloud users and certifications auditors. The pilot exercises and derived results are expected to illustrate the real-world application feasibility of the framework and accordingly the benefits or related concerns of the task, which will be open for discussion within activities of WP6.

1.3 METHODOLOGY

The methodology for this report involves collating and analysing feedback about the MPRF that participants in the four pilots, T4.1-4.4, provided in subsequent reports. Each of the reports

was prepared by multiple authors representing both auditees and auditors involved in that specific pilot.

In preparing the material for this report D4.5, findings from each of the use case reports were reviewed and summarised, with the aim of presenting the input in reformatted, edited and filtered form for consistency in order to be useful for D2.5.

The content of this document also draws upon deliverable 1.4 of the EU-SEC project, which presents the responses of participants in all four use case to a questionnaire which was presented at a workshop after the exercises were completed. This questionnaire is part of activity 2 of the MPRF framework and is included in an annex at the end of this document.

Where appropriate, this document presents the auditees' and auditors' experience of using the MPRF as synthesised findings where there was broad consensus. It augments this with specific commentary and findings from the individual use cases where they help to illustrate a point for the reader.

1.4 DOCUMENT STRUCTURE

This document is organised as follows:

Chapter 1 provides a brief background to the report, with an overview of the multiparty recognition framework theoretical model and its reason for being. It outlines the pilot scope of the report, its objectives in summarising four pilot projects, and details the methodology in assembling this final report.

Chapter 2 summarises the results of the validation stage of the multiparty recognition framework, across the evaluation, execution and governance phases.

Chapter 3 describes the comprehensive audit results, looking specifically at the results of the ISO27001-based audits and then the ISAE3000-based audit.

Chapter 4 details the readiness assessment of the tools used in the pilot exercises and summarises their fitness for purpose, including the Nuvla tool from deliverable 4.3.

Chapter 5 provides a brief summary of the conclusions from all four pilot reports 4.1-4.4 and lists the recommendations for improving the framework that emerged from each project.

2 SUMMARY OF MULTIPARTY RECOGNITION FRAMEWORK VALIDATION RESULTS

This chapter presents the summary findings of validation works carried out across all four pilots, which considered all components and activities of the framework. Throughout all four pilots, there was a process of describing the work with regards to the MPRF's five activities and concluding whether the practical work validated the theoretical model. Per the MPRF model, this involved testing the following, as defined in D2.1:

- Evaluation activities 1, 2 and 4
- Execution activities under activity 3,5
- Governance (with relevant processes, roles and responsibilities).

2.1 EVALUATION PHASE

Evaluation is a key part of the MPRF lifecycle, because it's envisioned that this process will allow an organisation currently holding a certification such as ISO 27001, for example, to also become certified to their own national certification, or to another compliance scheme. The MPRF evaluation phase determines if that second certification is suitable to become eligible for the EU-SEC framework. The evaluation includes the following steps:

- Multiparty recognition request
- Request assessment and acceptance
- Comparison results validation.

Multiparty Recognition Request is the provision and collection of inputs that will be fed to the framework, involving requests from the compliance schemes to start the MPRF process. The compliance scheme owner asks the EU-SEC governance body to gain a Request ID which includes all representative details such as contact information, description of the compliance scheme's security requirements, auditing requirements and governance model. For pilot 4.1,

the scheme owner's contact details were used, and the compliance schemes used were ISO27001, ISO27017 and Slovenian national requirements, which were already mapped in EU-SEC security and privacy requirements repository and included in the MPRF Framework. The auditing requirements were used as described in the MPRF, and the governance model used was based on the ISO-standard and Slovenian national legislation governance. A similar process was used for pilot 4.2, the only difference being that the compliance schemes involved both ISO standard and the Slovakian national requirements. For pilots 4.3 and 4.4, the schemes are already included and mapped in the Framework. This meant that the compliance scheme's security requirements, auditing requirements and governance model description were available, and the request activity did not need to take place.

With regards to the "**comparison results validation**" steps, the pilots' works involved:

In pilot 4.1, ISO 27002 includes 77 requirements with specified controls directly applied by ISO 27001 and ISO 27017. For example, the same control specified in ISO 27001 A.6.1.4 requirement directly applies to ISO 27017 6.1.4 requirement. Consequently, no mapping differences in EU-SEC requirements and controls repository are expected to such 77 pairs of ISO 27001 and ISO 27017 requirements. Many other pairs like this can be found both mapped and marked with No gap level but mapped to different CCM controls. In the existing EU-SEC requirements and controls repository only five such pairs of No Gap level requirements are mapped identically to same CCM controls.

In the requirements comparison validation phase for 4.2, the EU-SEC governance body CSA, with the help of auditors NIXU, validated the requirements comparison results, as provided by the MPRF activity #3, and more specifically, its sub-activity 3.I. Validation works involved assessing the gap analyses and missing requirements compensating works of the mappings performed between SK national requirements, ISO27017 and ISO27001. The remaining requirements comparison results and their validation for activities 3.II-3.V were also performed. During the validation of mappings from ISO 27017 to CCM also those controls from ISO 27017 not selected to auditees' extended SoA were cross-checked.

To adhere to activity 4 of the MPRF in pilot 4.3, the participants performed two mappings and gap analyses validations during the pilot. The initial assessment and validation of the EU-SEC mappings provided a preliminary validation of the EU-SEC repository mappings performed in WP1. In fact, the integration of ISO27001 requirements into the EU-SEC repository was assessed for its correctness and consistency by the auditor.

For pilot 4.4, the CSA took the role of governing body for the framework to assist the auditor PwC and validate its results. Comparing the security controls, PwC found that comparison and validation is crucial in activity 4 of the lifecycle, as the security requirements repository changes over time. The verification of mappings and closing of gaps led to increasing the maturity of mappings and of the framework itself. Fabasoft, the auditee, was subsequently able to narrow the list of requirements for future audit scope.

With regards to the "**Request assessment and acceptance**" step, the pilots' works involved:

The partners applied in practice the principles, criteria and requirements to test the eligibility of the certification schemes to participate in the multiparty recognition process. This section briefly outlines the evaluation activity for the pilots, followed by the formal opinions of WP4 auditors and auditees on MPRF criteria and requirements, using their responses to parts A and B of the Principles, Criteria, Requirements, or P-C-R, questionnaire (see Annex A).

Principles

This section summarises the opinions of WP4 auditees and auditors on all components and activities of the MPRF, which are the foundation on which multiparty recognition is based. These four principles are: repeatability, equivalence, relevancy, and trustworthiness.

The first question asked whether the results are the same when two different entities conduct an independent audit of the same information system's security/privacy requirements, under the same scope and conditions. All auditees said yes, as did auditor PwC. NIXU replied "yes and no", elaborating as follows: "for instance in ISO audits, samples are commonly used, selection is always based on the auditor's decision and knowledge, there are always small deviations, thus *mostly only minor and no influence on certification itself*." [Our emphasis.]

Addressing the equivalence principle, the participants were asked whether the security/privacy level in two information systems are equivalent when a security/privacy requirement that is assessed in these two independent information systems and the evidence collected or the measurement results are the same. Responses were mixed: auditees said they were "probably not exactly the same" or said they did not know. SIXSQ gave the most specific answer, noting that the levels might overlap but that does not mean they are exactly the same. The auditors were more definite on this point. NIXU believed the security/privacy levels are the same, while PwC said they "probably" are, but added that this would depend on further safeguards or controls that are not in scope.

On the relevancy principle, the participants were asked if the security/privacy requirements and the associated processes used for assessing an information system were chosen in order to provide actionable information to the auditee? The response among auditees was mixed; SI-MPA said "probably yes", while MFSR said "not now, but after end of project when the guidance will be in place".

