EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D 6.2 EXPLOITATION PLAN

VERSION 1.1

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: APRIL 2018	DELIVERY DATE: DECEMBER 19. 2018
AUTHOR: Fabasoft	PARTNERS CONTRIBUTED: all partners
DISSEMINATION LEVEL: * PU	NATURE OF THE DELIVERABLE: ** R
INTERNAL REVIEWERS: SixSq, PwC	

*PU = Public, CO = Confidential

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

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

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	30.04.2018	Submitted deliverable	Björn Fanta, Fabasoft
1.1	16.12.2018	Revised deliverable; added Annex regarding the comments of the mid-term review	Björn Fanta, Fabasoft

EXECUTIVE SUMMARY

The Plan for the Exploitation of Results (PER) presented here is one of the compulsory reports that H2020 projects are required to submit to the EC. The PER summarizes the consortium's strategy and concrete actions to disseminate, exploit and protect the foreground generated by a project and should serve as a guideline to the consortium for the exploitation activities to be carried out in the context of the EU-SEC project.

This report is the first PER release and provides a summary of the progress done concerning EU-SECs exploitable results and the potential routes for their exploitation that project partners have envisioned at the beginning of the project and which are being redefined as the project technically has progressed. In the development of the corresponding tasks, the project partners have collaborated in order to define their individual exploitation plans and to develop the market analysis. In further steps, the reports will be complemented with the partners' support in order to evaluate the position in the market of the EU-SEC main results, to identify the risks of the project and to define the mitigation plan.

Besides this executive summary, the deliverable is structured in five chapters: Chapter 2, containing information about the scope and objectives, the strategy. Chapter 3, illustrating the preliminary exploitable foreground and products. Chapter 4, which contains information on who to contact with regard to the exploitation activities and Chapter 5, which is the references section containing some useful web links.

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

AB	Advisory Board
AP	Action Point
CEN	European Committee for Standardization
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
e.g.	for example
EC C-SIG	European Commission Cloud-Select Industry Group
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
IPR	Intellectual Property Rules
ISC	International Standardization Council
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
KPI	Key Performance Indicator
MF-SR	Ministerstvo financii Slovenskej republiky
MRL	Market Readiness Level
n.a.	not applicable
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NIXU	Nixu Oyj
PwC	Pricewaterhouse Coopers 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
TRA	Technological Readiness Assessment
TRL	Technology Readiness Level
WP	Work Package

TABLE OF CONTENTS

1 PROJECT OVERVIEW 9

2 EXPLOITATION STRATEGY 10

2.1 EXPLOITATION OF MULTIPARTY RECOGNITION FRAMEWORK 10
2.2 EXPLOITATION OF CONTINUOUS AUDITING 13

3 PRODUCTS 16

3.1 LIST OF EXPLOITABLE PRODUCT CONCEPTS 16
3.2 POTENTIAL IMPACT 18

4 EXPLOITATION MANAGEMENT 20

4.1 EXPLOITATION TEAM & CONTACT 21

5 REFERENCES AND USEFUL LINKS 22

APPENDIX A 23

APPENDIX B - EXPLOITATION ACTIVITY TRACKING 27

LIST OF TABLES

TABLE 1: EXPLOITATION TEAM & CONTACT 21
TABLE 2: FAST EXPLOITATIONS 29
TABLE 3: EXPLOITATION PERSPECTIVES 31

LIST OF FIGURES

FIGURE 1: GRAPHICAL ILLUSTRATION OF EXAMPLE EXPLOITATION OF RESULTS FOR AUDITING BODIES 11
FIGURE 2: EXPLOITATION ROADMAP 28

1 PROJECT OVERVIEW

In recent years, the ICT market has evolved towards a cloud-based approach. This shift, together with the rapidly changing legal and regulatory landscape, has heavily affected security assurance, governance and compliance. Players in the IT security market have tried to provide suitable solutions to cope with issues such as:

- lack of means to provide higher level of assurance (e.g. continuous monitoring and auditing),
- not taking privacy adequately into account,
- limited transparency,
- and lack of means to streamline risk management and compliance.

In the certification space, this has resulted in the creation of several schemes creating an additional problem, i.e. the proliferation of certification schemes.

With the support from Horizon 2020 (H2020), a funding programme created by the European Union to support and foster research in the European Research Area, the European Security Certification Framework (EU-SEC) Consortium aims to solve the aforementioned issues by:

- improving the effectiveness and efficiency of existing approaches for assurance and compliance,
- creating a framework under which existing certification and assurance approaches can co-exist,
- providing stakeholders in the ICT security ecosystem with a validated governance structure, a reference architecture, and the corresponding set of tools,
- and enhancing trustworthiness and transparency in the ICT supply chain through business cases developed and piloted by industrial partners.

2 EXPLOITATION STRATEGY

This chapter describes the exploitation of the project results from the perspective of the project partners. This allows us to give an overview of the exploitation possibilities of accredited auditing bodies, research institutes, ministries, financial institutes and cloud service providers.

All perspectives offer exploitation approaches of the corresponding project partners, leading to a better understanding of how to use the project results and future product thoughts. We give an overview on enhancements of existing service portfolios (e.g., audit and consulting services) as well as activities to provide new services based on the innovations, developed in this project (e.g., Continuous Auditing).

