EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D6.3 INTERIM REPORT ON DISSEMINATION STANDARDISATION AND EXPLOITATION

VERSION 1.1

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 31.12.2018	DELIVERY DATE: 21.01.2019
AUTHOR: CSA	PARTNERS CONTRIBUTED: SixSq, Fabasoft
DISSEMINATION LEVEL:* Public	NATURE OF THE DELIVERABLE:** R
INTERNAL REVIEWERS: MFSR, SI-MPA	

*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

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	21/01/2019	Initial Version	Damir Savanovic, CSA Louise Merifield, SixSq
1.1	24/05/2019	Updates regarding KPIs, workshop description and conclusion section	Damir Savanovic, CSA Louise Merifield, SixSq

EXECUTIVE SUMMARY

The report outlines the dissemination, standardisation and exploitation activities of the EU-SEC project in its first two years, from 1 January 2017 to 31 December 2018. It summarises progress related to those activities, including online communication, internal and external communication. In addition, the report defines upcoming priorities and tasks in the third year.

ABBREVIATIONS

AB	Advisory Board
AP	Action Point
API	Application Programming Interface
CENELEC	European Committee for Standardisation
CIO	Chief Information Officer
CSA CCM	Cloud Security Alliance's Cloud Control Matrix
CSA	Cloud Security Alliance (Europe) LBG
CSC	Cloud Service Customer
C-SIG	Cloud-Select Industry Group
CSP	Cloud Service Provider
DS	Dissemination Strategy
DSM	Digital Single Market
e.g.	for example
EC	European Commission
EC C-SIG	European Commission Cloud-Select Industry Group
EDPB	European Data Protection Board
ENISA	European Network and Information Security Agency
etc.	et cetera
ETSI	European Telecommunication Standards Institute
EU	European Union
EU-SEC	European Security Certification Framework
Fabasoft	Fabasoft R&D GmbH

Fraunhofer	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
GDPR	General Data Protection Regulation
H2020	Horizon 2020
i.e.	*id est* (It is)
ICT	Information and Communication Technology
IoT	Internet of Things
IPR	Intellectual Property Rules
ISC	International Standardisation Council
ISO	International Organization for Standardisation
ISO/IEC	International Organization for Standardisation/International Electrotechnical Commission
KPI	Key Performance Indicator
MF-SR	Ministerstvo financii Slovenskej republiky
MPRF	Multi-Party Recognition Framework
n.a.	not applicable
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NIXU	Nixu Oyj
PwC	PricewaterhouseCoopers GmbH WPG
SDO	Standards Development Organization
SI-MPA	Ministry of Public Administration
SIXSQ	SixSq Sàrl
SME	Small and Medium-sized Enterprise

tbd.	To be defined
WG	Working Group
WP	Work Package
WP29	Article 29 Data Protection Working Party

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

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

Table 1. Terms and definitions

Term	Definition	Source
Accreditation	Accreditation assures users of the competence and impartiality of the body accredited.	http://www.iaf.nu/
Addendum	A set of complementary requirements that is found to be missing from a certification scheme Y (and hence added to Y), after a gap analysis between schemes X and Y has been performed.	https://cloudsecurityalliance.org/artifacts/ccm-c5/
Assessment	Refers in this document to risk assessment, which overall process of *risk identification [ISO Guide 73:2009, definition 3.5.1], risk analysis [ISO Guide 73:2009, definition 3.6.1]* and *risk evaluation [ISO Guide 73:2009, definition 3.7.1]*.	ISO Guide 73:2009, definition 3.4.1
Attestation	An issue of a statement that conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees.	ISO 17000:2004, 5.2
Audit	A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled	ISO/IEC 19011:2011, 3.1
Audit criteria	Set of policies, procedures or requirements used as a reference against which *audit evidence* is compared Note 1: Policies, procedures and requirements include any relevant Service Qualitative Objectives (SQOs) or Service Level Objectives (SLOs).	ISO/IEC 19011:2011, 3.2

Term	Definition	Source
Auditee	Organization being audited.	ISO 9000:2005, definition 3.9.8
Auditor	Person who conducts an audit.	ISO/IEC 19011:2011, definition 3.8
Authority	A trusted party that is responsible for the correct organization of a certification scheme, including the accreditation of auditors and keeping a registry of certified cloud services.	
Authorized Auditor	An auditing organization/auditor authorized by the certification authority/scheme owner to conduct assessments against the requirements of the scheme. A certification body is considered as an authorized auditor.	
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	https://www.iso.org/certification.html
Certification scheme	The set of rules, requirements and mechanisms that govern the process of certifying a process or a product. **NOTE**: In this document we use interchangeably "certification scheme" and "compliance scheme" noting that in the real term 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 [1]
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.	

Term	Definition	Source
Cloud service customer	A body that contracted a cloud service.	
Cloud service provider	A third-party company offering a cloud service.	
Continuous auditing	Continuous auditing is an automatic method used to perform auditing activities, such as control and risk assessments, on a more frequent basis.	
Control	A safeguard or countermeasure requirement prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	CCM mapping methodology
EU-SEC Security Requirements Repository	A repository of all collected requirements mapped against the CSA CCM, making it a native control framework to address the identified requirements	EU-SEC D1.2 v1.2 [2]
Governance Body	A body responsible for governance of the Multiparty 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-based security decisions to adequately protect organization information.	NIST SP 800-57
Management system	System to establish policy and objectives to achieve those policies.	ISO 9000:2005, definition 3.2.2

Term	Definition	Source
Multiparty 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
Scheme Owner	The organization (individual, for-profit corporation, not-for-profit corporation, certification body, government department, agency or other body, trade association, group of certification bodies or other just about any other body or group of bodies) that is responsible for the development and maintenance of the scheme and owns the intellectual property, copyright, trademarks and other rights to a certification scheme.	
Software-as-a-Service	Software as a service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).	

1 INTRODUCTION

A critical element of the work of the EU-SEC project is that the results of its respective work packages are disseminated and brought to the attention of the relevant target audiences, as a means to maximizing their value proposition and market uptake. To this end, the drafting and enacting of an efficient and well organised communication strategy for the dissemination, exploitation and standardisation of such results was deemed imperative (ref. D6.1).

In this report, the results derived from the implementation of the project's communication strategy and dissemination activities are presented. The activities of this task and respective results are organised and presented under three main pillars, namely, dissemination, exploitation and standardisation, which collectively target the increase of user trust in ICT products and services and the long-term sustainability of the EU-SEC certification framework.

Various dissemination activities took place throughout EU-SEC communication channels, such as social media applications[1], website portals (including the EU-SEC project's website[2]), presentations at international conferences and industry seminars (e.g., infosecurity Europe 5-7 June 2018[3]). Moreover, within the same activities, a series of workshops (e.g., "Join the workshop on European Security Certification"[4]) were organized attended by various stakeholders, i.e. from industry, public bodies, researchers, standardisation experts, etc., supported by the preparation and distribution of project flyers[5] and publication of press releases.

