EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

FINAL ANNUAL REPORT ON DISSEMINATION, STANDARDISATION AND EXPLOITATION

1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 31.12.2019	DELIVERY DATE: 09.01.2020
AUTHOR: CSA, Fabasoft	PARTNERS CONTRIBUTED: All Partners
DISSEMINATION LEVEL: * PU	NATURE OF THE DELIVERABLE: ** R
INTERNAL REVIEWERS: SIXSQ, SI-MPA	

*PU = Public, CO = Confidential **R = Report, P = Prototype, D = Demonstrator, O = Othe

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

EXECUTIVE SUMMARY

The dissemination, exploitation and standardisation activities played a critical role for the EU-SEC project. Given the perceived complexity of the solutions proposed, especially the Multiparty Recognition Framework (MPRF) and Continuous Auditing certification, we focus on ensuring that the results we produced were understood by our target audience and ready for immediate adoption.

The consortium produced comprehensive exploitation plans, disseminated the project results and materials according to the performance indicators and was involved in thorough standardization activities.

The main focus of our work in WP6 has been threefold. Firstly, the production of educational and training material so to help our reference stakeholders in putting in action the EU-SEC framework. Secondly the close monitoring of and engagement in standardisation activities related to the implementation of the EU Cybersecurity Act. And finally, the monitoring of the activities within the European Data Protection Board (EDPB) in relation to the entering into force of the GDPR.

Exploitation plans are rolled out for each partner and contain activity steps for short-, mid- and long-term visions. Some results are already exploited by so called fast exploitation, meaning that opportunities along the path were taken. For example, the project results directly led to an improvement of the Cloud Control Matrix, handled by CSA, and Fabasoft was able to apply the MPRF pilot mappings for a real business case outside the pilot.

Despite the challenges involved in relaying information on a complex and sometimes dry topic, great strides have been made in terms of dissemination. The KPIs have been met and a significant amount of material has been created to ensure the results will remain accessible after the end of the project.

From the standardisation perspective, the participation in the EC CSPCert and the frequent alignment meetings with ENISA are to be considered the most relevant achievements.

The consortium had a change in the lead of working package 6 during the middle of the project lifetime. This change brought some obstacles and delays, but the consortium as a whole was able to rise to the challenge.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

The final deliverable of the project EU-SEC is split in three major parts: Exploitation (chapter 1), Dissemination (chapter 2) and Standardization (chapter 3).

Chapter 1 presents the way of all project partners to short-, mid- and long-term exploitation plans and activities. It starts out by showing the efforts by applying a business model canvas approach with the help of two Fraunhofer FOKUS innovation experts (Nathalie Brandmayr and Alexander Mappes) and the result tables. In the following parts of this document, each partner presents their individual exploitation perspective and exploitation tables. Exploitation in the EU-SEC project is split into two categories: Multiparty Recognition Framework (MPRF) and Continuous Audit Based Certification (CABC). Not all partners have exploitation plans for both, MPRF and CABC, this is due to the fact that partners like Fraunhofer AISEC where only involved in working packages and activities related to CABC, for instance.

Chapter 2 showcases the key performance indicators (KPI) the consortium set up for this project and lists them together with the reached values over the past three years. It also presents the dissemination activities carried out during the project, including information on website activity, the social network accounts and how they have been used. The EU-SEC consortium has been successful with respect to the dissemination plan for all activities, and disseminated the project results at conferences and events, organised workshops and webinars, and reached out to the certification community. Following the increase in social network activity, the project became more visible in these media and reached a wider public. The consortium has been attending events as put forward in our dissemination plan in order to establish contacts with the target groups defined initially. Finally, the consortium was successful in contacting relevant projects, in order to establish collaboration networks with our target groups that will continue existing after the end of the project.

Chapter 3 is focused on standardization activities and it looks into the compliance landscape during the project life-cycle. The biggest change was introduced in 2019 with the new EU Cybersecurity Act and its cybersecurity certification scheme. Additionally, the survey was conducted towards the end of the project to identify any additional standards that might not have been originally considered by the project and evaluate how the MPRF and CABC approaches are accepted.

1 EXPLOITATION

In this chapter we discuss the EU-SEC project innovations together with the minimal viable products (MVP) for Multi Party Recognition and Continuous Audit Based Certification and wrap up the business model canvas results conducted during the first half of 2019. After presenting the result tables of the business model canvas workshops, each partner will frame their exploitation plans for the time of the end of the project and beyond.

To talk about the exploitation activities within this project and beyond, one question plays a central role: "What is innovative about the project?"