As mentioned, the EU-SEC Framework offers two approaches, the Multiparty Recognition Framework and Continuous Auditing. Therefore, two possible exploitable result paths derive from the project. Below, we describe the vision and afterwards the exploitation approach, obstacles and problem solving for both derivatives. Obstacles and problem-solving steps line up with the exploitation approach and are listed in small letters, to indicate, which step of the problem solving corresponds to which obstacle.

2.1 EXPLOITATION OF MULTIPARTY RECOGNITION FRAMEWORK

To talk about the result exploitation of the Multiparty Recognition Framework, it is best to start exemplary with the intention of one of the project partners, PwC. By participating in the development of continuous auditing schemes and the Multiparty Recognition Framework, PwC is able to improve current audit processes, integrate existing cloud standards on an international level and support clients during the corresponding transition process.

As of now, audits are time-consuming projects that tie up key resources on the auditor and auditee's side. Related evidence gathering and inspection activities are complex and cumbersome, which results in expensive and long audits. As for these needs, PwC and their clients are facing the conflict to implement one unified framework to reduce audit complexity.

Therefore, PwC and their clients are interested in reducing the total effort of a traditional audit in terms of shortening the audit period and decreasing its complexity. In this case, defined tools such as the Multiparty Recognition Framework support the comprehension and strategic development of auditing measures.

The establishment of a Multiparty Recognition Framework is where we as the consortium see potential to solve this dilemma. Currently, many different standards and frameworks coexist that are addressing different elements of cloud service providers (see Project Overview). However, many of these (mainly national) standards overlap at certain points so that it would be beneficial to identify those common grounds and merge them to one comprehensive framework. Since the Multiparty Recognition Framework addresses these topics, the application of the framework in the audit business is guaranteed. Such an international framework leads to a comprehensive overview of available standards and offers the possibility of their integration. Thereby, auditors can help their clients to cover various requirements of standards simultaneously, combine the audit activities and comply with them on a broader basis.

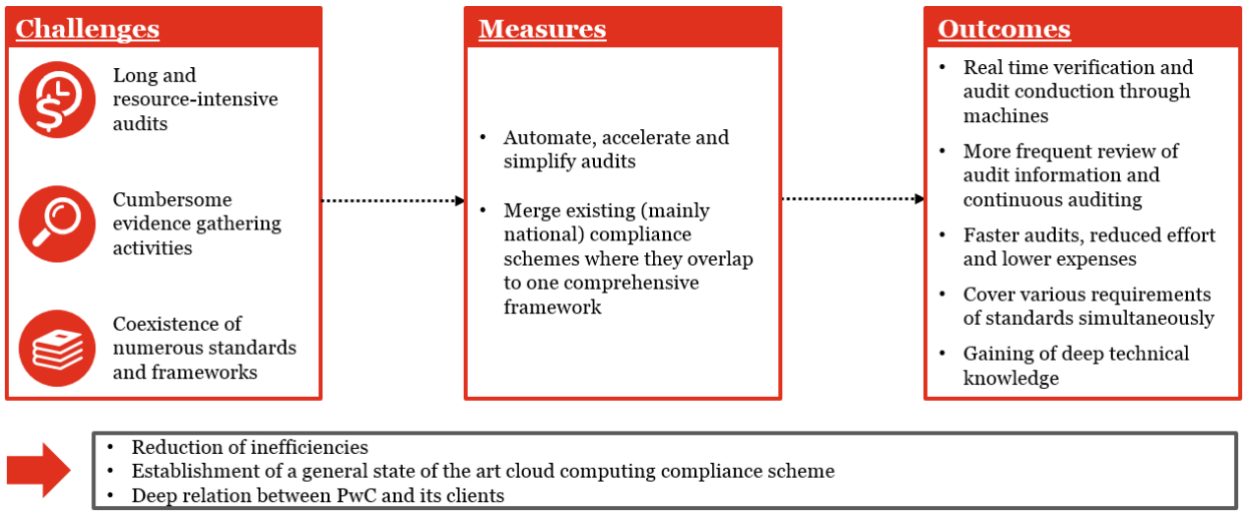

Figure 1: Graphical illustration of example exploitation of results for auditing bodies

As a further example, from the CSA perspective, the project results will be exploited to support the CSA research agenda as well as the CSA standardization strategy. The CSA is planning to take advantage of the results of the EU-SEC project in several ways.

The current state of the Cloud Control Matrix (CCM), which was used to achieve the current version of the Controls and Requirements Repository within the project, will be improved thanks to the results of the EU-SEC, and in particular because of the work done in the context of the Controls and Requirements Repository.

The STAR Registry will receive a considerable boost from the EU-SEC project since the project will give additional visibility and branding support to the registry. The amount of organization on the registry is likely to increase, so to generate a better market transparency as well as increase revenues for CSA. The STAR Program Level 2 foresees the need to have accredited and qualified

auditors. With the extension of the program to new requirements and need, it is estimated that there will be an increase demand for training services. That will create benefits for both the CSA's training and certification partners as well as indirectly for CSA that will have increase revenues from royalties. The CSA OCF / STAR Framework was created to be a global house for different compliance and assurance needs. The results of the EU-SEC will be used to support that vision. Moreover, the harmonization work done within the European market will be extended on a global scale in order to create compatibility between the certification approaches of EU Members States and other countries outside Europe, e.g. Japan, Singapore, USA, Canada, Brazil, etc.