As for the auditors, NIXU believed that the requirements and processes were selected with a view to giving auditees actionable information. "Within the ISO standards the auditee can define the scope of certification based on their needs," NIXU said. PwC said it would depend on the auditor and on project-specific agreements.

The final question related to the trustworthiness principle. It asked whether the process of collecting, verifying and evaluating evidence against audit criteria was transparent, unbiased, complete and unambiguous in order to provide a trustworthy representation of the security/privacy level provided by an information system. Among both auditees and auditors, the broad consensus was affirmative. Only the auditee MFSR answered "don't know", while SIXSQ had questions about the process of collecting and who defines it.

Criteria

The first question in part A ("Criteria's Questionnaire", see Annex A) of the P-C-R questionnaire asked whether the requirements in different compliance or certification schemes are comparable, and therefore possible to be mapped to each other for any gaps to be identified. All of the auditees and auditors said yes. Comparability criteria and requirements were met among all schemes that were provided to the framework.

The following question C2 addressed the comparability of auditing mechanisms, covering both the test procedures executed and the metrics used. It also covered whether the mechanisms resulted in the same level of assurance and audit comfort. All four auditees responded affirmatively. As auditor, NIXU answered yes; PwC hedged its answer by saying it depends on design suitability or operating effectiveness.

A follow-up question, asking: "Do audits refer to or require compliance to a named code of practice(s), e.g., BSI C5 requires the auditor to apply the ISAE 3000?" drew a mixed response.

Auditors NIXU and PwC both said yes, but there was more confusion among auditees. SI-MPA and SIXSQ responded "don't know". MFSR and Fabasoft said yes.

Question C3 asked whether the evidence collected was "suitable evidence"; that is accurate, reliable and suitable to support the audit conclusions. All project participants said it was suitable. PwC added the note that professional judgement is also important.

Question C4 addressed whether auditors' qualifications were transparent and well defined. All of the pilot participants said yes they were. Equally, all respondents said the auditors are required to demonstrate knowledge of the cloud sector and be qualified to perform assessments in line with relevant auditing standards. PwC went further, saying: "This is a requirement – only with the right knowledge, the auditor can address certain cloud-specific risks". What's more, all participants were in agreement that auditors are required to demonstrate relevant formal education and personal certifications, minimum work experience, adherence to Code of Professional Ethics, training and continued professional education.

Question C5 asked whether the compliance/certification schemes have a transparent and well-defined governance model with an independent standard-setting body with no conflict of interest. The auditees SI-MPA and MFSR said yes, with the latter noting that the model is clear for ISO certification, but the Slovak governance is still in development. SIXSQ deferred to its auditor NIXU who answered yes. Fabasoft and PwC said STAR Attestation relies on the Open Framework Community, but BSI C5 does not have a specific governance model, to their knowledge. As to whether the governance models use a change management process to ensure that the standard stays fit for purpose, the response was mixed. SI-MPA, SIXSQ and NIXU all said yes. MFSR and Fabasoft said they were not aware of such a process.

Requirements

Questions R1-1.3 related to the comparability of the control framework. R1 asked if the EU-SEC Governing Body had suggested the compensating requirements to bridge the identified gaps between the requirements of different certification schemes. R1.2 asked if the EU-SEC governing body had determined the nature of the gaps between the different certification schemes. R1.3 asked if the EU-SEC Governing Body suggested compensating requirements to bridge the identified gaps between the requirements of different certification schemes.

All the auditees said yes to the three questions, as the EU-SEC governing body performed the mapping and gap analysis of the different certification schemes' requirements. As auditor, PwC said yes, that the 'simulated' governing body performed this task, while NIXU said no such

body had been implemented yet, so initial mapping of requirements was performed as part of T1.2. Further mappings were performed by CSA and involved parties (auditees and auditors) and as such acting as one in pilot audits.

There was less clarity over question R1.4, which asked if the EU-SEC governing body had adopted a clear, well documented and transparent approach for carrying out a comparison and gap analysis between the requirements of different security frameworks. As the framework is still being developed, the consensus was that the approach is not clear yet. As Fabasoft noted, "there is room for improvement here", and NIXU said "there is still a lot of work to be done here". A note in the report says that additional operating instructions would be desirable. "The auditors need reassurance that mutual recognition is doable. It needs to be simple and understandable how the requirements from different schemes can be compared and managed under the EU-SEC framework."

Auditees agreed that the Authority accepts the requirements mapping, gap analysis and potential compensating requirements of the EU-SEC framework (R1.5). The auditors NIXU and PwC commented that it was not evaluated or not done yet.

Asked about comparability of auditing mechanisms, all pilot participants said the authorized auditor used comparable control procedures and metrics that result in the same level of assurance (R2.1). Equally, all six agreed that the authorised auditor performed audits which referred to, or required compliance to, a named code of practice (R2.2). There was also universal agreement that the authorised auditor accepts performing an audit on a scope that is considered relevant. Fabasoft further clarified this in its answer, saying that in its specific case involving BSI C5, the scope is always "all domains".

There was wide agreement among the participants about the issues concerning suitability of evidence, addressed in question R3. In the four pilots, they confirmed that the authorised auditor collects evidence that needs to be appropriate, sufficient, selective and persuasive. They also agreed that the authorised auditor determines the timeframe of collected evidence (R3.2), and also identifies the criteria against which evidence is needed for audit to ensure the correct conclusions. All participants confirmed that the authorised auditor records findings to make an informed decision on compliance with the requirements (R3.4). All participants also confirmed that the authorised auditor records nonconformities with specific requirements and makes clear statements about them using objective evidence. All participants found that the authorised auditor follows a consistent and relevant sampling approach when collecting evidence.

For section R4 of the questionnaire covering auditor qualifications, several of the participants were unable to answer whether the EU-SEC governing body had initiated the process for mutual recognition only between certification schemes that impose clear, transparent, comparable and relevant qualifications. NIXU clarified further, noting that an evaluation was carried out in the pilot as a table top exercise because the Governing body was not officially in place, but said it would have passed the actual process.

Questions 4.2-4.5 produced broad agreement among all parties; they found that the auditors:

- led the assessment engagement as required by the standards
- had sufficient subject matter expertise and knowledge
- had sufficiently qualified professional personnel to conduct the audit
- adhered to the professional code of ethics.

The PCR-based questionnaire is a valuable additional way of assessing the MPRF concept, by obtaining detailed and direct feedback from the auditees and auditors who took part in the four pilot exercises. Taken as a whole, the questionnaire provides strong evidence that it is possible to achieve a mutual comparison between the various schemes used during the pilots – which is a cornerstone of the framework concept. Answers C1-C5 were almost universally positive, proving that the criteria have been met. There were similarly strong positive replies to questions about the comparability of auditing mechanisms. Moreover, the requirements for multiparty recognition, aligned with the framework's governance structure (i.e., testing the operability the governance body) have been satisfied and have shown the validity of the operations. The P-C-R questionnaire also indicated some areas for further investigation: per R1.4, there was wide agreement that more work is needed to obtain a well-documented and transparent approach for comparison and gap analysis between requirements of different security frameworks.

2.2 EXECUTION PHASE

The purpose of this section is to summarise the works that took place in order to validate activity 3 "Requirements Comparison Analysis" of the MPRF's theoretical model. All four pilots followed the steps outlined in the MPRF's lifecycle, under the "execute" heading. For clarification, Figure 1, the MPRF Operational Phase's Process Diagram, is a simplified model that lists three sub-activities. All four pilots T4.1-4.4 used five sub-activities as part of the model.

Both versions are correct, since three out of five sub-activities have a common topic, which is auditing requirements. The five sub-activities are as follows:

- Security controls comparison
- Auditors qualifications comparison
- Certifications audit mechanisms comparison
- Evidence suitability comparison
- Governance comparison

The comparison work in pilot 4.1 involved a sample of selected controls from ISO 27017 and Slovenian national requirements which were compared to ISO 27001 through CSA CCM controls. Any identified gaps, or deltas, identified between the control schemes were then revised by CSA to close the gaps between the schemes. A similar process was followed for pilots 4.2 and 4.3.