In the context of standardisation activities, a strategy for orchestrating the EU-SEC project's contributions to relevant standards and best practices has already been developed (see D6.1). Participation in standardisation processes is expected to benefit the EU-SEC project in two

[1] https://twitter.com/EU_SEC, accessed on 19/12/18.

[2] https://www.sec-cert.eu, accessed on 19/12/18.

[3] https://www.infosecurityeurope.com/, accessed 19/12/18.

[4] https://sixsq.com/news/2018-09-04-news-eusec-workshop/, accessed on 19/12/18.

[5] https://cdn0.scrvt.com/fokus/65f3409bd0d759d9/0519855bbc41/EU-SEC_Flyer_170627.pdf, accessed on 19/12/18.

ways. On the one hand, it will bring higher international recognition to the project and new opportunities for collaboration, and on the other hand, it will widen the exploitation potential of project outputs, including providing the project with access to a large pool of external/international expertise. Several meetings in this respect have been held and more are planned to take place with various standardisation bodies in 2019, as a result of EU-SEC's multiparty recognition[6] (D2.1) and privacy code of conduct[7] (D2.3) deliverables. This involves, for example, ENISA, ETSI, CENELEC, EC DSM WG on Certification, BSI - German Federal Security Agency and others.

Exploitation activities of EU-SEC project results enabled all EU-SEC consortium partners, among them auditors and ICT companies, to exploit the project's results for their business by providing guidance though educational and training material, thought workshops, webinars, events and finally via the project website. Highlights are CSA's extension of the multiparty recognition approach to the USA program FedRAMP, and the launch of the CSA GDPR Centre of Excellence using the experience and findings from the works on the EU-SEC privacy code of conduct.

The EU-SEC framework will continue to help building trust in the use of ICT services. An early involvement of market players, organization of workshops with user communities, will help to better understand the market needs in the future. In addition, expected feedback from stakeholders gained by the dissemination, standardisation and exploitation will be used to optimize the framework and its components in terms of practicability and trans-European adoption.

1.1 SCOPE AND OBJECTIVES

The objective of this report is to provide a summary and assessment of findings with respect to the dissemination, standardisation and exploitation activities that took place up to the development of this current D6.3. version, by using EU-SEC project's work packages results.

[6] https://cdn0.scrvt.com/fokus/f93eb2159eeb8b18/d9091b56e4fd/6Multiparty-Recognition-Framework-for-Cloud-Security-Certifications-Draft.pdf, accessed on 19/12/2018.

[7] https://cdn0.scrvt.com/fokus/b46fac6d509ee426/724ab3e73ad4/8Privacy-Code-of-Conduct-Draft.pdf, accessed on 19/12/18.

The focus is on reporting the respective content that targets the following three main areas and their respective objectives:

1. **Dissemination**: Summarise and present the established and maintained mechanisms for effective communication and outreach that were used to share EU-SEC project results with the relevant target audiences on a timely basis and by the most effective means so as to achieve the broadest most possible outreach.
2. **Standardisation**: Summarise and present any actions for liaison with relevant standardisation bodies on the project's results to ensure that they become a generally accepted standard with high market update.
3. **Exploitation**: Summarise and present the consortium partners and how they have managed to exploit the EU-SEC project's results for their business by any means of educational and training material, through workshops, webinars, events and finally through the project's website, or other.

The scope of work involves the identification, collection, organization and listing of all activities, communication channels and respective material that was used up to this point of the project by all consortium partners in relation to the three aforementioned objectives. In addition, future dissemination, standardisation and exploitation plans that will collectively result in achieving the WP6 communication strategy's objectives are also to be provided, and are expected to be presented in the next updated version of this report at the end of the project.

1.2 DOCUMENT STRUCTURE

The content of the document is divided into three main categories and corresponding chapters called, dissemination, exploitation and standardisation.

In Chapter 2 the dissemination activities of EU-SEC project are presented, including the communication tools and channels used, the challenges met and achievements.

Similarly, the standardisation and exploitation activities, challenges, target groups, meetings and achievements are presented in chapters 3 and 4 respectively.

Finally, chapter 5 concludes the document and presents a summary of achievements, lessons learnt, and future planning of activities.

2 DISSEMINATION ACTIVITIES

2.1 CHALLENGES

All consortium members are committed to disseminating and exploiting the project's activities. The huge effort put into the technical work packages will be in vain if the project fails to communicate sufficiently with peers in the research field, industry, other commercial players and policymakers. Similar to many other research projects, however, the subject matter of the consortium's work can be complicated, confusing and uninteresting for a non-research audience. For this reason, the EU-SEC partners struggled to find the right path regarding dissemination in the first 18 months. Website activity was low and few documents other than deliverables were published. This resulted in disappointing results in terms of dissemination. The consortium is acutely aware of this and is committed to implement changes to remedy the situation.

In October 2018, CSA took over as leader of WP6 and implemented a review of the communications, including the website. A communication manger was appointed and is now active daily, with the mission of ensuring regular communication on the project's work, as well as undertaking a website review and improving activity on social media.

The consortium members are now focused on producing content which is easily understandable to its target audiences. It is recognised that communicating with appropriate stakeholders is essential to ensure success of the exploitation activities which will take place in 2019. Weekly meetings of WP6 now take place to ensure work stays on track and evolves with requirements.

2.2 TARGET GROUPS

Based on the goals of the project, the EU-SEC Consortium initially identified the following target audiences:

1. Auditors
2. Cloud Service Customer (CSC)

3. Cloud Service Provider (CSP) and Security Provider
4. Financial sector and other critical infrastructure service provider
5. Governments/Agencies
6. ICT Companies
7. Partners
8. Public Administrations
9. Scientific Community
10. Privacy Professionals
11. Public

2.3 ACHIEVEMENTS

The project has developed the following resources:

- Technical documentation
- Presentation slides
- Deliverable documents
- Website[8]
- Presentation of project on 7 partner websites[9]
- 14 news items published

[8] https://www.sec-cert.eu/

[9] https://sixsq.com/r-and-d/eusec; https://cloudsecurityalliance.org/project/eu-sec/; https://www.nixu.com/services/compliance-and-certification; http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/eu_sec/

https://www.fabasoft.com/en/about-us/sustainability/active-memberships

https://www.fokus.fraunhofer.de/en/sqc/projects/eu-sec

https://www.pwc.de/de/digitale-transformation/europaeische-initiative-fuer-vertrauen-in-cloud-computing.html

https://cloudsecurityalliance.org/project/eu-sec/

- 15 deliverables available read or download
- 3 flyers available to read or download
- 4 whitepapers available to read or download
- 2 newsletters available to read or download
- Twitter channel[10]
- LinkedIn page[11]
- Content for Workshop on Security Certification
- 1 'Partner Focus' document, describing the partner's role and contribution to the project

2.4 DISSEMINATION TOOLS AND CHANNELS

2.4.1 Offline presence

2.4.1.1 WORKSHOPS

The Workshop on European Security Certification was held in Brussels on September 10th, 2018. The aim of the workshop was to increase awareness of the project's work on the Multiparty Recognition Framework and lay the foundations for exploitation of the scheme at a later date.