The Ministry of Public Administration of the Republic of Slovenia is a horizontal ministry and plans to implement the tools developed in EU–SEC project to improve information security compliance of Slovenian Cloud Ecosystems. The economic-political improvements that the EU-SEC Framework provides in that regard are:

- compliance with requirements of a fair coverage of standards,
- acceleration of the process of constant improvement of information security,
- promoting the involvement and participation of stakeholders from the public, private and social spheres in shaping public policies and developing public administration services,
- strengthening international cooperation between countries and across borders,
- increasing transparency, openness and inclusion in public cloud computing services.

2.1.1 EXPLOITATION APPROACH

One certification facilitates the audit of many. There is one existing matrix to map all or at least a specific number of requirements to a wide range of controls. With this matrix, it is possible for auditing bodies to audit cloud service providers more efficiently with regard to time and money (see Exploitation). This matrix (more precisely the Controls Repository) is developed by the EU-SEC project within the Multiparty Recognition Framework.

2.1.2 OBSTACLES

a. The approach and goal of the Controls Repository has to be rolled out and accepted on EU level, private sector and governing sector.
b. 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.
c. Audits applied by more than one body for several certificates might again rise the overhead.

2.1.3 PROBLEM SOLVING – DEALING WITH OBSTACLES

a. The project will provide the framework to work with, including the methodology to set the right scope and to integrate (as well as update) certificates into the framework. The next step is providing best practices by the project partners, which will be done in the pilots within the project (see Working Package 4). Additionally, the project dissemination plays a role here. By presenting the project and its results to a broad audience and by giving educational workshops, we raise knowledge and acceptance of the framework.
b. There will be certification bodies with certain accreditations and certain gaps. In the case that a CSP wants to receive more than one certification and an auditor is only able to provide a fraction of the desired amount, the framework can only yield a gain in efficiency, if another auditor, audits the "missing" certificates; and accepts the results of the first auditor. Reality will show if this might be the case.
c. This argument is strongly connected to argument b). If the framework is strong enough in its maturity and widely acknowledged, another auditing body might accept the results of the first auditor and thus a gain of efficiency is still viable.

2.2 EXPLOITATION OF CONTINUOUS AUDITING

Further understanding of the matter is based on the definition of two categories of customers. These are defined by the activity and intention, namely direct and indirect customer. Cloud service providers are, by its very business model, the ones in need to certify their services to provide a trustworthy environment for their own customers. Thus, cloud service providers are called direct customers for the understanding of EU-SEC exploitable results. In line with this definition, customers of cloud service providers that outsource some (or all) of their digital activities to them and need proven trust are called indirect customers with respect to the EU-SEC Framework exploitable results.

At this point, Continuous Auditing comes into play. It is a solution to automate, accelerate and simplify audits done by direct customer of auditing bodies as a trust benefit for indirect customers. It enables real time verification and the audit as such is mainly conducted not by humans but continuously through appropriate machines. Human resources are applied to monitor the machines and establish the underlying processes but they are relieved from recurring audit procedures. Although the result of continuous auditing will be the same as the conventional audit, audit related information could be reviewed and generated more frequently in continuous auditing. After Continuous Auditing is implemented, direct and indirect customers profit from faster audits and reduced effort. In addition, detailed technical knowledge is gained in automation

of classical audits and related realization and implementation scenarios that auditing bodies, like PwC and Nixu in the project, will apply to support their client's transition

In Addition, partners in the consortium have great innovation potential. However, realizing this potential, in the forms of products or services, is a real challenge, especially in the public sector or in regulated private sectors such as health and finance. In the case of SixSq, which develops global solutions that can apply to a pan-European footprint, and beyond, the challenge is even more acute. Fragmentation in regulations and the way to reach the right level of certification (including how to substantiate these with respect to the different sectorial and national scheme) is a real headache and an inhibitor to success. SixSq is not alone, as we assume most if not all SMEs face similar significant hurdle. With Continuous Auditing, EU-SEC will provide SixSq the solution to the certification of its novel multi-cloud brokerage service. This has the potential to open opportunities for them, which up to now were unattainable. The entry barriers just were too high, both in terms of upfront investment in multiple auditing processes to cover, time to perform these lengthy individual audits and especially the risk of following the wrong audit, for a targeted sector or country. By addressing new markets with its established service record, SixSq expects to be able to show significant growth within the project lifetime, thanks to the proposed schedule, where the third year of the project will enable SixSq to take full advantage of the certification it will have helped to define and attain during the second year.

2.2.1 EXPLOITATION APPROACH

In a financial institution like CaixaBank, the management of sensitive information is extremely important and subject to very strict regulations. For this reason, any technology providing a higher degree of regulatory compliance on information management is key for the core for such businesses. In this sense, the idea of Continuous Auditing perfectly aligns with this necessity. This means the technical contributions of EU-SEC for Continuous Auditing of cloud service providers Saas, Paas, or Iaas have important exploitation opportunities for businesses in the financial sector.