During the security control mapping and gap analysis process in pilot 4.1, the acting Governance body (CSA) had to create compensating controls to fill in each gap before executing the actual pilot. Compensating controls were implemented to the extended SoA. The EU-SEC requirements and controls repository, upon initialization of the pilot, did not include these compensating controls for the partial/full gaps found on requirements. Additional verification of the partial/full gaps of previous ISO 27017 and CCM mapping was done as part of the project. An additional verification process performed, resulted to changing Partial/Full gap level to No gap level for 10 requirements and to Full gap level for 1 requirement. This work is to be considered as part of the validation process of the initial WP1 D1.2 mapping that is to be considered in the context of the Multiparty Recognition Framework and its Execution Phase and activity 4 “Comparison Results Validation” described in D2.1.

During this pilot the ISO standards and Slovenian national legislation governance schemes were compared. The comparability criteria and requirements were satisfied, and hence multiparty recognition was deemed feasible. The auditors noted in report 4.1 that the current level of mappings maturity would require high knowledge from the auditee and the auditor to go through the MPRF process. It was also noted by auditor NIXU that the accuracy of the repository is expected to improve along with its maturity increase.

The EU-SEC requirements and controls repository was built as Excel spreadsheet where one or many requirements are mapped to one or many CSA CCM controls (N:N). Due to N:N mapping

of the extensive number of different requirements (804) to one or more corresponding CCM controls (133), the spreadsheet became non-transparent and consequently difficult to handle.

In pilots 4.1 and 4.3, the maturity level of the mappings in the Multiparty Recognition Repository at the time of the pilot led to the actual exercises being restarted. During the pilot's second phase, several additional steps had to be added to perform mappings, create compensating controls and test the framework.

In pilot 4.2, the auditee had selected 12 controls from ISO 27017 and 19 controls from Slovak national requirements to be included in the extended SoA. All mappings in the chosen sample between ISO 27017 and CCM controls from the EU-SEC repository of requirements did not include any gaps. These controls were also evaluated by the auditor during the audit for further assurance. As the Slovak national requirements were not mapped earlier during the MPRF, the requirements were created during the pilot process and mapping of those is still at early stages and can be considered preliminary. Based on the initial analysis carried out by the auditee (MFSR), the Slovak national requirement included 2 controls with full gap, 3 controls with partial gap and 12 controls with no gap between the requirements.

For project 4.2's MPRF "execute" phase, the participants performed the necessary activities to validate the MPRF model as defined in activities #3 and #5:

- Requirements comparison analysis
- Results output and dissemination.

For ISO 27017-based controls there was no further analysis carried out, because there were no existing gaps identified in the sample of controls selected. All the governance models used in 4.2 were compatible, and no additional efforts were needed.

For pilot 4.3, the auditee chose a well-defined set of requirements for the ISO extension based on the following criteria:

a) requirements from ISO 27017 which had partial and full gaps in the repository, and additional testing was needed;

b) requirements fit tightly with the auditee's scope and core business.

The requirements comparison in D4.3 involved two distinct mapping exercises between the ISO 27017 and CCM requirements and those of ISO 27001, in order to infer the differential

number of requirements that were to be used to build the extended SoA for the audit. Based on the comparison results, the auditee chose 22 requirements from ISO 27017 to be included in its extended SoA. From those 22 requirements, the EU-SEC repository had mapped 4 CCM controls with Full Gap, 6 CCM controls with Partial Gap and 12 CCM controls with No Gap. These controls were evaluated both before and during the audit process.

In pilot 4.4, Fabasoft was assumed to have a STAR attestation + AICPA TSC 2016 and wanting to use the EU-SEC repository to obtain BSI C5. This use case provided further detail on MPRF's execution phase. As a first step, the 114 mandatory requirements of the BSI C5 catalogue were selected and listed in an Excel table. When consulting the Security Requirements Repository, it showed that 83 requirements (labelled "no gap") of BSI C5 were already covered by STAR Attestation due to the mappings. These 83 requirements were found semantically equivalent to those of the repository (CCM) hence are not to be audited as they are already covered by the STAR. The remaining 31 controls not covered by the existing STAR attestation were collected in a T4.4-repository. The final list of requirements to be used in the audit included just 27 after PwC validated the mappings. The preliminary math for deriving the *Delta* was as follows: 114 (BSI C5) – 83 (EU-SEC *no gaps*) – 8 (PwC revised to *no-gaps*) + 4 (PwC revised to *partial gaps*) = 27 requirements in the T4.4-repository, to be used in the final audit. When comparing security controls, PwC needed to map and double check. However, the more mature the framework gets, the more efficiency auditors may gain.

    - **Result:** The comparison and validation (in activity 4 of the life-cycle) is crucial for the auditor at this point, as the Security Requirements Repository by its nature is changing (updating) over time, thus cross checking is a mandatory activity.

- Verification of mappings and *closing* of gaps

    - **Result:** An increase in maturity of mappings and the framework itself

- Fabasoft was able to subsequently narrow down the list of requirements for the future audit scope.

    - **Result:** the preliminary math for deriving the *delta* was: 114 (BSI C5) – 83 (EU-SEC *no gaps*) – 8 (PwC revised to *no-gaps*) + 4 (PwC revised to *partial gaps*) = 27 requirements in the T4.4-repository, finally to be used in the audit.

2.3 GOVERNANCE PHASE

For pilot 4.4, the Cloud Security Alliance, which is the technical lead in the EU-SEC project, continuously double-checked and verified PwC's work during this pilot, effectively assuming the role of governing body. CSA governed work carried out by PwC as the auditor, and suggestions made by Fabasoft as the auditee. After the framework reaches maturity and is applied in real-world audits, these responsibilities and duties will need to be fulfilled by the EU-SEC Governing Body. This will be defined as part of the D2.5, later in the project.

It is worth making the point that this governance work accompanied the entire duration of the pilot. Report 4.4. noted that this is most likely to be the way it will be, as governing the MPRF approach cannot be a point-in-time exercise.

The auditor checked already mapped requirements and in some rare cases (approximately 5%) came up with revised interpretations and mapping argumentations. These inconsistencies were discussed with the Governing Body to provide the auditee a sound solution to advance with the audit: as described by chapter 4 in D2.1, the complaint management process would process the complaint from PwC and the repository would be updated using the change management process.

Section R5 of the P-C-R questionnaire (see Annex A) referred to the governance model. In general, the auditors' responses were more decisive than the auditees in the pilot exercises. NIXU and PwC both responded affirmatively to the questions about whether the EU-SEC Governing Body had allowed for mutual recognition only between schemes with well-defined, transparent and documented governance structures (R5.1); between schemes that guarantee independence (R5.2); and mechanisms for collecting complaints (R5.3). They said mutual recognition had been defined and tested affirmatively in the pilots, while NIXU added that the pilots did not test complaints management.

Three of the pilot auditees said the questions did not apply to them, while MFSR said that as pilot auditee, it initiated the process of comparison Slovak requirements against the EU-SEC framework.

There was a mixed response to the question of whether the compared certification schemes envisage internal audit mechanisms that would allow the scheme owner to audit certification

bodies periodically. SI-MPA, Fabasoft and NIXU said the scheme did so; MFSR and SIXSQ were not sure, while PwC said the answer was "no".

Question R5.5 addressed whether the certification scheme under comparison had a governance structure that clearly identified the governing body, along with its roles and responsibilities. The majority said yes; SISXQ deferred to NIXU, who answered positively, while only MFSR said no. This may be due to Slovak national requirements. PwC answered yes but added that further details are needed.