Our answer to this is: The growth of cloud services poses challenges to both cloud users and cloud service providers (CSPs). Potential customers are prevented from adopting cloud services due to concerns about transparency, security and privacy, as well as confusion over the plethora of certification schemes. The innovative ***European Security Certification Framework (EU-SEC)*** tackles this by providing a set of tools based on a tailored architecture, currently unavailable on the market, to improve the **efficiency** and **effectiveness** of current assurance schemes targeting **security**, governance, risk management and **compliance** in the Cloud. It provides and evaluates:

- a multiparty recognition approach between existing cloud security certification schemes (MPRF) and
- a continuous auditing-based certification scheme (CABC).

1.1 SHORT INTRODUCTION TO THE EU-SEC RESULTS

MPRF: third-party audits and certifications provide assurance and promote trust regarding a cloud service provider's approach to security and privacy. They are also a credible way to show compliance to standards and regulations. Unfortunately, though, the number of existing national, international and sectorial standards, laws and regulations has drastically increased in recent years, leading to increased complexity of the area of compliance. Just take a look at the number of schemes around. And that's not the whole picture. Such a proliferation of requirements has had the direct consequence of an increased cost of compliance for Cloud Service Providers (CSPs), which in some cases is reflected in an increased service price for the cloud customer.

Cloud service providers are under considerable pressure to comply with several international, national, and sector specific standards and requirements. Such a proliferation of standards and requirements demands more resources be spent, increases compliance acquisition costs, and potentially also creates room for security vulnerabilities. Consequently, the process of adhering to different standards, laws and regulations for CSPs is inefficient, with a lot of duplicated work that unduly increases costs and complexity. The EU-SEC project has worked on addressing these issues by, for instance, identifying the common denominators between widely known standards and presenting them under a well-defined and comprehensive framework, namely the EU-SEC's "Multi-Party Recognition Framework" (MPRF). The Framework has been validated by 4 consortium members in a 12-month pilot, the results of which have been used to improve the Framework.

CABC: Concerns about security, privacy and regulatory requirements hinder cloud adoption, especially for customers working with sensitive data. Third- party certification and attestation play a key part in a cloud assurance program, but they don't go far enough. Traditional point-in-time auditing doesn't completely allay fears, due, amongst other things, to lapse of time between audits and lack of automation. The EU-SEC project's solution is to adopt a Continuous Auditing based Certification for cloud services.

Third party security audits and certifications are traditionally performed annually or bi-annually, which means that whenever interim changes are made to security and privacy practices, the change and effectiveness of these amendments are not evaluated by the assessors until the next official check. The EU-SEC project has developed a process that allows continuous assurance by addressing the lack of regularity and proactivity of traditional "point-in-time" certifications. Continuous auditing-based certification completes the Level 3 of the Open Certification Framework and builds upon the STAR Level 1 and Level 2. By using technology to monitor and flag non-compliant activity on an ongoing basis, continuous auditing delivers an enhancement to traditional certification. It increases the assessment frequency via a continuous workflow. State of the art security monitoring systems supervise the organization's security status by collecting data from the CSP's information system. This collected data is further assessed and normalized making assessments unambiguous, repeatable and comparable across different information systems.

1.2 BUSINESS MODEL CANVAS ACTIVITIES IN THE LIGHT OF EU-SEC EXPLOITATION

In February 2019, the project partners conducted a business model canvas workshop under the guidance of Fraunhofer FOKUS Innovation Expert Alexander Mappes. The results will be shown on the following pages in the form of pictures and tables.

Figure 1 and Figure 2 show the first results achieved during the project Meeting in Helsinki, at the Nixu headquarters. All partners contributed and discussed their view on key partners, key activities, value propositions, customer segments, channels, cost structure and revenue streams. This activity was moderated by Alexander Mappes and conducted for both innovations: Multiparty Recognition Framework and Continuous Audit Based Certification.

After this workshop, individual (internet call based) workshops were planned and held with the first results as input. For this exercise, the project partners were distributed to the identified stakeholder groups:

- Scheme Owners: CSA (Figure 3)
- Auditors: Nixu (Figure 4)
- Cloud and Digital Service Providers: Fabasoft, SixSq (Figure 5)
- Cloud Customers Caixa Bank (Figure 6)

Again, these workshops were moderated by Alexander Mappes, with support by Björn Fanta, Fabasoft.

The results were aggregated and used to comprise value propositions for MPRF as well as CABC (see Figures 3 - 6). With these value propositions, each partner had to work on their individual exploitation plan and activities. This is presented in the following chapters of Section 2 of this document.