Another possible added value for a bank who is buying SaaS and offering IaaS PaaS to the internal IT department, is that it can help to solve internal audit findings on IaaS, PaaS, because it provides additional assurance. It can make life of the second line easier in their reporting to the regulator, because it offers more detailed compliance information. Additionally, it can reduce the workload on the first line when procuring SaaS applications. When the SaaS vendor or a cloud service provider adopts EU-SEC. This is a multiparty recognition aspect within the Continuous Auditing.

From the point of view of a cloud service provider, an accredited tool which can be installed and not only monitors predefined, formalized controls, but also maps them to the right controls and requirements due to a working framework would yield a lot of advantages. The tool provides a

continuous stream of report outputs that can be (re)viewed internally and checked for status of the controls (e.g., like a traffic light: red, yellow and green). Based on this continuous report, the auditing body can issue a public certificate, which is valid, as long as the required controls are green (or yellow). A cloud service provider can then publish an aggregated report on their website for instance to show the current certificates and "live-status", if desired.

2.2.2 OBSTACLES

a. An (automated) Continuous Auditing tool must be certified / accredited on its own. That is what would distinguish it from existing standard monitoring tools.
b. Given the complexity, the intended audience probably needs to be made aware of their needs. Continuous Auditing distinguishes from simple monitoring, but this is no common knowledge.
c. There is no proof that Continuous Auditing saves cost or time over a point in time audit conducted by traditional means.

2.2.3 PROBLEM SOLVING – DEALING WITH OBSTACLES

a. Whereas the certification/accreditation of a continuous auditing tool, is not in the scope of the EU-SEC project, the consortium can and will offer the technical tool kit, the first research as well as the first steps in a pilot (see Working Package 5) to address the challenges. The important value added produced in this project is the combination of the tool kit with automated monitoring capabilities that will be tied to certain certification requirements and selected internal controls.
b. The complexity is something the consortium is dealing with since the beginning. Therefore, special dissemination chapters exist, pursuing a schooling and information frame for potential customers and stakeholders the like. However, this information is not within the scope of this document and explained in Deliverable 6.1.
c. All consortium members, especially the potential direct customers of such an approach, are convinced that this approach yields benefits. Time and cost savings are only one of many. Pilot 2 in Working Package 5 will demonstrate them to an extent an offer a field test contributing to an exploitable product in the sense of Continuous Auditing. Regarding the vision, a lot of technical question remain currently open and unanswered, only a fraction of them can be tackled in the project. This is well within the scope and defined in the Grant Agreement.

3 PRODUCTS

Both, the Multiparty Recognition Framework and Continuous Auditing, are providing a profound auditing experience to simplify audits and integrate existing or recently developed compliance frameworks. They are valuable initiatives that address current weak points in auditing and compliance. In course of the EU-SEC project, new insights are developed that help to reduce inefficiencies and elaborate on the integration mechanisms of various compliance schemes. As a close exchange between auditors and auditees is necessary to ensure correct and efficient execution, the implementation of Continuous Auditing and the Multiparty Recognition Framework will build a deep relation between accredited auditors and customers (e.g., cloud service providers).

The results of the EU-SEC project are important for many stakeholders and are likely to be applied broadly in various countries. Accordingly, the existing service portfolio accredited auditors will be impacted on different levels, as increased (technically oriented) consulting services are to be developed and offered during the initiation of Continuous Auditing and the Multiparty Recognition Framework.

Therefore, with this in mind, the following list of exploitable products can only provide a glimpse of what is possible.

3.1 LIST OF EXPLOITABLE PRODUCT CONCEPTS

This list is a point-in-time view on current available product concepts. As the pilots in Working Package 4 and 5 will move on, and the innovation strategy kicks in, there will be new product ideas and concepts, based on the project results.

1. Multi-Party Recognition Framework
    - With the Multi-Party-Recognition-Framework, a bunch of updated and enhanced services will be established. Auditors like PwC or Nixu can offer more custom tailored services and provide their customers (cloud service providers) with a huge saving in time and therefore costs for audits and thus for receives desired certificates.
    - CSA plans to improve the Cloud Control Matrix and their own STAR Program
    - Currently, this planning involves development of a CSA a framework of CSA branded consultancy services around the results of the EU-SEC that will be leveraged by some members within the CSA's community (320 corporate

members and over 80,000 individual members) so to improve the current approach to governance-risk management-compliance consultancy services.

- Guidelines for structured interviews will be developed to assess the quality as well as the usability of the Multi-Part-Recognition-Framework. These interviews will be held with the pilot partners. This approach leverages the benefits of the framework by implementing a customer centric product development. At the same time this approach makes it possible to adapt the framework to the intended usability and validate it in a natural setting.