The workshop was attended by 31 experts from different backgrounds, including scheme owners, cloud service providers and auditors. The agenda included presentations on the EU Cybersecurity Act by Domenico Ferrara from the European Commission and Adele Naudy Chambaud from DIGITALEUROPE. The Cyber Security Act presentation raised a number of questions from the audience regarding the standards needed to support a cybersecurity certification framework and the role of the different cybersecurity stakeholders, which validated the objectives of the EU-SEC Project.

[10] https://twitter.com/EU_SEC

[11] https://www.linkedin.com/company/eu-sec-eu-security-certification/

Additional discussions about cloud compliance in Europe further supported the goal of a certification assessment framework, although this also highlighted the challenge of having multiple schemes (such as BSI C5, CSA STAR, ISO27001, SOC 2) in scope. Participants welcomed the potential impact of a reduced burden for cloud service providers in terms of process and cost.

Overall, the outcome of the workshop was the clear validation of EU-SEC Project's goal to develop a multiparty recognition between existing cloud security schemes. The audiences fully supported the EU-SEC Project's objective of streamlining compliance efforts and implementing an overall governance. Participants contributed excellent ideas and valuable perspectives for further enhancing the framework which will be taken into account in the development of the scheme.

The presentation material is available for download on the project website[12].

2.4.1.2 EVENT PARTICIPATION

All partners are expected to present and/or attend external workshops, seminars, domain exhibitions and other relevant events in order to bring more awareness to the EU-SEC Project. An event participation list is available for completion on a regular basis and this is supervised by the communication manager. A full list of attended events is shown in the table below.

Table 2: List of attended events

Date	Location	Name of conference/workshop/event	Contributing partner	Form of the contribution	Title
27-29.03.17	Taipei, Taiwan	31st IEEE International Conference on Advanced Information Networking and Applications	Fraunhofer	Paper and presentation x 2	"A process model to support continuous certification of cloud services"

[12] https://cdn0.scrvt.com/fokus/91974c693d94816a/4152229e7123/EU_Sec_Workshop.pdf

					"Towards continuous security certification of Software-as-a-Service applications using web application testing techniques"
14.-17.5.2017	Madrid, Spain	2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing	Fraunhofer	Paper and presentation	Evaluating the performance of continuous test-based cloud service certification
05-08.06.2017	London, UK	Infosecurity Europe	CSA	Booth presence	
4.-5.12.2017		IJU 2017 Informatics in Public administration	SI-MPA	Paper and presentation	The European Security Certification Framework EU-ESC
11.12.2017	Brussels, Belgium	Digital Single Market Stakeholder Meeting	Fraunhofer	Presentation	The European Security Cerification Framework EU-ESC
11.-14.12.2017	Hong Kong	2017 IEEE 9th International Conference on Cloud Computing Technology and Science	Fraunhofer	Paper and presentation	Continuous location validation of cloud service components
01.03.18	Brussels, Belgium	ENISA Workshop Towards the EU Cybersecurity Certification Framework	Fraunhofer	Presentation	EU-SEC presentation

31.01.18	Athens, Greece	H2020 Project Clustering Workshop	CSA	Presentation	EU-SEC presentation
17.04.18	Brussels, Belgium	Security Certification Working Group	Fraunhofer	Presentation	EU-SEC presentation
17-18.04.18	Portorož, Slovenia	DSI 2018 Days of Slovenian Informatics	SI-MPA	Paper and presentation	Development of the new EU-SEC certification framework for cloud computer services
18.04.18	Brussels, Belgium	Stakeholder Workshop on data protection certification mechanisms, seals, and marks	CSA	Participation	
23.05.18	Online	Ihr Nutzen aus Datenschutzzertifizierungen nach DSGVO für Cloud Dienste	Fabasoft	Webinar Branding	EU-SEC
23.05.18	Tokyo, Japan	CSA Japan Security Summit	CSA	Presentation	GDPR, Compliance fatigue and Continuous Assurance
05-08.06.18	London, UK	InfoSecurity Europe	CSA	Presentation & booth presence	GDPR and Mutiparty recognition
20.06.18	Vienna, AT	Fabasoft TechSalon	Fabasoft	Booth presence	EU-SEC
27.06.18	Graz, AT	Trust in ICT	Fraunhofer	Presentation	EU-SEC presentation

04.07.18	Online	Was bringen Datenschutzzertifizierungen?	Fabasoft	Webinar Branding	EU-SEC
17.09.18	Cologne, Germany	T Security Conference of the LKRZV	Fraunhofer	Presentation	The EU-SEC Project in When data becomes action - systematically preventing cyber risks in the IoT
19.09.18	Bratislava, Slovakia	Conference: Risks and their management in cyberspace and enterprise IT infrastructure	MFSR	Presentation	Accreditation Slovak government cloud with using EU-SEC framework
27.11.18	Neckarsulm, Germany	Automotive Innovation Summit	Fraunhofer	Presentation	Providing Trust in Cloud Security - The EU-SEC Project
11.10.1.8	Brno, Czech Republic	DaZ & WIKT 2018	MFSR	Presentation	Semiautomatizované porovnávanie certifikačných schém cloudových služieb
06.11.18	Ljubljana, Slovenia	Annual Conference ISACA.SI	SI-MPA	Presentation	Achieving compliance with the requirements of the various information security frameworks
10.-11.12.2018	Brdo pri Kranju, Slovenia	IJU 2018 Informatics in Public Administration	SI-MPA	Paper and presentation	EU-SEC pilot use case, from ISO 27001 to ISO 27017
31.10.18	Milan, Italy	CSA Summit	CSA	Presentation	Cloud Security Alliance: Where we

					are &where we are going
06.11.18	Ljubljana, Slovenia	Annual Conference ISACA.SI	CSA	Presentation	Continuous audit-based certification
06.12.18	Vienna, Austria	EU Cyber Security and Cloud Computing conference	CSA	Presentation	CSA Code of Conduct for GDPR Compliance
11.12.18	Vienna, Austria	DSM Cloud Stakeholder event	Fabasoft	Organisation & participation	
12.12.18	Lille, France	Truessec Final Symposium	Fraunhofer	Presentation	Providing Trust Through Efficient Cloud Security Certification
13.12.18	Lille, France	Halfway Through the Digital Single Market Strategy	Fraunhofer	Presentation	Increasing the efficiency of cloud certification - Continuous certification

2.4.2 Online presence

In this digital era, the project's online presence is considered critical for engagement with all different stakeholders, from the general public, to industry and academia.

2.4.2.1 WEBSITE

A website is an important communication tool, and serves as the central hub for information about the EU-SEC project. The website fulfils the following functions:

- provide information about the project and the consortium,
- provide updates on project progress through news items and newsletters,

- publish resources and deliverables for the public and for consortium members,
- serve as a portal for other communication methods (email, post mail, social media).

The website was launched in March 2017 and is hosted and maintained by Fraunhofer, with support from all partners. The website can be viewed at https://www.sec-cert.eu/.

In addition to the project website, the work of the consortium is presented on partner websites.

Figure 1: The EU-SEC website

A process has been put into place whereby all partners can funnel website updates via the communications manager for publication to ensure regular changes.