As to whether the governance structure of the scheme under comparison includes a clear change management process (R5.6), the results were mixed. SI-MPA said yes, while MFSR and SIXSQ did not know. Fabasoft and PwC said it was not included with all schemes; no official process relating to BSI C5 was available for the pilot, although it was communicated to the participants that one exists. Question R5.7 drew a similarly mixed response. It asked if the governance structure of the scheme under comparison transparently defines the rules of participation to governing bodies and their decision-making mechanisms. SI-MPA, MFSR and SIXSQ were not sure, while PwC said not yet. Only Fabasoft and NIXU said yes. The latter added: "in Finland it is SFS (ISO National Body) which is part of the decision-making mechanisms. If required [an] organisation could try to push changes through that, not directly."

The EU-SEC security requirements repository is audited by accredited auditors in the view of SI-MPA, SIXSQ and NIXU. Fabasoft did not know and PwC answered: "not yet but a good idea".

For 5.9, asking if the authority maintained a publicly available register of authorised auditors, most of the auditees said they did not know; only Fabasoft said yes. NIXU said the answer was yes if talking about ISO, where national bodies would maintain such a register. PwC said there was a register for CSA STAR but not for BSI C5. The responses were broadly the same for the follow-up question R5.10 of whether the authority maintained a publicly available register of certified CSPs. NIXU said such a list is available on request. PwC said there is such a register for CSA STAR but not for BSI C5.

Only two out of the six participants, MFSR and NIXU, answered affirmatively to question R5.11, which asked if the EU-SEC Framework Governance Body maintained a repository of standards, best practices and control frameworks that are covered under the mutual recognition framework and provide reference to the specific requirements/controls in each standard. NIXU went further, saying "It is documented in the requirements repository as a result of T1.2 but

this document is a snapshot on a certain point in time and it needs to be appropriately governed in future".

There was a similarly mixed response to question R5.12, about whether the authority periodically audits the authorised auditors to maintain acceptable quality levels. SI-MPA and SIXSQ were not sure, PwC said no while the others said yes.

3 COMPREHENSIVE AUDIT RESULTS

3.1 ISO27001-BASED AUDITS

This section summarises of the ISO-based audits that took place in the context of WP4.

For project 4.1, after the auditee had prepared their environment and the extended SoA, the auditor started the official process and conducted it as a standard ISO-based audit. The auditor continuously followed the specifications set by earlier phases of the EU-SEC project. The audit aimed to test the conformity of the additional SI national, ISO27017 and CCM requirements (defined in the extended SoA) against the respective implemented controls at SI-MPA's existing environment. The audit was conducted using CSA CCM as a tool for auditing.

The audit was conducted in two stages: the first reviewed the ISMS scope and documentation to confirm that the auditee fulfils the set requirements. The second stage involved auditing security controls from SoA to verify compliance.

Requirements that were not met in ISO 27001 were marked to 'partial' or 'full' gap. For this pilot case, (ISO 27001-certified ISMS all Extended SoA controls with no gap to ISO 27001) can be considered as implemented and no further audit was needed. Final count was 51 No gap, 3 Full gap and 10 Partial gap controls to ISO 27001.

Although the preparation of extended SoA is based on the current version of EU-SEC requirements and controls repository, containing possible mapping gaps and being aware of different mapping subjective opinions, we can conclude that only thirteen (13) partial/full gap controls were identified between ISO 27001 requirements and a limited number of selected ISO 27017 and SI-07 National requirements. After applying the MPRF, only these 13 controls of the extended SoA were used for executing the audit pilot.

Based on gap analysis results, from 146 controls (CCM + ISO27017 deltas), there were only 31 partial/full gap controls identified between ISO 27001 and ISO 27017.

The conclusion from this exercise is that, if all the preparatory work is done well, the MPRF audit effort made to obtain ISO 27017 compliance should be much lower compared to the needed effort if the MPRF is not used.

For pilot 4.2, the audit was finalised after the stage 2 audit. The audit was conducted as an ISO-based audit as defined in ISO/IEC 27007. No additional comparison was required, as it fully complies to requirements set in MPRF.

As the pilot audit was conducted as ISO-based using the CSA STAR CCM base tool both governance model's comparison of those models was performed. During the pilot, selected Slovak national requirements were also added to Multiparty Recognition Framework. All additional requirements set by national legislation were also analysed.

The observations gathered during the audit were then analysed and used to evaluate the MPRF. The following observations were made about the audit process when the audit was finished.

- The audit process was straightforward
- The ISO-based audit process could be followed.

In project 4.3, the main objective was to validate the MPRF's lifecycle, when used to achieve compliance between ISO 27017 and ISO 27001. The results of the pilot show that the framework is based on solid as well as functional work and with the right governance and improvements, it can potentially be used in production environments.

For this specific use case, using the MPRF might not bring a significant added value since ISO ISO 27017 was conceived as an extension of ISO27001 for the cloud sector and the actual difference between both can be more easily fulfilled by implementing the native ISO requirements rather than relying on the EU-SEC repository. That being said, the report noted "an obvious upside" to using the EU-SEC framework and tools, as it allows the auditee "to exponentially decrease the future effort for acquiring other certifications".

The report found that the audit mechanisms and processes in exercise 4.3 did not deviate from a normal ISO 27001 audit.

3.2 ISAE3000-BASED AUDITS

This section summarises the ISAE3000-based audit from pilot 4.4, and its results. It focuses on the benefits that accrued from using the MPRF output to perform the audit.

One point to note is that since BSI C5 and CSA STAR Attestation are both based on ISAE 3000, there is no difference between the audit mechanisms. Given ISAE3000's description and rules for comparing schemes that rely on its ruleset, PwC as auditor accepted evidences produced for STAR Attestation requirements that map to BSI C5 requirements with no gap in the Security Requirements Repository.

As a first preparation step, the 114 mandatory requirements of the BSI C5 catalogue were selected and listed in an Excel table. When consulting the Security Requirements Repository, it showed that 83 requirements (labelled *no gap*) of BSI C5 are already covered by STAR Attestation due to the mappings. These 83 requirements were found to be semantically equivalent to those of the repository (CCM), and hence were not to be audited as they were already covered by the STAR. The remaining 31 controls not covered by the existing STAR attestation were collected in a T4.4-repository.

The report from this pilot exercise made a series of positive conclusions about using the MPRF to conduct the ISAE3000-based audit.

- The framework's technical aspects and expert work are sound and thorough
- Applying MPRF "substantially reduced the workload" for a BSI C5 2016 audit, coming from a STAR attestation and aiming at BSI C5
- By adhering to the framework, the pilot participants reduced an initial 114 BSI C5 requirements down to an auditable delta of 27 This figure is in line with a result in D1.2, that the absolute percentage of matching between all the requirements in the repository and CCM is 78%
- During the activities, Fabasoft and PwC were able to eventually reduce the Delta (and consequently the workload) consecutively by including additional mappings and comparing interpretations to revise mappings to a *no gap*
- By adopting controls gap analysis, cross checking mappings and compensating controls, the indicators collected in the pilot clearly point toward an increased efficiency, especially for auditing efforts

- Both the auditor and auditee experienced increased efficiency when applying the MPRF in a more mature version
- The increased efficiency will initially be more impactful on the auditee's side because an auditor will currently check and verify the mappings and interpretations for nearly all requirements of the compared schemes. As the MPRF gets more mature and an auditor is more involved in MPRF-based audits, these efforts will decrease, and the framework will also yield increased efficiency for the auditor.

This task 4.4 had the objective of validating the soundness of the approach defined in Multiparty Recognition Framework life-cycle as well as testing the portion of the framework based on the ISAE3000 auditing and attestation standard. The pilot tested the steps to enable possible recognition between CSA STAR Attestation and BSI C5.