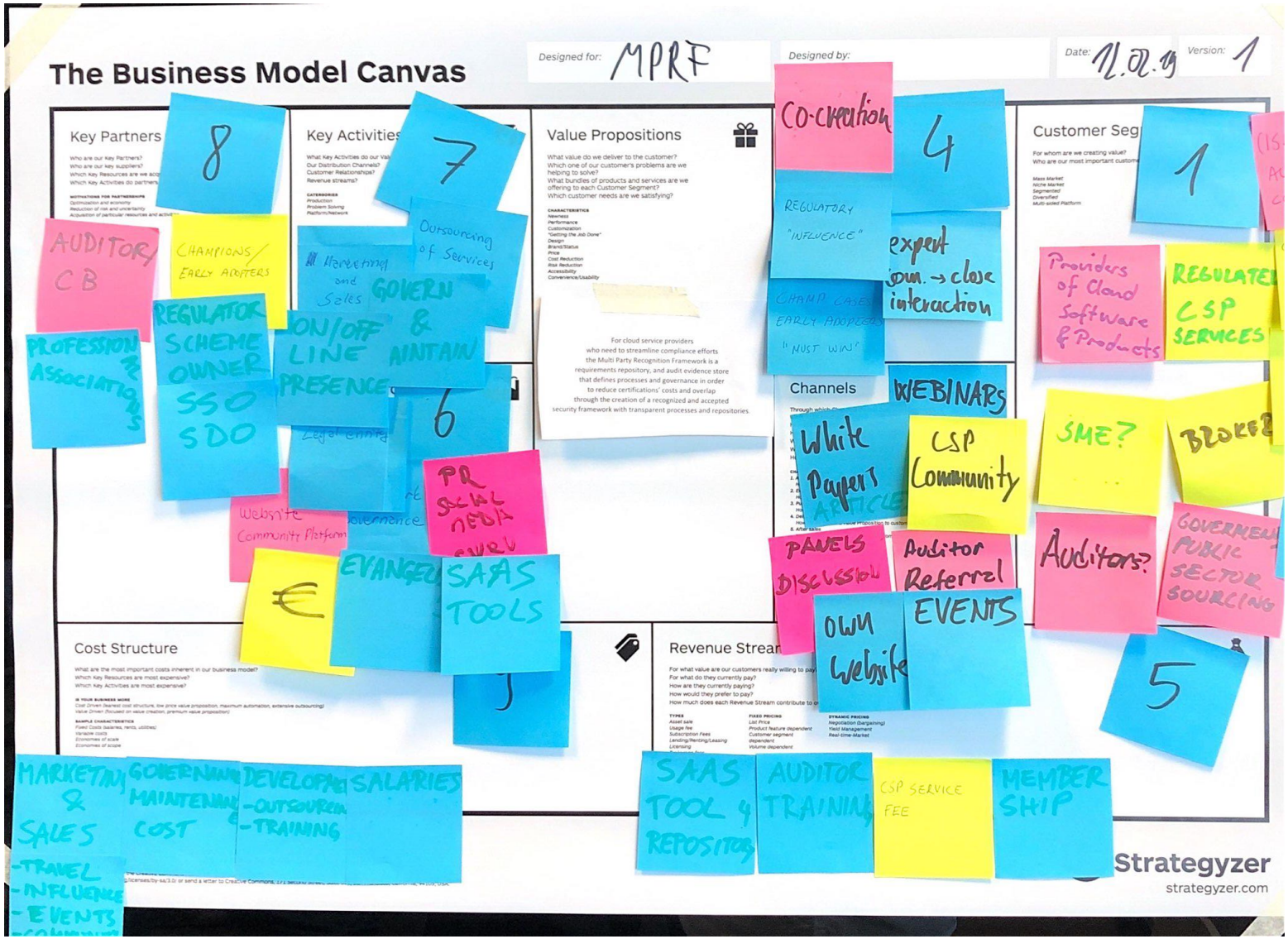


Figure 1: 1st Result Business Model MPRF

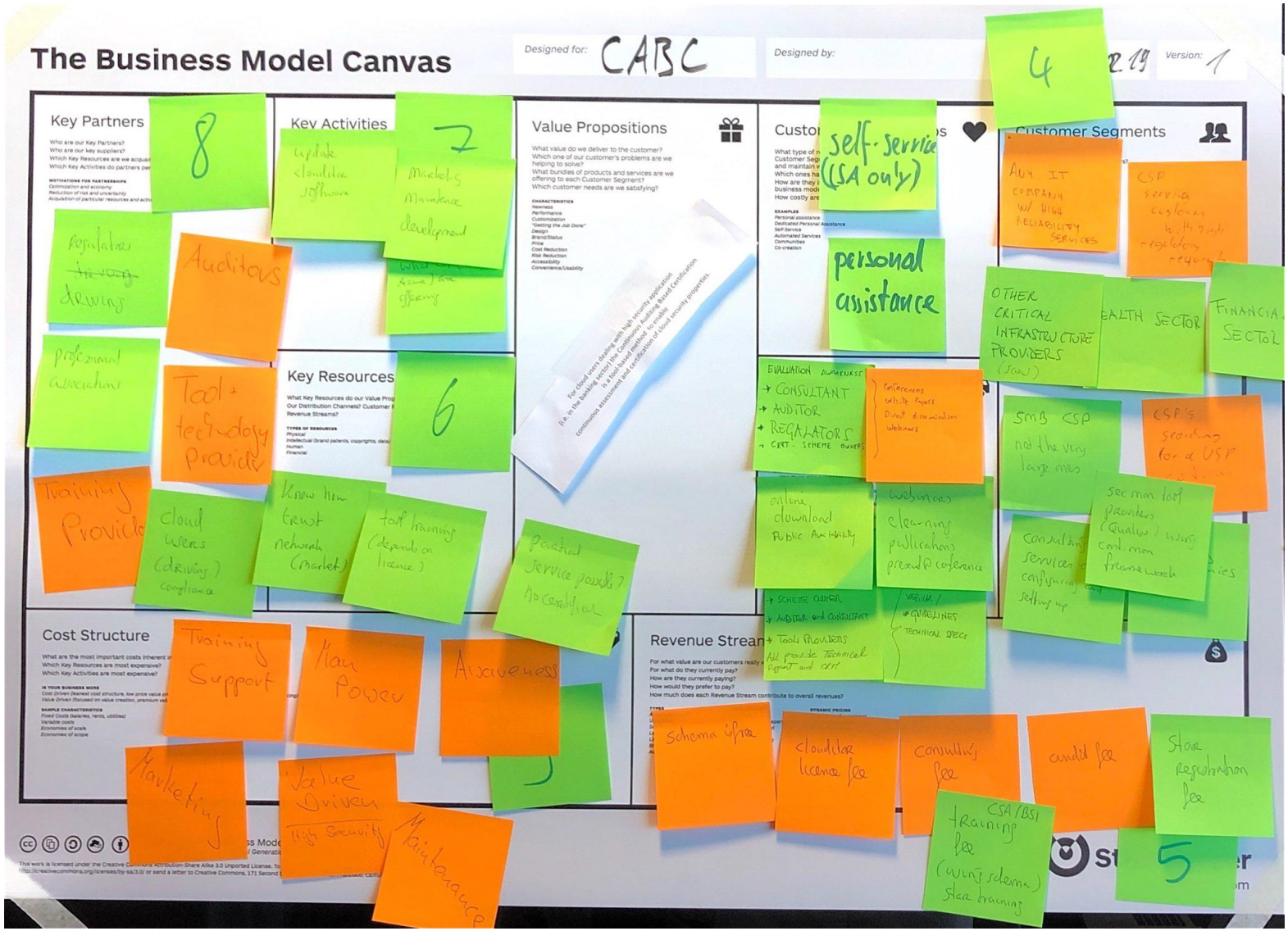


Figure 2: 1st Result Business Model CABC

The Business Model Canvas

Designed for: EU-SEC CABC
Designed by: SCHEME OWNER PERSPECTIVE (CSA)
Date: 21.03.19
Version: 1

Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquairing from partners?
Which Key Activities do partners perform?

MOTIVATIONS FOR PARTNERSHIPS
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities

CSP
- Auditors / Consultant
- Technology Provider
- Regulators (supporting / pushing the effort of being certified continuously)

Auditor / Consultant
- Auditors / Consultant
- Technology Provider

Cloud Customer
- Auditors / Consultant
- Technology Provider
- Regulators (supporting / pushing the effort of being certified continuously)

Key Activities

- Co-creation (offering of platform and channels) of marketing activities, when it comes to spread the word of the importance of the certification / schemes
- Creation of content for the website
- Networking activities
  - Community of public stakeholders
  - Community of target customers
- Development / refinement of intellectual property (within working group activities)
- Ensure that international standard is created out of what CSA is doing
- Contributing to and influencing international standard and (European) policy
- Set specification that technology providers have to follow
- Investigation on the exploitation of the data in the registry
- Creating awareness about
  1. the problem of / need for continuous auditing (creating the market) and
  2. How to implement it / do so (offering a solution)

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

TYPES OF RESOURCES
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial

- Intellectual property
- Network / community
- Well-known within the cloud community and trustworthy brand

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

CSP
- Assurance and transparency beyond the current state of art
- Framework which enables them to get certified continuously
- Methodology = overall approach needed to implement a continuous auditing
- Guidance to do the implementation (free material + paid trainings)
- Better visibility through public registry / website of their quality / excellence ("showoff" CSP)
- Differentiate / competitive advantage from "big players"

Auditor / Consultant
- Option of extending their offering (added value services = CSPs value proposition) ➔ continuous auditing requires guidance / support, especially in the beginning

Training partners
- Training (material created in house, trainings licensed, "business as usual, remaining trusted 3rd party") for the support / guidance needed from CSP (paid)

Cloud Customer
- Certification
- Information on the registry (API to registry's information) or: Better visibility (compare to insight / access to security / registry information)