2.4.2.2 SOCIAL MEDIA

Communication on social media can increase visibility, share expertise and build relationships. The EU-SEC project decided to concentrate on Twitter and LinkedIn to share

project information, reports and upcoming events, information about partners' activities, and subject-related news.

Twitter

The Twitter account was launched in August 2017 and had 262 followers at 31 December 2018. There is daily activity and it is used to share project updates and other relevant news. It has been particularly effective in raising awareness of EU-SEC workshops and participation in external events, and has led to communication and information sharing with similar H2020 projects.

LinkedIn

The project has a LinkedIn Group with 28 members and a Company Page with 42 followers.

All partners whose organisation engages in social media activity support the EU-SEC accounts.

2.4.3 Other documentation

A range of documentation is required to provide information in varying levels of detail. Flyers, for example, are intended to give an easily digestible overview whereas white papers go into greater depth for an audience which has prior knowledge of the topics.

2.4.3.1 FLYERS

The following flyers have been published so far:

- introduction to Project[13] ,
- continuous Auditing Pilot[14],

[13] https://cdn0.scrvt.com/fokus/aa1088df93003b7a/736c41bba24d/EU_SEC-Flyer-general-info.pdf

[14] https://cdn0.scrvt.com/fokus/c23b8da26b7c28e7/dd836aa31c7c/EU-SEC_Flyer_CA-PILOT.pdf

- multi-Party Recognition Framework Pilot[15].

They are available for download on the website and for distribution by partners via e-mail or in hardcopy at events.

The flyers are considered a useful format for presenting information in an easily digestible format, providing a lead into the more detailed descriptions given in white papers and deliverables.

2.4.3.2 NEWSLETTERS

Two newsletters have been published so far, giving a roundup of project activities and highlighting milestones. The intention is to provide the newsletters for download via the website and to circulate them by email to registered stakeholders.

2.4.3.3 WHITE PAPERS

Four white papers have been published on the following topics:

- continuous Location Validation of Cloud Service Components,
- a Process Model to support Continuous Certification of Cloud Services,
- towards continuous security certification of Software-as-a-Service applications using web application testing techniques,
- evaluating the performance of continuous test-based cloud service certification.

[15] https://cdn0.scrvt.com/fokus/6facaa36896042b8/bfdf149612d0/EU-SEC_Flyer_MPRF-PILOT.pdf

2.5 KEY PERFORMANCE INDICATORS

The following table shows progress against the KPIs defined at the beginning of the project.

Table 3: Achievements against KPIs

Area of impact	Description	KPI	Status at 31.12.18	Comments
Visibility of the project	Number of website visitors per year	1500	6,849	-
	Number of press releases issued per year	4	3	The project did not capitalise on important events by publishing press releases. At least 10 press releases are planned for 2019. In addition, 4 partners have engaged to publish news items in 2019.
	Number of domain exhibitions per year	>5	3	Activity in this area will increase in 2019, when results are available to present.
	Number of project hosted external workshop (per year)	>1	1	

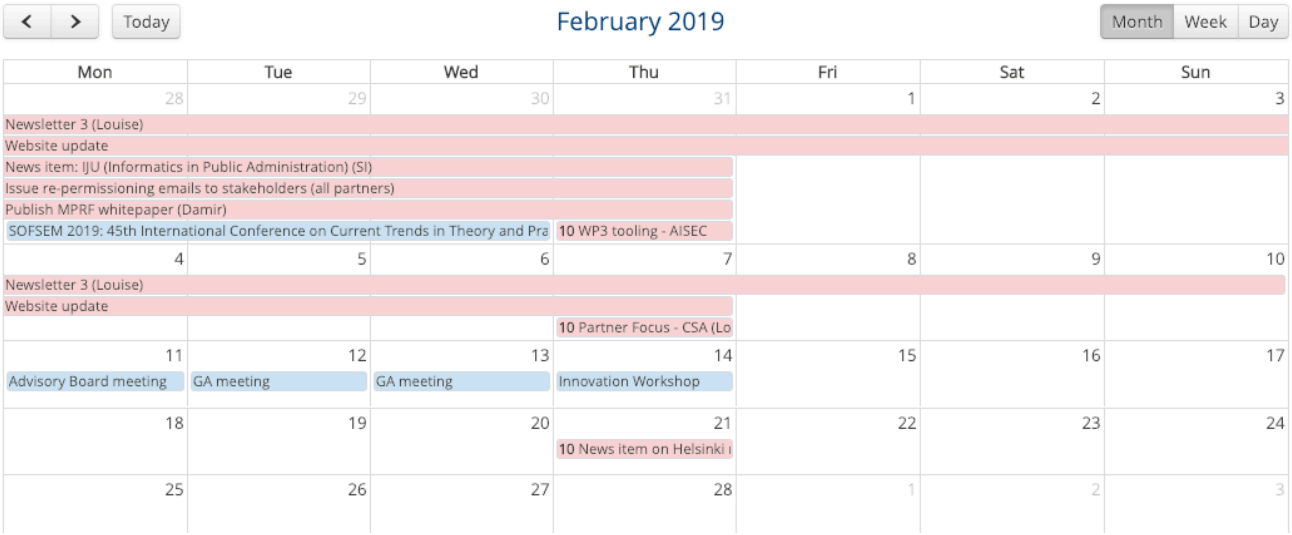
	Number of external workshops/seminars etc participation	>10	13	
Knowledge impact creation	New training seminars (project duration)	>3	1	Most applicable in exploitation stage. Planned for 2019
	Posters, flyers, exhibitions (project duration)	>5	3	Activity in this area will increase in 2019, when results are available to present.
	Number of journal publications (project duration)	>5	1	Planned for 2019
	Number of conference papers & presentations (project duration)	>15	27	
	Number of events attended (project duration)	50	28	
Impact on Europe's technology leadership	Number of market consultation meetings	>6	0	Activity in this area will increase in 2019, when results are available to present.
	Number of trainings with industry/SMEs	>6	0	Activity in this area will increase in 2019,

				when results are available to present.
	Number of trainings with certification authorities	>3	0	Activity in this area will increase in 2019, when results are available to present.

Some KPIs stated in D6.1, for example tracking of location of website visitors, became redundant with change of responsibility for the hosting of the web site since the analytics tools used by Fraunhofer FOKUS to date did not allow a complete analysis of these data. Web site analytics will be improved so that some of the KPIs can be reintroduced when the data is available.