The results show that the framework is based on solid and highly functional work and is usable already in its current stage of development; the application of the Multiparty Recognition approach allowed the comparability between STAR Attestation and BSI C5 and showed that its real-life application could indeed lead to saving time and resource from the perspective of an auditee that wants to achieve compliance with both the requirements of CSA STAR Attestation and BSI 5. This pilot also indicated some important areas of improvement which are covered below in chapter 5.

4 TOOLS READINESS ASSESSMENT RESULTS

One of the goals of the project is to test the readiness of EU-SEC tools proposed in WP3. This section addresses the readiness of the tools used in the pilot exercises and presents a summary of their fitness for purpose. As noted in deliverable 3.3 relating to architecture and tools for evidence storage, many existing cloud security certification procedures are manual in nature, and consequently sub-optimal from an efficiency and effectiveness point of view.

All four pilot projects addressed the readiness level of MPRF as a tool or framework; pilot 4.3 additionally addressed the readiness of Nuvla as a tool that is used as the evidence store, which is managed and provided by Nuvla. The readiness assessment performed is about the evidence store and its integration with Nuvla that already ranks at the highest level of 9 under the TLA methodology as outlined in D1.1.

In 4.3, the auditor NIXU requested the auditee SixSq to provide some reasonable evidence as a proof of compliance. Given that this task's objectives are mostly about assessment and testing, the requested evidence was chosen to fit tightly with the auditee's scope while meeting different certification requirements, and to be sufficiently diverse to allow the participants to test the evidence store which was in place and integrated with Nuvla. The auditor requested the following types of evidence:

- access control logs from one of the digital assets included in the ISMS Asset Inventory
- security policies used in a software repository
- physical security of the offices.

The auditee saved all the evidence records in the EU-SEC Evidence Store through Nuvla, and later shared them with the auditor for a practical assessment of the tool's capabilities and usefulness. NIXU tested the evidence storage as part of the T4.3 pilot and confirmed that all test evidence was stored as supposed. It observed that the evidence storage allows efficient filtering and customisable searches that allow the auditor to find specific information among the data in the evidence store.

Here is a summary of the findings of each pilot; in the next chapter, recommendations for improvements to the framework and tools are presented.

Project 4.1 found that by using the EU-SEC repository and adhering to the MPRF process, it had almost 80% fewer security requirements that were needed to be used in an audit, while the MPRF reduced the workload of the audit process and increased its efficiency. This audit used CSA CCM as a tool, and this has the maximum TRL score of 9.

Pilot 4.2 found the EU-SEC Requirements and Controls Repository proved to be "a beneficial tool for mapping and creating smaller sets of requirements and controls when stepping from one requirements' scheme to another".

- For the auditee, the EU-SEC framework provides significant potential to reduce the effort and resources needed to achieve multiple certifications
- Auditors observed that the actual auditing process was not affected when using MPRF.

"EU-SEC Requirements and Controls Repository has been proven to be a beneficial tool to mapping and creating smaller sets of requirements and controls when stepping from one requirements' scheme to another," the report 4.2 said.

Report D4.3 noted: "…there is an obvious upside of using the EU-SEC framework and tools, in the sense that it allows the auditee to exponentially decrease the future effort for acquiring other certifications."

It is worth emphasising the point that the TRL assessments outlined in this section aimed only to evaluate the technology tools EU-SEC has developed to help with partly automating the assessment process. Both the evidence repository and the requirements repository had a maximum TRL score of 9. This section should not be interpreted as an evaluation of the MPRF concept and structures themselves. More details on the assessment methodology and definitions of the tools can be found in D1.1 and D3.3.

5 CONCLUSIONS AND RECOMMENDATIONS

The four pilot projects in this working package shared two primary objectives: firstly, to test whether the theory behind MPRF would work successfully in practice (precious feedback gained, which we will use to further improve the MPRF and EU-SEC in total in D2.5), and secondly, to gain useful feedback from both an auditor and auditee about working with the framework in a practical setting. The conclusions presented here show that both objectives were achieved. This section outlines a summary of the conclusions from each pilot, followed by the recommendations from each exercise for the next phase of development.

5.1 CONCLUSIONS

The pilot use cases showed that the MPRF's theoretical model successfully worked in a real-life situation. The EU SEC requirements and controls repository worked as a "fundamental building block" of the MPRF. The repository included all the security requirements for the framework needed for this specific audit.

By using the EU-SEC repository and adhering to the MPRF process, pilot project 4.1 found the following outcomes:

- Almost 80% fewer security requirements that were needed to be used in an audit
- MPRF reduced the workload of the audit process and increased its efficiency

- Comparing security controls between ISO 27001, ISO 27017 and Slovenian national requirements were compared through already working CSA CCM, which gives EU-SEC MPRF higher level of trust and usability
- This first application of the MPRF was time-consuming and slow due to the lack of guidelines and supporting documentation. Both the auditee and auditor had not yet had practical experience with real-life implementation of the framework.

A possible explanation for the time taken to complete pilot 4.1 is the novel nature of the EU-SEC project and the new approach to the audit process in the pilot use case. At that time, the MPRF had yet to be tested and perfected for real-world use. Although the project partners carried out a real assessment, this was a pilot use case in which the roles and responsibilities of the auditor and the auditee were "slightly blurred", according to the report. This caused delays in performing the task.

In addition, although the certification audit mechanism comparison did not differ from a common ISO 27001 audit, pilot 4.1 required some further effort in order to be executed successfully. Additional steps were added for the second phase of the pilot, in order to validate mappings, create compensating controls and test the framework. (All of the required compensating controls were designed by the CSA and incorporated in the EU SEC repository during this pilot.) Another caveat to note is that the pilot was limited in scope, and therefore it did not provide a full picture on how collection and comparison would work in real life.

The experience from the pilot audit 4.2 shows that the MPRF process can be followed to achieve mutual recognition between certification schemes. The two principal conclusions from pilot 4.2 were that adopting EU-SEC framework has the potential to deliver valuable benefits for auditees and for auditors.

An additional outcome of the project was the stakeholders' decision to use the MPRF approach by extending onboarding methodology for cloud services within the Slovak G-Cloud. However, the report notes that guidelines for comparing schemes with the framework are desirable in order to use MPRF efficiently, and to work with internal rules within government.

The auditing experience for pilot 4.3 concluded that using the MPRF might not bring significant added value in this specific case, since ISO 27001 and ISO 27017 largely overlap. But it was also clear that using the framework does not affect the overall auditing process, which makes its adoption more appealing for both auditees and auditors.

For pilot 4.4, the conclusion was that the MPRF showed "a good level of maturity" in its current form, giving auditees a useful tool for comparing schemes and requirements. It also enabled them to align their own implementation of security controls make it easier to attain certifications they might want to comply with in the future.

5.2 RECOMMENDATIONS

Two principal recommendations were common to all four pilot exercises 4.1-4.4. One was the need for **additional supporting documentation and guidelines for MPRF**. Several project partners said these manuals would help to explain and clarify the model, to help auditees to prepare for it and auditors to execute it.

In addition, many of the participants found that using a spreadsheet as the requirements and controls repository for MPRF had limitations. Instead, they recommended **building a database with a user-friendly interface for the repository**, as it would improve its usability and efficiency, and consequently improve the framework.

These were the following specific recommendations from exercise 4.1:

- Due to N:N mapping of the extensive number of different requirements (804) to one or more corresponding CCM controls (133), the Excel spreadsheet becomes non-transparent and as such difficult to handle. **The partners recommend building the EU-SEC requirements and controls in a database, which will significantly improve the repository's usability and efficiency**. The application should provide a simple interface for adding and mapping new requirements to it and to extract required EU-SEC requirements and controls from it when acquiring new compliance.