2. Continuous Auditing
   - CSA plans to evolve the STAR Program by adding a Continuous Certification approach and to accelerate the development of the STARWatch tool v2.
   - Clouditor is sought to serve as a product for different target groups. Hereafter, incentives for identified target groups to utilize Clouditor are outlined:
     - **Auditor** The main task of an auditor is to check whether a control is implemented as specified. To that end, the auditor collects relevant information and, on this basis, concludes if a control objective holds. Clouditor reduces time needed by an auditor to conduct an audit noticeably by substituting lengthy information gathering techniques such as interviews or questionnaires with information provided by the Clouditor.
     - **Cloud user** The cloud user (i.e., someone leveraging cloud resources to build a cloud-based application) uses the Clouditor to determine if her cloud-based application is, in fact, sufficiently secure. The reasons for the cloud user to seek security assurance are to retain and acquire new customers through increased transparency and trust, to conform with regulations, to perform risk assessments as well as to reduce liability granted to the customer in case of security breaches. Figuring out whether a cloud-based application meets essential security requirements implies that a cloud user has to acquire security knowledge necessary to assess her cloud-based application and is able to conduct these assessments on a regular basis. Clouditor makes this cost-intensive activities obsolete since it incorporates a vast amount of cloud-specific security knowledge which is used to continuously (i.e., automatically and repeatedly) check the security of a cloud-based application.
     - **Third-party cloud integrator & operator** The cloud operator acts as a middleman between companies who want to outsource operation and maintenance of cloud resources used by the company (so-called operations-as-a-service). In order to minimize costly manual maintenance

activities, such cloud operators draw on means of automation, e.g. following the infrastructure as code approach where based on (more or less) complex configuration files, entire virtual infrastructures are launched. Other security-related tasks such as monitoring network traffic for anomalies are, again, outsourced by the cloud operator, thereby leveraging existing solution is the respective field. The rationale behind this is saving time and cost to build proprietary solutions, and using high-end approach provided by the specialized vendors. In general, those cloud operators act very similar to general cloud users who assign their own internal IT departments to operate cloud resources. Therefore, Clouditor to them is another tool with which they can continuously check whether essential security requirements are met.

        - **Cloud Security Consultant** A cloud security consultant performs security assessments of an existing cloud-based application and gives advice on how to improve the overall architecture and configuration. The security consultant provides his service on an ongoing basis, that is, security tests are also to be performed during operation of the application. Through using Clouditor, the consultant automates most of the security tests and thus significantly decreases the time to perform reoccurring security model reviews and improvements.
    - Fabasoft plans to implement a generic Audit API in its SaaS solution, to provide tools like Clouditor the right and meaningful access in the case of an accredited continuous audit process.

By means of the Technological Readiness Assessment (TRA) methodology, (see D1.1 TRA methodology) the developmental progress of Clouditor is monitored. This methodology sets a framework for assessing the current state of the Technology Readiness Level (TRL) as well as the Market Readiness Level (MRL) of each single component of the EU-SEC framework on the one hand, and helps to define a systematic action plan for refining each component's technical maturity level on the other hand. This is done to achieve the planned TRL 7+ in a step-wise manner. See Appendix A for a description of the current TRL of Clouditor.

3.2 POTENTIAL IMPACT

The potential impact has to be answered on an individual basis, taking into account the different natures of the businesses and activities of the consortium members.

Some partners estimate a significant increase in efficiency for multi-certification activities for their service portfolio, which is currently confirmed within the consortium in the upcoming pilots. For cloud service providers as potential direct clients of certifying bodies, a working EU-SEC Requirements Repository with a Multiparty Recognition Framework leads to cost savings eventually. As the landscape of cloud service providers is blooming in Europe (e.g., cloud services Made in Germany)[1] the need for a framework like EU-SEC seems obvious.

On the same page, it is expected that the exploitation of the EU-SEC results will generate additional revenues from increased sales of currently available products like the STAR Watch tool by improving them with the project results (e.g. a new STAR Certification and STAR Attestation). An improved market visibility will be the case.

Once the EU-SEC Framework achieves the adequate level of maturity in the case of Continuous Auditing, CaixaBank potentially becomes its first client. Even more, as soon as CaixaBank adopts the EU-SEC Framework that enables performing Continuous Auditing of cloud services (especially SaaS), other entities that interact with CaixaBank may be immediately involved as well, including regulators (e.g., BDE, EBA) and auditors. This could attract such organizations to further adopt EU-SEC in their respective environments. To illustrate this, several members of CaixaBank's information security team have been working in the last months on in-house tools to achieve continuous auditing of CaixaBank services running in the cloud. This demonstrates the potential business opportunities of the EU-SEC framework for CaixaBank and other financial institutions. Additionally, this shows the sustainability of the EU-SEC Framework by a group of specialists in CaixaBank headquarters, for instance.

All partners will contribute to the certification effort by providing concrete requirements in order to deliver its innovation, in a secure, streamlined, neutral and efficient manner. Our objective is to strike the right balance between a higher rate of innovation that is typical in regulated domains, with the need to demonstrate convincingly our ability to deliver to our customers the right level of assurance and compliance.

[1] http://www.cloud-services-made-in-germany.de/

4 EXPLOITATION MANAGEMENT

The PER is designed in order to multiply the impact of the proposed solutions and prepare the transition towards industrial and commercial uptake. The PER is focused on explaining the novel approach and solutions developed within the EU–SEC project, as well as benefits gained with respect to other existing approaches and solutions.