2.6 FUTURE ACTIVITIES

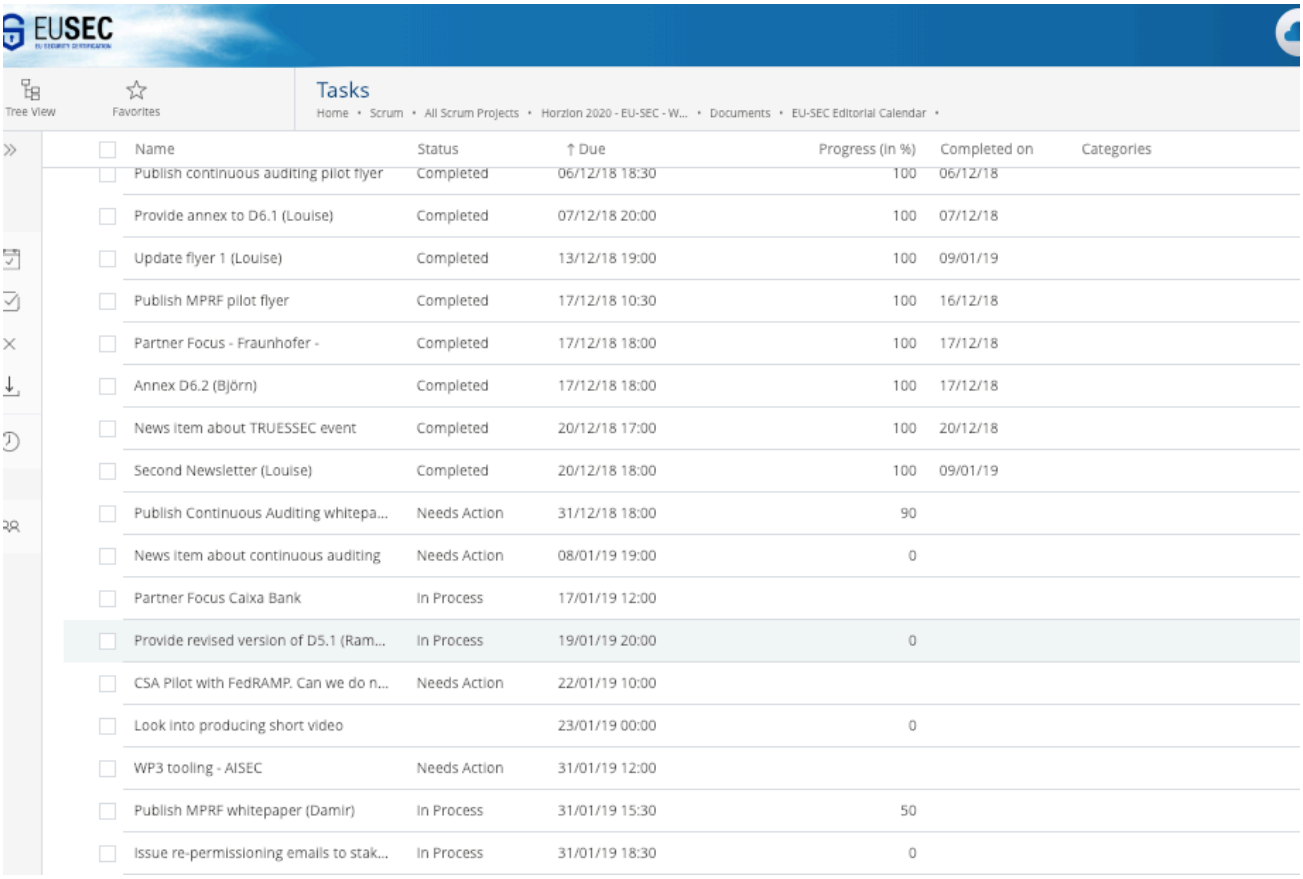
An editorial calendar with an associated task list has been put in place to ensure the continuation of regular, focused dissemination activities. This is updated regularly and is available in Fabasoft cloud to all partners.



Today February 2019 Month Week Day

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1	2	3
Newsletter 3 (Louise)						
Website update						
News item: IJU (Informatics in Public Administration) (SI)						
Issue re-permissioning emails to stakeholders (all partners)						
Publish MPRF whitepaper (Damir)						
SOFSEM 2019: 45th International Conference on Current Trends in Theory and Pra			10 WP3 tooling - AISEC			
4	5	6	7	8	9	10
Newsletter 3 (Louise)						
Website update						
			10 Partner Focus - CSA (Lo			
11	12	13	14	15	16	17
Advisory Board meeting	GA meeting	GA meeting	Innovation Workshop			
18	19	20	21	22	23	24
			10 News item on Helsinki			
25	26	27	28	1	2	3

Figure 2: Sample from editorial calendar



EUSEC

Tree View Favorites

Tasks

Home • Scrum • All Scrum Projects • Horizon 2020 - EU-SEC - W... • Documents • EU-SEC Editorial Calendar •

Name	Status	↑ Due	Progress (in %)	Completed on	Categories
Publish continuous auditing pilot flyer	Completed	06/12/18 18:30	100	06/12/18	
Provide annex to D6.1 (Louise)	Completed	07/12/18 20:00	100	07/12/18	
Update flyer 1 (Louise)	Completed	13/12/18 19:00	100	09/01/19	
Publish MPRF pilot flyer	Completed	17/12/18 10:30	100	16/12/18	
Partner Focus - Fraunhofer -	Completed	17/12/18 18:00	100	17/12/18	
Annex D6.2 (Björn)	Completed	17/12/18 18:00	100	17/12/18	
News item about TRUESSEC event	Completed	20/12/18 17:00	100	20/12/18	
Second Newsletter (Louise)	Completed	20/12/18 18:00	100	09/01/19	
Publish Continuous Auditing whitepa...	Needs Action	31/12/18 18:00	90		
News item about continuous auditing	Needs Action	08/01/19 19:00	0		
Partner Focus Caixa Bank	In Process	17/01/19 12:00			
Provide revised version of D5.1 (Ram...	In Process	19/01/19 20:00	0		
CSA Pilot with FedRAMP. Can we do n...	Needs Action	22/01/19 10:00			
Look into producing short video		23/01/19 00:00	0		
WP3 tooling - AISEC	Needs Action	31/01/19 12:00			
Publish MPRF whitepaper (Damir)	In Process	31/01/19 15:30	50		
Issue re-permissioning emails to stak...	In Process	31/01/19 18:30	0		

Figure 3: Sample from editorial calendar task list

2.6.1 CORPORATE IDENTITY

To ensure consistent and professional communication for the project, work will be done to improve the corporate identity of the EU-SEC project. A logo which visually reinforces the key security aspect of the project was designed at the beginning of the project. This will be supplemented by a template design which be applied to other project documents going forward, such as letterheads, whitepapers, newsletters, presentations, word documents, etc. The working language of the project is English but it is acknowledged that language can vary according to requirements.

2.6.2 WEBSITE

A full review of the website is being carried out. It is recognised that it is not currently easy to identify the aims of the project or its target audiences. There is a lot of useful content which is buried deep in the website, which explains why most visitors leave after viewing the homepage, and this must be addressed. The revised homepage of the website, which will be published by 31 May 2019, will clearly state what the project is doing, who it is for with clearly stated benefits for each target group. This will include the creation of user stories, exploiting the material that has been developed for WPs 4 and 5.

2.6.3 WHITE PAPERS

The white papers are in depth guides intended to educate an audience already familiar with certification work on the project's key areas of work, providing facts and evidence in detail. 2 further white papers will be published in 2019 on the following topics:

- Continuous Auditing Certification
- Multi-Party Recognition Framework

2.6.4 PARTNER FOCUS

The project intends to continue publishing descriptions of each partner, highlighting their role in the project and how they are exploiting the results. The aim is to demonstrate how research activities are benefiting a wide range of organisations and institutions. An article on one partner has already been published and the rest will follow at monthly intervals.