- **Further verification is needed to raise the maturity level of EU-SEC requirements and controls repository**. This would be done executing the change management process defined in D2.4 EU SEC Framework. Through the security controls comparison, the differences and inconsistency in mapping execution were discovered. This finding shows on different subjective opinions when mappings of ISO 27001 and ISO 27017 to CCM were performed.

As noted above, the recommendations from pilot exercises 4.2 and 4.3 centre on improving the MPRF process description, providing guidance and instructions to clarify each phase of the

process in more detail for auditors and auditees. We are listing them together because the summaries in each report closely match each other. The specific recommendations from the reports 4.2 and 4.3 are to improve the following instructions:

- How to access the MPRF for auditee and audit
- How to use the Multiparty Recognition Database for requirement mapping and building an efficient statement of applicability
- How to use the Requirements Repository for GAP analysis and validation of deltas and compensating controls
- How to conduct an MPRF-based audit.
- To perform and validate all mappings in advance before starting the actual audit process, and to use only existing and implemented national requirements
- To consider using ontology approach for automation of mapping requirements and controls in the future.

Some of the suggested recommendations from exercise 4.3 could be implemented during the EU-SEC project, but the deliverable notes that other recommendations might require more time and resources. As observed in the other deliverables, participants from 4.3 also recommended using a database for the repository, with a simple interface for easily extracting new requirements and controls when acquiring new certifications. This would help the auditee when creating deltas and compensating controls. Other recommendations from exercise 4.3 include:

1) **Further evaluate and improve mapping of the controls through a defined change management process**: Mapping of the EU-SEC requirements and controls repository (D1.2) is not consistent. During the pilot both auditee and auditor with the support of the CSA identified and fixed inconsistencies in some of the mappings defined in D.1.2. Moreover in some cases it appears that too many CCM controls have been mapped to ISO 27017.
2) **Highlight the MPRF's applicability to any company looking to obtain multiple certifications, not just cloud service providers**: throughout the definition of the MPRF, CSPs and respective sector-specific auditors are referenced as the main recipients of this framework. As concluded from this pilot, where the auditee is better described as a CSB, no applicable differences were identified when using the framework.

3) **Refine mapping to eliminate inconsistencies in the repository**: the exercise found that some CCM controls were mapped multiple times to the same requirement. This was attributed to a flaw in the current repository format, which moving to a database would address. The exercise also uncovered overlapping requirements that sometimes had different gap analysis.

4) For this kind of audit (starting from an existing certification and aiming for another), using the framework might be not possible unless **all the reverse mappings from the CCM to the desired certification also exist and are part of the EU-SEC repository**. Before the audit happens, the MPRF needs to already have all the mappings between the respective schemes in scope.

5) The MPRF's effectiveness and efficiencies will be more obvious when CSPs extend the scope of its compliance beyond two standards, ISO27001 and 27017 in this case, and **aim to cover multiple national, regional or sectoral requirements**.

6) **Build a storyboard as part of the EU-SEC dissemination plans and framework usage manuals**, explaining the motivation for using the framework, when to use it, and how.

The other specific recommendations from exercise 4.4 were as follows:

- To focus further efforts not on operational applicability, but on **improving the quality of the requirements interpretation and mapping process** and the usability of the MPRF.

- **To get preliminary interpretations and expert opinions** and then an 'appropriate experts group' either accepts or rejects the change of the mapping in the Security Requirements Repository. This task would fall into the jurisdiction of the Governing Body and is upcoming project work to be done in D2.5.

- Focus on **guidelines to help stakeholders, scheme owners, auditors and auditees to apply the tool**. This report elaborated on the reason for doing so, noting that if auditees understand the benefits, they will ask auditors to perform an MPRF-based audit. This in turn will create market demand and would accelerate adoption of the framework.

"The Security Requirements Repository should clearly help even auditees with the scoping activities for an audit and give the user guidance at hand to navigate from the requirements of one certification scheme to another (according to the mapping). The idea is to exploit the Framework's ability to offer users comparability and trust in collected evidences and applied

technical implementation across certification or attestation schemes. If the benefits are visible and easy to access, the Framework will find early adopters beyond the project consortium," the report says.

As per the previous pilots, the report from exercise 4.4 recommends transferring the EU-SEC Framework's Security Requirements Repository into a database. It further clarifies the reasons for recommending this approach, explaining that it would:

- Better support the linking of requirements by their mapping relationships
- Reduce potential human error significantly by detailing the mapping between various standards
- Increase market adoption by being easier to use.

5.3 SUMMARY

After the four pilot use cases, we feel confident in stating that an organisation seeking to become certified to multiple security standards may now do so without needing to go through multiple full audits but focusing only on the components of each respective standard where there is no overlap.

The results presented in this report demonstrate that the theoretical model of the MPRF successfully works in practice, and moreover that the framework offers considerable benefits for all stakeholders in the cloud computing security and privacy compliance arena. The MPRF has been shown to streamline the compliance process by identifying common or duplicate areas between differing certification standards. The MPRF has also been shown to significantly reduce the time and resources involved in preparing for an audit.

The pilot exercises revealed no issues that would prevent the framework from being used in practice. However, they were valuable in highlighting areas for improvement in the theoretical model, processes and activities. For example, one caveat in the findings from report 4.4 is that the experience was "highly susceptible" to the professional interpretation of auditors and certificate issuing bodies. It noted that the framework will need to address this in the future.

In addition, the pilot exercises shed light on some current gaps in understanding about the framework, which could have hindered the preparation and auditing process, causing it to

require more time to complete. All of the pilot project reports 4.1-4.4 noted that better supporting documentation and guidelines would address this shortcoming.

As noted in pilot 4.4, usability is critical to the framework's adoption. "Using the MPRF should not cost more time when going through the requirements of certificates and mapping them, than having to do so without having such a tool," it said.

Many of the issues raised were common to all four pilots. This commonality suggests a clear path to follow for the remaining working packages of this project. For example, it is already planned that WP6 will address the recommendation for supporting documentation and guidelines. EU-SEC aims to develop this material through a series of workshops, conferences and other activities.

ANNEX A: PRINCIPLES-CRITERIA-REQUIREMENTS QUESTIONNAIRE

Part A – Criteria's Questionnaire

C.1. Comparability of requirements

Are the requirements in different compliance/certification schemes comparable, and thus possible to be mapped to each other for any gaps to be identified?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, ISO 27017and SI national has many overlaps with ISO 27001	Yes. NIXU was audited against ISO27000, ISO 27017 and Slovak national requirements.	Yes. ISO 27017 has many overlaps with ISO 27001 and a direct correlation with the same. It can be seen as an extension of ISO 27001	Yes, for T4.4 they were: PwC investigated SOC2, CCM (for STAR), BSI C5

Auditors:

NIXU	PwC
Yes. Possible, thus still requires lot of work. It was expected in the pilot, most issues came from the validation of mappings (excel spreadsheet). Some difficulties as semantics between controls in each compliance scheme differs.	Yes, but this can not reflect the reality, entirely. The controls which are implemented at the CSP are also important to consider.

C.2. Comparability of auditing mechanisms

Are test procedures executed and metrics used in an audit comparable and resulting in the same level of assurance / audit comfort?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, for all schemes ISO based audit is executed	Yes	Yes, ISO 27007 defines all the necessary	Yes, PwC was able to audit experts from

		processes for this audit	Fabasoft like they "normally" would.

Auditors:

NIXU	PwC
Yes	Depends, consider e.g. Type 1 (Design Suitability) and Type 2 (Operating effectiveness).

Do audits refer to or require compliance to a named code of practice(s), e.g., BSI C5 requires the auditor to apply the ISAE 3000?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Don't know	Yes	Don't know	The question is not quite clear, but yes… in T4.4 the schemes did that.