We plan to disseminate the results of the EU-SEC project with the stakeholders that were identified during the development of the Slovenian State Cloud and with other interested governmental and public institutions from the SI-MPA's extensive communication database. The EU–SEC project achievement will be presented through established media channels: we will attend the meetings, conferences, seminars, and workshops, to exchange knowledge with other cloud computing enthusiasts and experts and through the official and unofficial governmental networks. We also plan to make a customer satisfaction analysis about a new eGovernment service. We believe that the EU–SEC project will have a positive effect on stakeholders and that it raises trust and confidence in eGovernment services.

Additionally, partners like SixSq, Caixa Bank, Nixu, PwC or Fabasoft intend to share this journey with fellow companies in order to:

1. Demystify regulations, certifications and audit processes
2. Build the right material to present to prospect customers to substantiate claims of complying certification
3. Provide real experience report of service certification, in our domain of operations: cloud computing and brokerage This will be done via a dedicated blog series and marketing one-pagers, such that other technology and service SMEs can benefit from our experience.

4.1 EXPLOITATION TEAM & CONTACT

The exploitation activities are rolled out under task 6.2 of the project proposal and stretch from month 12 to 36 of the project (January 2018 – December 2019). Task leader is the consortium partner Fabasoft.

Contacts for further questions:

NAME	FUNCTION	PARTNER	E-MAIL
Björn Fanta	Task Lead	Fabasoft	bjoern.fanta@fabasoft.com
Damir Savanovic	Workpackage Lead	CSA	dsavanovic@cloudsecurityalliance.org
Luoise Merifield	Partner	SixSq	louise.merifield@sixsq.com

Table 1: Exploitation Team & Contact

5 REFERENCES AND USEFUL LINKS

[1] European Research – A Guide to Successful Communication, Luxembourg (2004)
http://ec.europa.eu/research/conferences/2004/cer2004/pdf/rtd_2004_guide_success_communication.pdf

[3] European commission, Communicating EU research (2008)
http://ec.europa.eu/research/science-society/science-communication/pdf/communicating-eu-research.pdf

[4] IPR Helpdesk:
http://www.iprhelpdesk.eu/

[5] CORDIS FP7 homepage
http://cordis.europa.eu/fp7/home_en.html

[6] Research Participant Portal – H2020 Documents:
http://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html

APPENDIX A

Clouditor TRL / MRL

Description:

The Clouditor is designed with a micro-service approach in mind and consists of several main modules as well as a plug-in architecture to support the addition of supplementary checks, tools and metrics.

- The Clouditor Engine continuously executes a defined set of checks to validate whether a cloud service complies with a set of requirements and reports its results. It currently supports checks of cloud service components provided by Amazon Web Service (AWS), Microsoft Azure and OpenStack
- The Clouditor Simulator and Evaluator components are responsible for calibrating the check and metric functions. They can be used to simulate the violation of a metric and detection, respectively. This allows for a fine-grained calibration of the metric and checks.
- The Clouditor Explorer (currently in development) is responsible for defining necessary check parameters of the audited cloud services, such as IP addresses, URLs or desired metrics
- The Clouditor Dashboard serves as a management console as well as a overview of the results gathered by other components

Technical and systematical development of Clouditor is ensured through:

- Weekly developer meetings, a central code repository using Git flow and a continuous deployment paradigm, including static code analysis tools (SonarQube)
- required changes and additions to source code are organized through professional software development management tool (Jira), as well as
- major development activities (Epics) are aligned with overall business goals to market Clouditor as a product.

In order to compare the functionality of the prototype is compared to the laboratory scale tests of the earlier developmental phase, a field trial is currently conducted in cooperation with a medium sized security service provider. Once this field trial completes, comparison of laboratory results with real-world results will be feasible.

Most notable latest advancement and learnings:

- various platform-level checks of AWS and Azure have been added, especially covering aspects of the CIS Benchmark for Azure and AWS (TODO: cite here)
- conducting the above mentioned field trial required integration of application-level as well as application-specific checks, thereby showing how Clouditor can support checks of productive cloud service on platform and application level as well as provides means to craft application-specific checks
- front end development has also been advanced significantly, including automated asset discovery as well as configuration of novel checks to check secure configuration of these assets.

Requirement:

All modules have defined interfaces between them, either in the form of an API or a shared database scheme. Each module can be deployed independently from each other as long as API or database access is allowed between deployments. To support this, Fraunhofer AISEC is heavily using container technologies, such as Docker. Thus, all modules are available as pre-built Docker images.

Requirements of Clouditor are defined specifically and in dependence of the operating scenario (i.e., produce evidence and compute measurement results based on continuous checks which can be used to validate CCM controls), including:

- automatic asset discovery and configuration of checks per non-technical UI (front end)
- technical representation for mapping between checks and CCM controls
- platform specific checks (i.e., control plane level checks) for Azure and AWS

Requirements needed to interface between Clouditor and existing cloud service components consists of

- external: make use of AWS and Azure API through available libraries
- internal: support standardized data formats and APIs for communication with instances of evidence stores (possibly provided by another service, not part of Clouditor) as well as instances of compliance reporting tools such as CSA Security, Trust & Assurance Registry (STAR)
- Definition of flexible output adapters to integrate with evidence stores and reporting tools whose formats are yet not known

Verification:

The Clouditor is developed within a Continuous Integration (CI) workflow at Fraunhofer AISEC. Source code is maintained at a central git repository, following the git flow model[2]. All changes to the git repository automatically trigger a build process in a Gitlab CI[3] server. The build is executed according to a pre-defined CI instruction file which compiles the Java source code and runs individual unit as well as integration tests. While unit tests are designed to test individual functions or functionality within one module, the integration tests observe the behavior of the modules with an embedded test infrastructure (also based on Docker containers). The last step of the build is a code quality check using the tool SonarQube[4]. Only if all the previous steps are executed correctly, the build is passed.