2.6.5 NEWSLETTERS

4 newsletters will be published in 2019 to add to the 2 published in 2018. They will be posted on the website and circulated to stakeholders who have given consent to receive updates.

3 STANDARDISATION ACTIVITIES

We have been building the standardisation activities to support the long-term sustainability for the EU-SEC framework and its components and to encourage the adoption of the project's results in other products and services related to Governance, Risk and Compliance (GRC). As documented in D6.1, the main standardisation objective of the EU-SEC project is to initiate the process for the international standardisation of the multiparty recognition framework as well to define the format to be used for the security requirements, controls and audit/ assessment results expression.

Contributing to standards can help build a competitive advantage and can create the ability to design and validate the EU-SEC framework according to internationally agreed principles. In addition, participating in standardisation processes may bring the project to a higher level of international recognition and highlight new opportunities for collaboration.

3.1 CHALLENGES

The EU-SEC project has already produced substantial results which constitute significant contributions to the standardisation community. Throughout the ongoing standardisation activities, the partners of the EU-SEC project aim at achieving international recognition and creating new opportunities for collaboration and potential exploitation of project outputs with the relevant standardisation bodies. In this context, several challenges need to be tackled in order to achieve the standardisation objectives.

The first challenge to overcome is the gradual and effective establishment of awareness of the project's results within the standardisation community. The effort requires that the innovative concepts of the project, the cloud certification cost-efficiency solutions that it offers, and the expected benefits to the various cloud stakeholders are made known.

Furthermore, EU-SEC's adoption by the standardisation community has to be based on an increased and mutual trust. To this end, EU-SEC has to produce and provide support on educational material and guidelines that will add to transparency and thereafter better understanding of the developed EU-SEC frameworks, mechanisms and produced outcomes (e.g., continuous auditing, multiparty recognition).

Last but not least, the optimisation of the EU-SEC framework and its mechanisms, the pursuit of better quality of results, and overall the increase of its maturity, are considerable factors that will certainly add to more trust. In fact, standardisation activities can play a substantial role, since throughout the collaboration with the standardisation bodies, fruitful feedback can be used to better align the framework with the market's expectations. As a result of that feedback, an increase of the framework's maturity is to be expected, hence bringing more trust and greater chances for its wider adoption.

3.2 TARGET GROUPS

In line with the standardisation strategy (defined in D6.1) the main target group is the standardisation community, more specifically:

- ISO/IEC JTC 1/SC 27,
- ISO/IEC JTC 1/SC 38,
- ITU-T,
- CEN-CENELEC,
- ETSI,
- CSA,
- ENISA,
- EC CSIG - Cert,
- NIST.

Furthermore, the scheme owners/policy makers and governments/agencies are important target groups that develop, use and promote national, regional, sectorial and international requirements on security and privacy.

3.3 ACHIEVEMENTS

We have orchestrated the contributions from the deliverables D1.2, D2.1 and D2.4 to the relevant standardisation initiatives (for details see Table 4).

Table 4: Standardisation activities

Reported Semester	Organisation	Standardisation body	Working group	Form of the contribution	Date	Current status	Results
Q4	CSA	CSA	Privacy Level Agreement WG	Results of the Deliverable D2.3	11/2017	Completed	Contribution to the CSA Code of Conduct for GDPR Compliance
Q5	CSA	ENISA, ETSI, CENELEC	N/A	Panel	13/2/2018	Completed	Input on the discussion on the EU Cyber Security Act
Q5	CSA	BSI - German Federal Security Agency	N/A	Results of the Deliverable D1.2, D2.1, D2.4	03/2018	Ongoing	Initiating the process for acceptance of the MPRF from BSI
Q5	CSA	ICO (Information Commissioner Officer) UK	N/A	Results of the Deliverable D2.3	01/2018	Ongoing	Initiation process for the approval of the GDPR CoC

Q6	CSA	WP29 - European Data Protection Board (EDPB) - Through ICO	N/A	Results of the Deliverable D2.3	02/2018	Ongoing	Initiation process for the approval of the GDPR CoC
Q7	CSA	CNIL - French Data Protection Authority	N/A	Results of the Deliverable D2.3	07/2018	Ongoing	Initiation process for the approval of the GDPR CoC
Q8	CSA / Fraunhofer FOKUS	EC DSM WG on Certification	DSM WG on Cloud Certification	Results of the Deliverable D1.2, D2.1, D2.4	From 03/2018	Ongoing	Contribution to the EC Cloud Certification WG
Q8	CSA	CSA	Open Certification Framework WG	Results of the Deliverable D1.4, D2.2,	11/2018	Completed	Contribution to the CSA STAR Program Level 3, Continuous Self-Assessment
Q8	CSA	CSA	Open Certification Framework WG	Results of the Deliverable D1.4, D2.2,	11/2018	Ongoing	Contribution to the CSA STAR Program Level 3, Enhanced Third Party Certification

Q8	CSA	CSA	Open Certification Framework WG	Results of the Deliverable D1.4, D2.2,	11/2018	Ongoing	Contribution to the CSA STAR Program Level 3, Continuous Auditing Certification

3.4 KEY PERFORMANCE INDICATORS

The following table shows progress against the KPIs for standardisation activities defined at the beginning of the project:

Table 5: Achievements against KPIs

Area of impact	Description	KPI	Status at 31.12.18	Comments
Policy impact	Number of contributions to standards/best-practices	>5	1	The pilots for both innovations will finish in 2019, hence the number of contributions will increase after the results are available.
	Number of contributions to roadmaps, discussion papers (per year)	>2	2	The pilots for both innovations will finish in 2019, hence the number of contributions will increase after the results are available.
	Number of contributions to policy-makers	>5	4	The project has actively contributed to policy-makers and will continue with the efforts in 2019.

3.5 FUTURE ACTIVITIES

As defined in the standardisation strategy (D6.1), we will continue to monitor the standardisation landscape in order to identify:

1. new incubators/initiatives related to EU-SEC, and
2. standards that might not have been originally considered by WP1.

By following the developments in the standardisation landscape, we will align our WP6 activities with the changes in relevant regulations and standards. That will be done mainly as a desktop research and by surveying the relevant communities. The scope of the survey will be based on the four different categories of requirements elicited in WP1:

1. Information security and privacy,
2. Auditing,
3. Mutual / Multi-recognition,
4. Continuous monitoring-based certification.

In those areas we will aim to understand:

1. which standards are being leveraged within organisation,
2. the difference between the standards leveraged within EU-SEC and then those adopted by the organisations surveyed,
3. the potential gaps in the standards related to categories mentioned above,
4. and the potential barriers to the adoption of a certain standard

Our analysis and findings will be disseminated back to the standardisation community and involved stakeholders.

4 EXPLOITATION ACTIVITIES

Where deliverable D6.2 put forward the exploitation plan and strategy, this chapter of deliverable D6.3 provides a summary of the progress made concerning EU-SECs exploitable results and the potential routes for their continued exploitation. During the course of the past two years, the project partners have collaborated in order to define their individual exploitation

ideas and to track activities. In this chapter we list these exploitation activities and perspectives and elaborate on challenges and target groups for the exploitation of EU-SEC results.