Customer Relationships

Lifecycle of relationship (all customers)
- In beginning: close relationship, lots of guidance and personal support (empowerment of the customers) (cost intense)
- Later on: rather lose relationship specific questions, support for individual needs
- Co-Marketing (rethink the aspect of "patronage", Less influence / endorsement) (indirect revenue, no costs)

(Awareness => knowledge => guidance)

Channels

CSP
- Direct channels
  - Website / e-mail
  - Conferences / public speaking events
- indirect channels
  - Via partners such as auditors / consultants
  - Training partners

All customers
- Sales team (STAR program)
  - Membership is sold not certification itself
  - Scheme as a benefit
- Direct channels (see above)
- Journals and white papers

Customer Segments

For whom are we creating value?
Who are our most important customers?

Mass Market
Niche Market
Segmented
Diversified
Multi-sided Platform

Target customers
1. CSP
2. Auditor / consultant
3. Cloud Customer
4. Training partners (might include auditors, consultants or other training institutions preparing CSPs and auditors for audits with education, training etc.)

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

IS YOUR BUSINESS MORE
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)

SAMPLE CHARACTERISTICS
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope

Manpower
- Content (training, awareness material & website)
- Network
- Customer support
- Analysis of data expoitation

Marketing
- Traveling (time consuming)
- Website

Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

TYPES
Asset sale
Usage fee
Subscription Fees
Lending/Renting/Leasing
Licensing
Brokerage fees
Advertising

FIXED PRICING
List Price
Product feature dependent
Customer segment dependent
Volume dependent

DYNAMIC PRICING
Negotiation (bargaining)
Yield Management
Real-time-Market

Direct revenue
- Registration to the STAR-registry (public website)
- Royalties from trainings
- Monetarization of the registry data ➔
  1. licensing the API (= automatic access to the data)
  2. further ways of using the data generated (tbd)

Indirect
- CSA annually membership fee
- Up-sale ➔ additional marketing on CSA platform

Strategyzer
strategyzer.com

Figure 3: Individual BMC Scheme Owners

The Business Model Canvas

Designed for: EU-SEC CABC
Designed by: AUDITORS (NIXU)
Date: 28.03.19
Version: 1

Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquairing from partners?
Which Key Activities do partners perform?

MOTIVATIONS FOR PARTNERSHIPS
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities

- Fraunhofer AISEC (Clouditor)
- CSA (Star-Watch)
- SixSq (Nuvla)
- Certification scheme owner
  - Providing requirements of certificates
- Accreditor (providing the license to do audits)

Key Activities

What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?

CATERGORIES
Production
Problem Solving
Platform/Network

- Build the service
  - Design the service architecture
  - Databases of customers have to be implemented
  - Integration of Clouditor and star watch
- Create / buy hosting capacities
- Service description, model of operation and description for the customers
- Broaden customer-base
  - Marketing efforts
- Create a service / use case for the pilot customer

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

TYPES OF RESOURCES
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial

- Intellectual resources / Know How
- people offering operational support (human resources)
- Network of customers
- Infrastructure to run CABC

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

CHARACTERISTICS
Newness
Performance
Customization
"Getting the Job Done"
Design
Brand/Status
Price
Cost Reduction
Risk Reduction
Accessibility
Convenience/Usability

- Computer assisted, automated auditing
  - Audit support
  - Increase in productivity of audits
  - Raised confident that everything is audited / in place **continuously** → not just point in time auditing
- RoI increases → Assurance about security standards raises more than the costs

Customer Relationships

What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?

EXAMPLES
Personal assistance
Dedicated Personal Assistance
Self-Service
Automated Services
Communities
Co-creation

- Continuous service = Our desk, their desk and a service interaction with continuous exchange
- Re-occurring service (once-a-year-service)
- Strong and close relationship
- Audits remain personal (yearly) on top an ongoing automated, technology based data exchange including in person maintenance / support (technology augmented)

Channels

Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?

CHANNEL PHASES
1. *Awareness*
   How do we raise awareness about our company's products and services?
2. *Evaluation*
   How do we help customers evaluate our organization's Value Proposition?
3. *Purchase*
   How do we allow customers to purchase specific products and services?
4. *Delivery*
   How do we deliver a Value Proposition to customers?
5. *After sales*
   How do we provide post-purchase customer support?

- Pilot-Customer as a success-story and leverage for similar customers
- Contact / using existing customers
- Awareness also through webpage
- Breakfast seminars
- Awareness: Conferences (before market entrance)

Customer Segments

For whom are we creating value?
Who are our most important customers?