Auditors:

NIXU	PwC
Yes	Yes

C.3. Suitability of evidence

Is evidence collected "suitable evidence", that is accurate, reliable and suitable to support the audit conclusions?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes	Yes

Auditors:

NIXU	PwC
Yes	Yes. Also important is professional judgment.

C.4. Auditor qualification

Are the auditors' qualifications transparent and well defined?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. Each auditor and NIXU itself have explicitly shared their qualifications	Yes, for all investigated schemes in T4.4

Auditors:

NIXU	PwC
Yes	Yes

Are auditors required to demonstrate knowledge of the cloud sector and be qualified to perform assessments in line with relevant auditing standards?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, the auditors need to have ISO 27001 Lead Auditor certification.	Yes	Yes, for T4.3 the auditors need to have ISO 27001 Lead Auditor certification	Yes, for at least BSI C5 and STAR Attestation, investigated in T4.4

Auditors:

NIXU	PwC
Yes	This is a requirement – only with the right knowledge, the auditor can address certain Cloud-specifics risks.

Are auditors required to demonstrate relevant formal education and personal certifications, minimum work experience, adherence to Code of Professional Ethics as well as training and continued professional education?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, it is presumed by trusting the auditing entity NIXU	Yes all people form NIXU shows their experience	It is presumed, not explicit, by trusting the auditing entity (NIXU) which by itself is publicly qualified to conduct the audit	Yes, for BSI C5, at least half of the auditing team has to bring these qualifications.

Auditors:

NIXU	PwC
Yes, as all requirements are in place already in required certifications to auditors. And to organization performing the audits.	see Fabasoft's response

C.5. Governance model

Do the compliance/certification schemes have a transparent and a well-defined governance model with an independent standard setting body which is free of any possible conflict of interest?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	For ISO it was clear and Slovak governance for certification is under construction	NIXU?	STAR Attestation relies on the Open Framework Community, BSI C5 does not have a specific governance model, to our knowledge.

Auditors:

NIXU	PwC
Yes	see Fabasoft's response

Do the governance models use a change management process to ensure that the standard stays fit for purpose and

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Not as we know	NIXU?	Not to our knowledge

Auditors:

NIXU	PwC
Yes	see Fabasoft's response

Part B – Requirements Questionnaire

R1: Comparability of Control Framework

R1.1 Has the EU-SEC Governing Body performed the mapping and gap analysis of requirements of different certification schemes?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, involved task partners played the role of Governance Body	Yes	Yes, if we assume the project's TM as the temporary GB	Yes, the "preliminary Governing Body"

Auditors:

NIXU	PwC
No such body implemented yet, initial mapping of requirements was performed as part of T1.2, further mappings were performed by CSA and involved parties (auditees and auditors) and as such acting as one in pilot audits.	Yes, the simulated GB did support on this

R1.2 Has the EU-SEC Governing Body determined the nature of the gaps between the requirements of different certification schemes?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, involved task partners played the role of Governance Body	Yes	Yes, if we assume the project's TM as the temporary GB	Yes, again the "preliminary Governing Body"

Auditors:

NIXU	PwC
No such body implemented yet, initial gap analysis was done as part of T1.2, but the nature of the gap and the compensating controls were identified during the pilots by CSA and involved parties (auditees and auditors) and as such acting as one in pilot audits.	Yes, the simulated GB did support on this

R1.3 Has the EU-SEC Governing Body suggested the compensating requirements to bridge the identified gaps between the requirements of different certification schemes?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, involved task partners played the role of Governance Body	Yes	Yes, if we assume the project's TM as the temporary GB	Yes, also the "preliminary Governing Body"

Auditors:

NIXU	PwC
No such body implemented yet, initial gap analysis was done as part of T1.2, but the nature of the gap and the compensating controls were identified during the pilots by CSA and involved parties (auditees and auditors) and as such acting as one in pilot audits.	Yes, the simulated GB did support on this

R.1.4. Has the EU-SEC Governing Body adopted a clear, well documented and transparent approach for performing a comparison and gap analysis between requirements of different security frameworks?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Not yet	Not at all because framework is still in construction not all aspects are clear. It is written in conclusions	The governance of the compliance schemes in MPRF was not conducted. In the pilot, only ISO-based processes were used	Hard to tell. From our experience, the auditor wasn't always sure what to do. So we suggest that there is room for improvement here.

Auditors:

NIXU	PwC
No, still lot work to be done in this area.	See NIXU's response

Notes:
Additional operating instructions would be desirable. The auditors need reassurance that mutual recognition is doable. It needs to be simple and understandable how the requirements from different schemes can be compared and managed under the EU-SEC framework.

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes (assumed for the use case)	Yes	Ideally yes, but the pilot experience indicated that the auditor might not	For D4.4 we had to assume that.

		always agree with the proposed mappings.	

Auditors:

NIXU	PwC
Depends, not evaluated.	Not yet.

R2:Comparability of Auditing Mechanisms

R2.1 Does the Authorized Auditor (as required by the Authority) use control procedures and metrics that are comparable and are resulting in the same level of assurance?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. NIXU?	Yes

Auditors:

NIXU	PwC
Yes, in ISO audits standards were used, CSA CCM used and in line with ISO, no additional requirements set in any national body.	Yes

R2.2. Does the Authorized Auditor (as required by the Authority) perform audits which refer to or require compliance to a named code of practice(s)?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	They do with scheme	Yes. ISO 27007	Yes

Auditors:

NIXU	PwC
Yes	Yes

R2.3 Does the Authorized Auditor (as required by the Authority) accept to perform an audit on a scope that is considered as relevant?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes	Yes, for T4.4. For BSI C5 the scope is

			always “all domains”

Auditors:

NIXU	PwC
Yes	See Fabasoft’s response

R3: Suitability of Evidence

R3.1 Does the Authorized Auditor (as required by the Authority) collect evidence that needs to be appropriate, sufficient, selective and persuasive, providing an extent of information and guidance of procedure for a reasonable audit?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. Even though the three types (used in T4.3) of evidence might not be sufficient to cover the full extent of the audit, they are fine grained enough and suitable for the verification of multiple ISO based controls.	Yes

Auditors:

NIXU	PwC
Yes, evidence was collected as required by ISO	Yes

R3.2 Does the Authorized Auditor (as required by the Authority) determine the timeframe of collected evidence?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	The requested evidence was to be	The schemes do.

		collected at the last stage of the audit process, and stored in the evidence management solution proposed by EU-SEC, for an indefinite time period. The auditor has access to this evidence at any time.	

Auditors:

NIXU	PwC
Yes	Yes

R3.3 Does the Authorized Auditor (as required by the Authority) identify the criteria against which evidence is needed to be audited in order to secure understandability and correctness of conclusions?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. The requested evidence fulfils the criteria C.3 and have been individually mapped to the corresponding ISO controls (refer to D4.3): • E.1) maps to IAM-04, DCS-07, EKM-02, GRM-04, HRS-05, IAM-02, IAM-05 and IAM-01 in the CCM, with no gaps in the EU-SEC requirements	Yes.

		and controls (requirement domain is not defined however); • E.2) maps to GRM-06 in the CCM, with no gaps in the EU-SEC requirements and controls; • E.3) maps to DCS-02, DCS-06, DCS-07 and DCS-09 in the CCM, with no gaps in the EU-SEC requirements and controls	

Auditors:

NIXU	PwC
Yes	Yes

R3.4 Does the Authorized Auditor (as required by the Authority) record audit findings to enable informed decision on compliance with the requirements?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. The three different evidence types were chosen specifically to cover different type of evidence format: • E.1) text logs which can easily be stored digitally;	Yes

		• E.2) a reference or screenshot of an existing software configuration where the security policies have been applied; • E.3) and a visual proof (manually obtained) of the physical security. All evidence records were saved and made accessible to the auditor at any time, through the evidence store.	