4.1 CHALLENGES

When looking at exploitation, this project faces some challenges in its two main innovation areas, multiparty recognition and continuous auditing (see also chapter 2 of D6.2 Exploitation Plan):

- The approach and goal of the Controls Repository has to be rolled out and accepted on EU level, private sector and governing sector.
- One single body will not get all the needed accreditations for all the contents of this matrix – one single certification might not always be feasible.
- Audits applied by more than one body for several certificates might again raise the overhead.
- An (automated) Continuous Auditing tool must be certified / accredited on its own. That is what would distinguish it from existing standard monitoring tools.
- Given the complexity, the intended audience probably needs to be made aware of their needs. Continuous Auditing distinguishes from simple monitoring, but this is not common knowledge.

There is no clear proof that Continuous Auditing saves cost or time over a point in time audit conducted by traditional means. Other benefits have to be made clear to target audiences.

These challenges are being addressed in the value proposition workshops described in section 4.1.2. Although these difficulties make it harder to directly exploit the results and derive *shippable* products from them, the consortium, within the remit of WP 6, has agreed on two paths to address and mitigate them, while keeping a mid- to long-term exploitation strategy in mind. These steps, further explained below, are:

- fast exploitation
- value proposition workshops.

4.1.1 FAST EXPLOITATION AS "QUICK WINS"

We identified so called *fast exploitations*. A fast exploitation is an ad hoc opportunity to convert project results directly into market value. In the development and verification phases of the Multiparty Recognition phase, for instance, the project produced different mappings of certification schemes. These works resulted in additional gap analysis and reverse mapping between the Cloud Control Matrix and the BSI C5. The publication of the C5 Addendum to the CSA Cloud Control Matrix, which is currently under public peer review, is the corresponding fast exploitation: a result, which could directly be used to improve an existing service.

4.1.2 VALUE PROPOSITION WORKSHOPS

In Q4 2018 the project partners launched a series of value proposition workshops under coordination and moderation of innovation experts from Fraunhofer FOKUS. In a first step, the market pains & gains as well as proposed benefits of the Multiparty Recognition Framework and the Continuous Audit Approach were collected. A second iteration of these workshops is planned for the first quarter of 2019.

The goal of these workshops and activities is to analyse and identify opportunities for our developed solutions and to further refine the exploitation roadmap, presented in D6.2.

4.2 TARGET GROUPS

- Auditor
- Cloud User
- Cloud Integrator & operator
- Cloud Security Consultant
- Scheme Owners
- Governments
- Standardisation Institutions

4.3 DEFINING THE BUSINESS MODELS.

One major aspect of exploitation is bringing the Innovations of EU-SEC to the market. The innovations are namely the Multi-Party Recognition Framework and the continuous auditing-based certification. Both have been developed to match concrete existing market needs, which makes bringing them to those demanding markets natural. As part of the exploitation activities the specific market value has to be determined to enable the creation of a business model. The applied methods are Value Proposition Canvas and Business Model Canvas. Both are described in D7.2 Innovation Management Chapter 5.

As part of the exploitation activities in 2018, Value Proposition Workshops were held. Due to the circumstances, the workshops were held via phone and screen sharing, which introduced the necessity of splitting the participating groups into customer and developer. In the case of the multiparty recognition framework workshop the customers were divided even further into auditors and auditee.

Table 6: Topics, Dates and Participants of the Value Proposition Workshops.

WHAT	WHEN	WHO
Continuous Auditing Customer	November 8th 2018	Caixa Bank
Continuous Auditing Developer	November 8th 2018	CSA, Fraunhofer
Multi-Party Recognition Framework Customer Auditee	December 7th 2018	SixSq, Fabasoft, SI-MPA
Multi-Party Recognition Framework Customer Auditor	December 11th 2018	PwC, Nixu
Multi-Party Recognition Framework Developer	January 2018	CSA, Nixu

Each individual workshop contributed to a defined value proposition for the potential customer addressing the needs and a service definition by the developer. The results are the following:

- Continuous Auditing
    - Customer Jobs:
        - Moving to cloud makes regular audits obligatory (depending on control range from seconds to years).
        - Maintain the control while system is out of own control.
        - Maintain compliance of legal requirements.
        - Define level of control: cloud is providing services to different kinds of customers with different requirements.
        - Define the scope of the audit: decide which services, parts of infrastructure, applicability.
        - Define referring scope of controls.
        - Integrate the results / state of a services of the cloud into the service of the company continuously.
    - Customer Pains:
        - Different infrastructures which customers don't own → ask / pay for permission.
        - Responsibility stays.
        - Point in time audit doesn't offer enough control.
        - Costs of point in time audit are high.
        - Human errors can cause damage.
        - Different criteria for different controls are obligatory but not existing (manual adjustment).
        - Dependency on external service provider (no assurance that it is correct).
        - More controls than before when moving to the cloud → more controls make validation harder.
        - Scope of point in time certification is limited.
    - Customer Gains:

        - Rely on automated processes rather than manual.
        - Reduced time between audits (once every 2 years).
        - Warranties going to the cloud = Maintain control.
        - Validation of trust, which is not static in time.
    - Developer Pain Relievers:
        - Continuous auditing gives control to the customer process & is less prone to errors (in the case where there are agreed standards regarding the controls, errors could even be eliminated completely).
        - Individual standards can be implemented.
        - Reduction of long term costs in case of high level of automation.
        - Reduction of human errors as the auditor is assisted by the system.
        - Follow up: Trust for customer by implementing a certification for cloud providers (the base for this cloud provider certification will be Continuous Auditing Certification).
        - Tools (such as APIs of external providers) can be trusted as they are verified by auditor.
        - Support in monitoring and managing increase in controls by tools and automated processes.
        - No limitation in scope of (automated) continuous auditing.
    - Developer Products and Services:
        - Continuous auditing certification: Combination of automated auditing tools (Clouditor) and real-time validation tools for standards and rules of certification.
        - API and data-driven (instead of process driven).
- Multiparty Recognition Framework:
    - Customer Jobs:
        - Structured overview of different controls / technical implementation and possible mapping, comparability.
        - Create an output defining the control environment / security architecture.

- Get certified for multiple certification and multiple schemes with one audit.
- Streamlining compliance efforts.
- Auditee: Reduce "unnecessary"/ redundant efforts (unnecessary = too many requirements overlap).
- Define and execute the controls in a multi-compliant way (detailed description) and map them to the requirements.
- Analyse which compliance requirements might be important for the customers of the providers.
- Provide feedback to the database on new / updated requirements / compliance schemes.
- Derive complementary safeguards the customers of the provider / end-user can implement.
- Auditor Job: Derive the criteria needed for the audit ("audit paper" production / audit program).