Mass Market
Niche Market
Segmented
Diversified
Multi-sided Platform

- Financial sector = Banks
- Cloud Service Providers (digital service providers In general)
  - Platform providers
  - Infrastructure providers
  - Something-as-a-service providers

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

IS YOUR BUSINESS MORE
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)

SAMPLE CHARACTERISTICS
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope

- Operating cost of running the service
  - ramp up cost (once / not very often per customer)
  - Operating costs continuously
  - Hosting, infrastructure, databases…
- Building the service
  - Plan, design, build phase (manpower, software, hardware)
- Auditing costs (for the service itself)
- Licensing costs for the tools
- Marketing costs
- Training costs
  - Operating trainings
  - Sales trainings

Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

TYPES
Asset sale
Usage fee
Subscription Fees
Lending/Renting/Leasing
Licensing
Brokerage fees
Advertising

FIXED PRICING
List Price
Product feature dependent
Customer segment dependent
Volume dependent

DYNAMIC PRICING
Negotiation (bargaining)
Yield Management
Real-time-Market

- Add on (and continuous) service
- Monthly fee (additional to regular auditing fee)
  - Including predefined services e.g. Technical support
- Individual pricing depending on…
  - Depending on the scope (is the scope the same as in the audit? One or one hundred requirements being checked?) there are different fees charged
  - Cross service → cyber defense service + auditing certificate + …
- Limiting factor: Impossible to audit and consult at the same time → chose which perspective / role you take