Once a build is passed, it is automatically deployed into a test environment within Fraunhofer AISEC, which serves as a demo platform and continuously checks security metrics of internal AWS deployments of Fraunhofer AISEC.

Various relevant scenarios are used to verify the correct behavior of Clouditor, including:

- integration tests are designed and deployed using the Kubernetes-based platform which simulate real-world scenarios
- evidence produced and measurement results computed during these integrations are rendered by the dashboard
- pilot with productive, cloud-based security service provider (see above, pilot and thus data collection to evaluate correct functionality of Clouditor in the wild is not yet completed)

Viability:

While the Clouditor development process already has a good set of unit and integration tests of individual modules, only rudimentary tests exist to automatically test the interaction between different modules. However, this is currently achieved manually by interacting with the deployments in the two test environments mentioned above.

The Clouditor Explorer, which is currently in development, will also allow a strong interoperability with existing cloud service APIs (such as OpenStack) through the automated discovery of certain parameters of cloud services (such as IPs, URLs), in contrast to a static configuration.

Potential deviations between the functionality of the Clouditor in the test environment versus the functionality of the Clouditor in the eventual operating environment have been identified, e.g.

[2] http://nvie.com/posts/a-successful-git-branching-model/
[3] https://about.gitlab.com/features/gitlab-ci-cd/
[4] http://sonarqube.com

- unexpected behavior of the service under test which may corrupt evidence production as well as measurement result computation,
- intentional, i.e. malicious modification of evidence production by a third party (external attacker) or the cloud service provider himself (internal attacker), and
- depending on the deployment and integration mode, corruption or loss of produced evidence due to error on the network layer.

Addressing such deviations from expected behavior, different measures have been implemented to discard faulty evidence and to log such errors in a verbose manner.

MRL:

The prototype originated from a funded research project, which also included industry partners. This allowed for an initial input of metric and test cases that were developed in the prototype. Fraunhofer AISEC also started to validate these test cases outside of the initial research project by establishing contact to several cloud service providers as well as service customers and is currently in the process of feeding this input back into the development process. Additionally, first steps have begun to create a financial and business plan.

A business plan which includes a milestone plan how to achieve identified business objectives given the available resources at Fraunhofer AISEC has been developed. Trademark and brand strategy have been handed over to specialized personnel at AISEC and is currently under consideration.

Further, various meetings with potential customers in the industry have been conducted to validate the overall approach, e.g. considering deployment and integration strategies and test coverage, as well as to identify unique selling propositions of Clouditor. On this basis, a market entry strategy has been developed based on a prioritized list of potential target groups, including a pricing model and a first estimation of turnover bandwidth.

Conclusion:

Clouditor has completed TRL 6, with a strong indication that the prototype is moving towards TRL 7, especially with the initiated steps such as:

- the debugging through the validation of test cases
- the use in the actual operating environment
- the automation of the interaction between different modules and
- financial plans.

APPENDIX B - EXPLOITATION ACTIVITY TRACKING

In this document, we identified four *exploitation perspectives*, which are outlining the exploitation roadmap for the project in 2019 (see also Figure 2: Exploitation Roadmap):

1. Multi-Party Recognition Framework
    - Enhance services of stakeholders like CSA, PwC and Nixu
2. Evolve STAR Program with Continuous Certification
    - adding a Continuous Certification approach and accelerate the development of the STARWatch tool v2
3. Clouditor as a product for different target groups:
    - Auditors, Cloud Users, third-party cloud integrators, Cloud Security Consultants
4. Fabasoft CAAPI
    - a generic Audit API in its SaaS solution, to provide access for accredited continuous audit processes and tools.

Additionally, we identified so called *fast exploitations*. A fast exploitation is an adhoc-opportunity to salvage project results directly into market value.

It has to be noted that such a roadmap is an evolving document; it will be subject to changes and especially in the field of Multiparty Recognition, there will be additional goals added to the timeline. To facilitate this, we are planning a series of Value Proposition Workshops with Innovation Management experts from Fraunhofer for Q4 2018 and Q1 2019. The goal of these workshops and activities is to analyze market pains and gains and to identify opportunities for our developed solutions early. The first Workshop sessions will be held online (e.g., goto Meeting) in week 49 of 2018.

To streamline the activities and to keep track of exploitation opportunities, we list all exploitation activities by the consortium and consolidate them in a jointly edited Excel spreadsheet since summer 2018. Table 2 shows an outline of these activities and their forecasts. More detailed information will be given in Deliverable D6.3; the annual dissemination and exploitation report.