- Customer Jobs:
  - Many requirements overlap / are the same
    - Non-transparency of meeting compliance schemes Y when a provider is compliant with compliant scheme X.
    - Same control gets audited multiple times .
  - No internal system that accepted outside the company .
  - No EU-framework that you can rely on (code of conduct).
  - No possibility to make the framework generic / very specific for each use case.
  - Roles of auditor and auditee are unclear → who is responsible for what?
  - No mapping database for the compliance scheme requirements / security requirements.
- Customer Gains:
  - Reduce costs of certification.

- Implementation in micro area (for ministerial issues: learnings from the framework and derive next steps e.g. evidence storage).
- Make communication between authority and auditor easier.
- User instruction / manual / training for the users.
- Compliance (maintenance) clock → schedule of tasks.
- Possibility to communicate / estimate time / cost reduction by using the framework (RoI demonstration to stakeholder).

4.4 ACHIEVEMENTS

Table 7 shows the achievements with respect to exploitation.

Table 7: Fast Exploitations

Reported Semester	Organization	Projects results being exploited	Short description of:			Current status
			how	where	when	
			these results have been or are being exploited			
Q7	Fabasoft	Results on how to design a Continuous Audit API in WP3 and WP 5; set-up of FISH application in WP5 (pilot 2)	Fabasoft Continuous Audit API (CA API) prototype	Fabasoft Cloud App Project Repository	Q4 2018	prototype available, non-public
Q8	Fraunhofer FOKUS / Fabasoft	Results on how to design a Continuous Audit API in WP3 and WP 5; set-up of FISH application in WP 5 (pilot 2)	Continuous Audit API (CA API) definition and documentation	White Paper	Q4 2018	available in Fabasoft Cloud EU-SEC
Q9	SI-MPA	T4.1 Pilot audit report	Updating the ISO 27001 ISMS documentation	SI-MPA ISMS	Q1 2019	planning

			with ISO 27017 requirements, Extended SoA controls			
Q6	CSA	Privacy Code of Conduct	Launch of the CSA Code of Conduct for GDPR Compliance - Self Assessment	NA	At InfoSecurity London 2018	Available to the general public
Q7	CSA	Privacy Code of Conduct	Launch of the CSA GDPR Center of Excellence	Berlin	At the Bitkon Privacy Conference	Available to the general public
Q8	CSA	Gap analysis and reverse mapping between CCM and C5	Publication of the C5 Addendum to the CSA Cloud Control Matrix	NA	Peer review in December 2018 and final publication expected in	Under public peer review

					January 2019	
Q9	CSA	Continuous Auditing Certification scheme	Launch of the CSA STAR Continuous Self Assessment	NA	In January 2019	Scheme and other supporting material ready, CSA web site ready. Working on the marketing material to support the launch
Q9	CSA	Multiparty Recognition Framework	Extension of the approach to the USA program FedRAMP	Washington D.C.	Ongoing	Preparatory activities for the pilots with Google, AWS, SAP and Work day. Pilot results to be available in Q2 2019
Q10	CSA	Privacy Code of Conduct	Launch of the CSA Code of Conduct for GDPR Compliance - Certification	NA	Ongoing	Final draft of the certification scheme to be submitted to the European Data Protection Board

4.5 FUTURE ACTIVITIES

Table 8: Exploitation Perspectives

Quarter	Year	Organization	Project results being exploited	Short description of: how these results are going to be exploited	Short description of: where these results are going to be exploited	Short description of: when these results are going to be exploited	Current status
Q2	2019	Fabasoft	Results on how to design a Continuous Audit API in WP3 and WP 5 Set-up of FISH application in WP 5 (pilot 2) Results and findings from FISH application tests in pilot 2 Results from Clouditor application in pilot 2	Developing the non-public prototype of the Fabasoft CA API into an initial release Offering documentation to the release	Fabasoft Cloud	During the final phase of pilot 2	planning

Q4	2019	CSA	Continuous Monitoring certification scheme, Multiparty recognition scheme and Privacy Code of Conduct	CSA will create a new version of the STAR Registry, which will become the public registry for cloud security and privacy assurance and compliance, via the integration of the current CSA activities, the results of the EU-SEC project and its extension to cover extra European Countries (e.g. USA, Japan, Singapore, Malaysia) as well as the regulated business sector such as Finance and Healthcare.	N/A	Between Q3 2019 and Q4 2020	Several components under development (see fast exploitation tab)
Q2	2019	Fraunhofer AISEC	Results of pilot 2 (WP5) and CA API	Clouditor: adapt and further develop the tool Clouditor shall serve as a product for different target groups: auditors		After finishing pilot 2	planning

				cloud users 3rd party cloud integrators cloud security consultants			
Q4	2019	CSA	Continuous Monitoring certification scheme	Launch of a full fledge program Continuous Auditing certification program, i.e. the CSA STAR Continuous Auditing, which will include Continuous Self-Assessment, 3rd party audit + Continuous Self-Assessment, and a Continuous Auditing Certification.	NA	Between Q4 2019 and Q2 2020	Continuous Self-Assessment ready. The CSA Open Certification Working Group is leveraging the results of the EU-SEC to build the Continuous Auditing Certification
Q6	2019	Fraunhofer FOKUS	Results of pilot 2 (WP5) and CA API	Evolve existing Fraunhofer FOKUS Security Risk Assessment tools (i.e.	Fraunhofer Services	After finishing pilot 2	planning

				Fraunhofer RACOMAT) to integrate the CA API.			
Q6	2019	Fraunhofer FOKUS and CaixaBank	FISH implementation for public cloud	Evolve existing and develop new demonstration setups base on the FISH implementation. Also improve on the implementation with the goal of making it a standalone product.	Fraunhofer Services	After finishing pilot 2	planning
Q10	2019	SixSq	Preparation for ISO 27001 certification	Security consolidation and improving user trust	SixSq	Q2 2019	ongoing
Q13	2020	SI-MPA	MPRF	Building MPRF requirements and controls repository of Slovenian Government Cloud CSU demands	SI-MPA ISMS	After finishing EU-SEC project	planning
Q6	2019	CaixaBank	Results of Pilot 2: Continuous Audit Certification (WP5)	Develop and evolve Continuous Auditing Certification architecture in order to be further used or	N/A	After finishing pilot 2	planning

				integrated in CaixaBank for the management and control of cloud services.			
Q10	2019	PwC	EU-SEC Requirements Repository	Application of the EU-SEC Requirements Repository for analysing the potential reduction of audit effort	future projects	mid 2019	pending
Q10	2019	Nixu	EU-SEC Requirements Repository	Application of the EU-SEC Requirements Repository and the multi-party recognition for analysing the potential reduction of audit effort	future projects	mid 2019	pending

5 CONCLUSION

The project's communication activities in the first two years included face to face, offline and online activities with internal and external stakeholders. The efforts in terms of standardisation were more successful than those for dissemination and exploitation. As initially planned, exploitation activities will intensify in the final year of the project to ensure that the value proposition and business benefits are understood, and the innovations commercially exploited.

During the second part of this reporting period, the project consortium recognised that the dissemination activities were not achieving the goal of raising awareness of the EU-SEC project results with potential users. Dissemination was not built into every activity and not always timely. Changes were therefore put into place to improve results in this area. The project consortium members are confident that these changes will bear fruit in the final year of the project.