Figure 4: Individual BMC Auditors

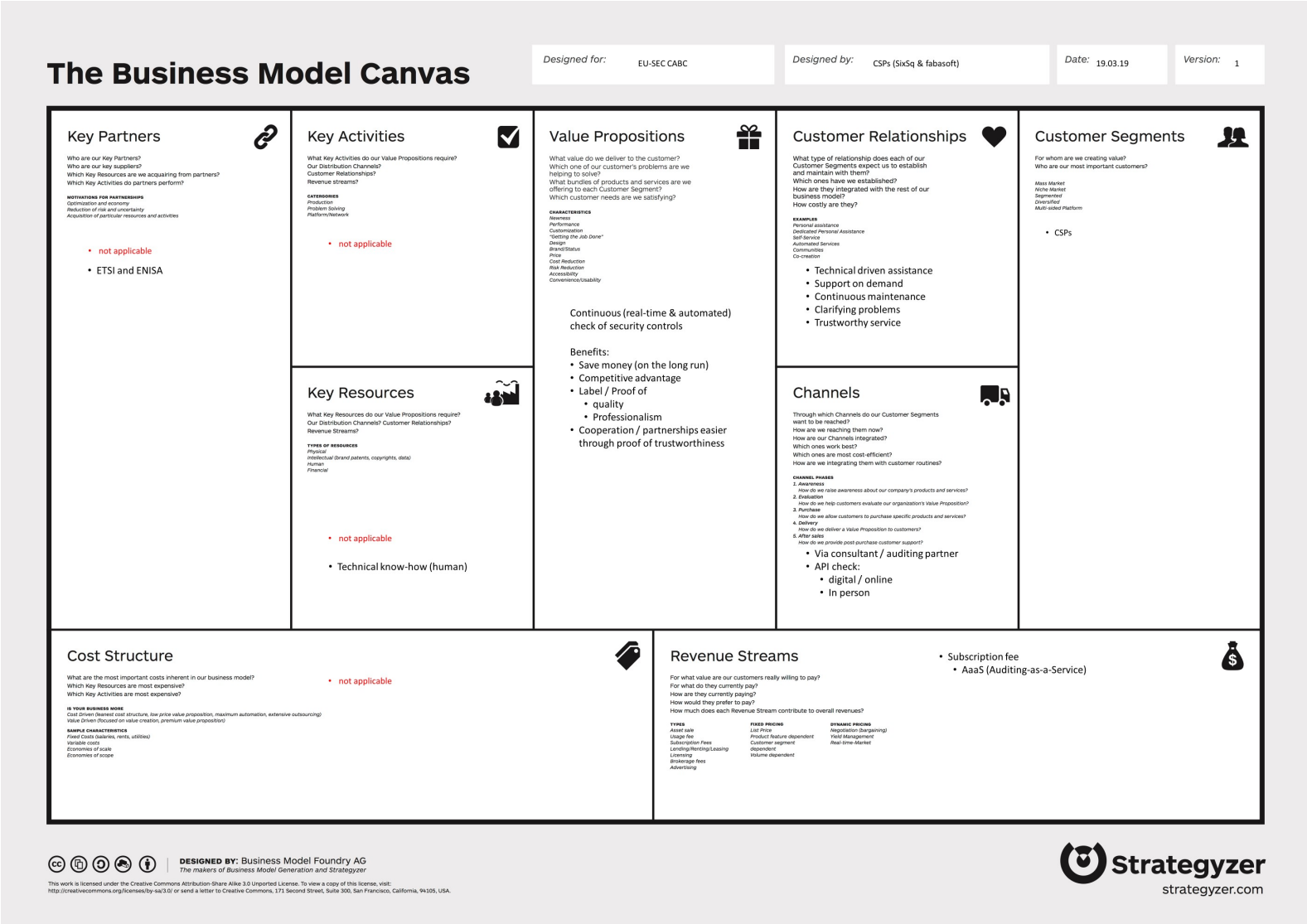


Figure 5: Individual BMC Cloud and Digital Service Providers

The Business Model Canvas

Designed for: EU-SEC CABC
Designed by: Caixa Bank
Date: 01.04.20019
Version: 1

Key Partners

Who are our Key Partners?
Who are our key suppliers?
Which Key Resources are we acquairing from partners?
Which Key Activities do partners perform?

MOTIVATIONS FOR PARTNERSHIPS
Optimization and economy
Reduction of risk and uncertainty
Acquisition of particular resources and activities

- not applicable

Key Activities

What Key Activities do our Value Propositions require?
Our Distribution Channels?
Customer Relationships?
Revenue streams?

CATEGORIES
Production
Problem Solving
Platform/Network

- not applicable

Key Resources

What Key Resources do our Value Propositions require?
Our Distribution Channels? Customer Relationships?
Revenue Streams?

TYPES OF RESOURCES
Physical
Intellectual (brand patents, copyrights, data)
Human
Financial

- not applicable

Value Propositions

What value do we deliver to the customer?
Which one of our customer's problems are we helping to solve?
What bundles of products and services are we offering to each Customer Segment?
Which customer needs are we satisfying?

- **Certification: Compliance is proven** & assurance about security check → demonstration to regulators that standards / requirements are being met = credibility
- Facilitate the adoption of cloud services and the externalization of services to the cloud
- Sharing of best practices in continuous auditing (missing information)
  - Especially when many CSPs get involved / use CABC
- Cost reduction → especially if no point in time audits are needed anymore (payment just for the solution if CABC would substitute point in time audits) otherwise reduced time for point in time audits
- Demonstrate trustworthiness to own customers

Customer Relationships

What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
Which ones have we established?
How are they integrated with the rest of our business model?
How costly are they?

- Support (from a European, public institution / organization) when talking to regulatory instances
- Community of stakeholders from different public institutions
- Regulatory aspects should remain by "objective" scheme owner
- Professional relationship, personal assistance not needed (CSP would need personal assistance)
- Public, objective, transparent and detailed documentation of certification / auditing process

Channels

Through which Channels do our Customer Segments want to be reached?
How are we reaching them now?
How are our Channels integrated?
Which ones work best?
Which ones are most cost-efficient?
How are we integrating them with customer routines?

- Personal contact to auditor
- Request or recommendation of regulatory instance
- Change of auditor every x years → providers of audits are in data bank, are then invited to propose their service, "best" is chosen ("best" depending on the criteria)

Customer Segments

For whom are we creating value?
Who are our most important customers?

Mass Market
Niche Market
Segmented
Diversified
Multi-sided Platform

- Caixa as a customer of cloud service providers & auditors

Cost Structure

What are the most important costs inherent in our business model?
Which Key Resources are most expensive?
Which Key Activities are most expensive?

IS YOUR BUSINESS MORE
Cost Driven (leanest cost structure, low price value proposition, maximum automation, extensive outsourcing)
Value Driven (focused on value creation, premium value proposition)

SAMPLE CHARACTERISTICS
Fixed Costs (salaries, rents, utilities)
Variable costs
Economies of scale
Economies of scope

- not applicable

Revenue Streams

For what value are our customers really willing to pay?
For what do they currently pay?
How are they currently paying?
How would they prefer to pay?
How much does each Revenue Stream contribute to overall revenues?

TYPES
Asset sale
Usage fee
Subscription Fees
Lending/Renting/Leasing
Licensing
Brokerage fees
Advertising

FIXED PRICING
List Price
Product feature dependent
Customer segment dependent
Volume dependent

DYNAMIC PRICING
Negotiation (bargaining)
Yield Management
Real-time-Market

- Option1: If CABC is independent of auditors: subscription fee (preferred option)
- Option2: If CABC added service of auditors: extra cost to "normal" audits (dynamic price)
- Value willing to pay for: Continuous audit and framework consisting of an accepted set of predefined, continuously updated controls

Figure 6: Individual BMC Cloud Customers

1.3 FRAUNHOFER FOKUS

Fraunhofer FOKUS is a research institute contributing to research projects and providing consulting services for the private and public sector. Working on Projects like EU-SEC gives FOKUS a first-class opportunity to evolve on its previous research and development as well as start new initiatives. During EU-SEC FOKUS was able to proceed on its research on risk assessment and certification methods and therefor extend its experience in that area as well as starting the development of new technologies. The exploitation plans are based on the two innovations multi-party recognition framework as well as the continuous auditing-based certification.