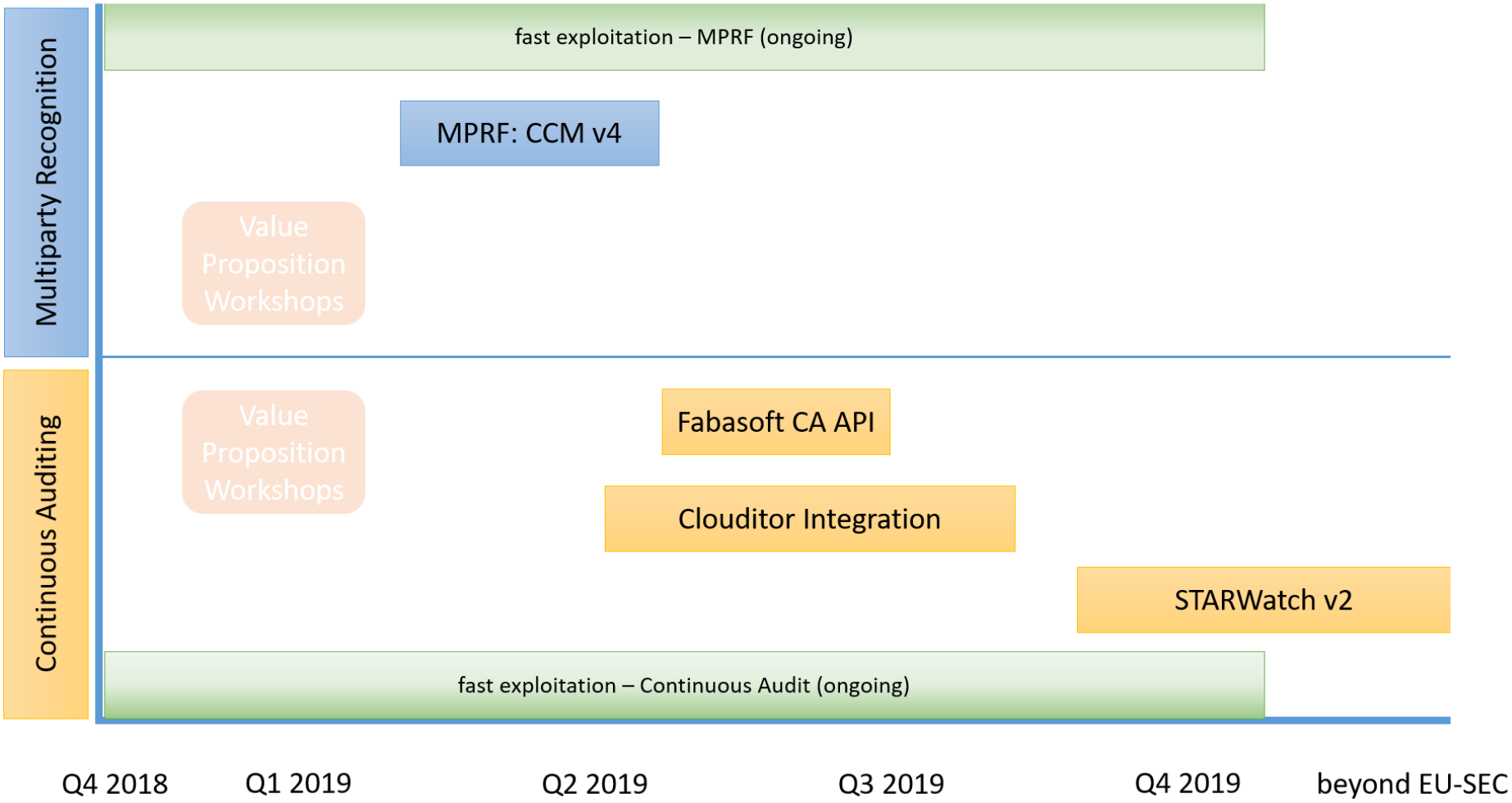

Figure 2: Exploitation Roadmap

Table 2: Fast Exploitations

Reported Semester	Organization	Projects results being exploited	Short description of: how theses results have been or are being exploited	where	when	Current status
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 documentation of implemented ISO 27017 Extended SoA controls	SI-MPA ISMS	Q1 2019	planning
Q9	SI-MPA	T4.1 Pilot audit report	Updating the documentation of implemented ISO 27017 Extended SoA controls	SI-MPA ISMS	Q1 2019	planning
Q6	CSA	Privacy Code of Conduct	Launch of the CSA Code of Conduct for GDPR Compliance - Self Assessment	NA	At InfoSecurity London 2018	Available for the general public
Q7	CSA	Privacy Code of Conduct	Launch of the CSA GDPR Center of Excellence	Berlin	At the Bitkon Privacy Conference	Available for 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 January 2019	Under public peer review
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

Table 3: Exploitation Perspectives

Quarter	Year	Organization	Project results being exploited	Short description of: how theses results are going to be exploited	where	when	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 cloud users 3rd party cloud integrators cloud security consultants		After finishing pilot 2	planning
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 RACOMAT) to integrate the CA API.	Fraunhofer Services	After finishing pilot 2	planning
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 integrated in CaixaBank for the management and control of cloud services.	N/A	After finishing pilot 2	planning
Q10	2019	PwC	EU-SEC Requirements Repository	Application of the EU-SEC Requirements Repository for analyzing 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 analyzing the potential reduction of audit effort	future projects	mid 2019	pending