Auditors:

NIXU	PwC
Yes	Yes

R3.5 Does the Authorized Auditor (as required by the Authority) record nonconformities with specific requirements and contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Probably Yes (final confidential report is not finished)	Yes	Any of the required evidence could be easily mapped to a nonconformity. These would need to be recorded by the auditor itself. The original evidence record provides an	Yes

		absolute and unique reference which can be used to access it (digitally) from wherever the nonconformity would be.	

Auditors:

NIXU	PwC
Yes, thus keep in mind pilot-based approach the auditing activities were done on limited scope to prove that the auditee's compliance can be assessed by the use of MPRF.	Yes

R3.6 Does the Authorized Auditor (as required by the Authority) follow a consistent and relevant sampling approach in the collection of evidence?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Sampling was ensured by the auditee itself when generated the evidence records E.1	Yes

Auditors:

NIXU	PwC
Yes, ISO.	Yes

R4:Auditor Qualification

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Don't know	Yes	Not applicable in T4.3.	Don't know

Auditors:

NIXU	PwC
Yes, evaluation done in pilot. Thus as Governing body is currently not officially in place the evaluation is based on the table top exercise - but yes, would have passed the actual process.	No answer possible

R4.2 Does the Authorized Auditor (as required by the Authority) lead the auditing or assessment engagement as required by standards and schemes in the scope of the engagement?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. The auditors were qualified for the audit and followed the processes mandated in ISO 27007	Yes

Auditors:

NIXU	PwC
Yes	Yes

R4.3 Does the Authorized Auditor (as required by the Authority) have sufficient subject matter expertise and knowledge to allow for professional judgement based on relevant expertise that is supported by relevant professional certifications?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. The auditors personal qualifications are stated in D4.3	Yes

Auditors:

NIXU	PwC
Yes	Yes

R4.4 Does the Authorized Auditor (as required by the Authority) have sufficient number of personnel with adequate professional experience to conduct the audit or assessment engagement?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes. T4.3 had 2 auditors from NIXU	Yes

Auditors:

NIXU	PwC
Yes	Yes

R4.5 Does the Authorized Auditor (as required by the Authority) adhere to the Code of Professional Ethics?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	Yes? NIXU	Yes

Auditors:

NIXU	PwC
Yes	Yes

R5:Governance Model

R5.1 Has the EU-SEC Governing Body allowed for mutual recognition only between schemes that have a well-defined, transparent and documented governance structures?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
N/A	We as pilot auditee initiate the process of comparison of Slovak requirements against EU-SEC framework	N/A	N/A

Auditors:

NIXU	PwC
Yes it is defined, tested in theory, thus will need to be proved in real-life audits.	As far as it is understood: yes.

R5.2 Has the EU-SEC Governing Body allowed for mutual recognition only between schemes that have a governance structure that guarantee independency and prevent any possible conflict of interest?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
N/A	Yes	N/A	N/A

Auditors:

NIXU	PwC
Yes	Yes

R5.3 Does the governance structure of the certification schemes under comparison envisage mechanisms for the collection of complaints?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
No, not sure	Yes	Don't know	No

Auditors:

NIXU	PwC
Yes, complaint management exists under the ISO standardization structure, however it was not tested in pilots.	Yes

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, not sure	I don't know	Don't know	Yes, to our knowledge

Auditors:

NIXU	PwC
YES, ISO 27001 Certification Body (who audits and grants certifications) is controlled by national Accreditations Body. Accreditation Body has accredited Certification Body to grant	As far as it is understood, no. This would contradict the status of audit firms and may clash with their code of conduct / relevant

certifications and has the obligation to audit that Certification Body is in conformity with relevant standards (ISO 17021 being perhaps the most important. Accreditation Body's surveillance comes in the main instruments: annual audits and the obligation of the Certification Body to conduct internal audits. In ISO 27001 the scheme owner is ISO, but it is purely an organization to develop and maintain standards. In a way, ISO has delegated the surveillance to national accreditation bodies.	regulation / confidentiality requirements etc.

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, not sure	No	Don't know	Yes, where applicable

Auditors:

NIXU	PwC
Yes	Yes, but should be detailed further

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	I don't know	Don't know	Not with all schemes*

Auditors:

NIXU	PwC
Yes, Thus is really formalized and changes are not fast to adapt. (ISO)	See Fabasoft's response

*BSI C5 - no official process available to us, even though it was communicated that it exists.

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, not sure	I don't know	Don't know	Yes

Auditors:

NIXU	PwC
Yes, thus example in Finland it is SFS (ISO National Body) which is part of the decision-making mechanisms. If required organization could try to push changes through that, not directly.	Not yet, from our point of view

R5.8 Is the EU-SEC Security Requirements Repository audited by accredited auditors?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes, not sure	/	An accredited auditor did validate the repository	Don't know

Auditors:

NIXU	PwC
Yes	Not yet, but however a good idea.

R5.9 Has the Authority maintained a publicly available register of Authorized Auditors?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
No, not sure	I don't know	Not applicable, but no.	Yes, to our knowledge

Auditors:

NIXU	PwC
Yes, if we are talking about ISO, typically national bodies	CSA STAR yes, BSI C5 no

R5.10 Has the Authority maintained a register of Certified CSPs and made publicly available?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
No	I don't know	Same as above	Cannot answer

Auditors:

NIXU	PwC
Yes, upon request	CSA STAR yes, BSI C5 no

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

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Not to our knowledge	Yes	Not to our knowledge	Not to our knowledge

Auditors:

NIXU	PwC
Yes. It is documented in the requirements repository as a result of T1.2 but this document is a snapshot on a certain point in time and it needs to be appropriately governed in future.	Not to our knowledge

R5.12 Does the Authority periodically audit the Authorized Auditors to maintain acceptable level of quality?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Not sure	Yes	Not sure? NIXU?	Yes, to our knowledge

Auditors:

NIXU	PwC

Yes	No see R5.4

Part C – Principles Questionnaire

P1. The repeatability principle

Are the results the same when two different entities conduct an independent audit of the same security/privacy requirements of an information system, under the same scope and conditions?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	Yes	It should be, as the final SoA is quite objective.	With respect to our learnings in T4.4 we would say: the result yes.

Auditors:

NIXU	PwC
Yes and no, for instance in ISO audits, samples are commonly used, selection is always based on the auditor's decision and knowledge, there are always small deviations, thus mostly only minor and no influence on certification itself.	Yes

P2. The equivalence principle

Is the_security/privacy level in two information systems equivalent when a security/privacy requirement that is assessed in these two independent information systems and the evidences collected or the measurement results are the same?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Probably not exactly the same	I don't know	No. They might overlap but that doesn't mean they are exactly the same.	Cannot answer.

Auditors:

NIXU	PwC
Yes	Probably – depends on further safeguards / controls not in scope

P3. The relevancy principle

Are the security/privacy requirements and the associated processes used for assessing an information system selected so as to provide actionable information to the auditee?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Probably yes	Not now, but after end of project when the guidance will be on place	I guess so…	?

Auditors:

NIXU	PwC
Yes. Within the ISO standards the auditee can define the scope of certification based on their needs.	Depends on the auditor and further, project-specific agreements (as well as the motivation of the auditee to learn from audit results)

P4. Trustworthiness principle

Is the process of collecting, verifying and evaluating evidence against audit criteria transparent, unbiased, complete and unambiguous in order to provide a trustworthy representation of the security/privacy level provided by an information system?

Auditees:

SI-MPA	MFSR	SIXSQ	Fabasoft
Yes	I don't know	What is the process of collecting? Who defines it?	Yes

Auditors:

NIXU	PwC
Yes, different collection methods used in pilots.	Yes