1.3.1 MPRF BASED EXPLOITATION

The MPRF provides the potential of streamlining certification efforts by using artefacts of already existing certifications. FOKUS will evolve its consulting services by applying the knowledge of MPRF. Other exploration activities based on MPRF include the development of a Web application which makes the usage of the EU-SEC repository more intuitive than in its current spreadsheet form.

1.3.2 CABC BASED EXPLOITATION

CABC provides assurance based on continuous auditing. This requires the knowledge of breaking down certification goals in to measurable artefacts, an expertise that FOKUS obtained during the EU-SEC project. Therefor FOKUS is expanding its consulting services in this area. FOKUS mainly participated in the development of the Audit-API, which was publishes as an open source software during the project. Further improvement in other research projects is planned. FOKUS will use its Implementation of the FISH use case for demonstration purposes.

1.3.3 EXPLOITATION PLAN FRAUNHOFER FOKUS

Table 1: Detailed exploitation plan Fraunhofer FOKUS

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Define a viable product (Audit API, Methodology, consulting and development services, CABC package) and its business requirements 2. Spread and announce the innovation and its potential 3. Get community involved in specification and development 4. Develop the prototype of the MPRF Web application	R&D activities Improvement of the technology on the basis of the EU-SEC use cases and pilots. Launch as an open source project (see detailed actions in columns below) Start the development of the MPRF Web application	Getting contributions from the open source community. Engaging CSP to use the MPRF Web application	**Running**
	1. Identify the business value of consulting in CABC and development services implementing the audit API	Creating a Business Model Canvas for CABC.	Business canvas validated	**Success (Canvas created)**

	1. Raising awareness on conferences and workshops 2. Increase acceptance at the industry and open source community	Participation in industrial or academic conferences, workshops and fairs	Publication and adoption at conferences and workshops	**Success** (WETICE 2019, 16 BSI Sicherheitskongress, ETSI Security Week) **Running** (more tutorials on conferences and workshops)
	1. Acquisition of funding for product preparation Fraunhofer consulting on CABC and API implementation	Application for European Business Acceleration Programs	Project application is successful	**To be started**
	1. Acquisition of future projects for extending and specializing the CABC concept and the Audit API	Application for H2020 and national follow up programs	Project application is successful	**Running** (Fraunhofer applies for several H2020 projects related to cyber security e.g. CERT-ATTEST)
	1. Collecting user feedback	Tool evaluation with project partners.	Partner shows interests and provides feedback.	**Success (Pilots succeeded)**
	1. Start to develop the Audit API as an open source project.	Publish the project on Github.	Github is the main development resource for the Audit-API.	**Success (available)**
	1. Start the development of the MPRF Web application.	Define use cases and develop a prototype	Get feedback from the community.	**Success**

Market Evaluation phase: During 2 years after the project	1. Establishing a customer base for consultancy in the (continuous) certification market 2. Establishing an active open source community around the Audit API 3. Achieving TR-Level 6 for the Audi API 4. Achieving TR-Level 3 for the MPRF Web application	R&D activities Improvement of the technology on the basis of customer experiments. Acquisition of additional funding. Acquisition of customers for continuous based auditing. Active open source development of the Audit API. Improve on the MPRF Web application (see detailed actions in columns below)	Reaching TR-Level 6 for the Audit API An initial customer base for consultancy in the (continuous) certification market has been established. Managing the development of the Audit API. Managing the development of the MPRF Web application (see detailed criteria in columns below)	**To be started**
	1. Acquisition of funding for product preparation of CABC and the Audit API	Application for FhG start-up funding schemes	Project application is successful	**To be started**
	1. Establishing a customer base for consultancy in the certification market 2. Establishing a customer base for the Audit API 3. Establishing an active open source community. 4. Achieve a proper TRL Level for the MPRF Web application	Contacting potential customers in the critical cloud domain. Contacting multipliers like auditing companies Contacting multipliers like cloud service providers	Customer are interested in certification services from Fraunhofer Web application attracts User	**To be started**

Market Establishing phase: During 4 years after the project	1. Establishing the Audit-API as stand-alone product and service 2. Establish the MPRF Web application as the go to place for automated MPRF and generating revenue. 3. Establishing a Freemium Model for the MPRF Web application.	Improvement of the technology on the basis of customer relationships and internal use. Acquisition of customers for security testing as a service. Acquisition of customers for the Audit API. Attraction of Users for the MPRF Web application. Having a significant Number of paid Users for the MPRF Web application	A solid customer base for security testing as a service has been established. An initial customer base for the Audit API and CABC has been established. A solid user base for the MPRF Web application (see detailed criteria in columns below)	**To be started**

1.4 FRAUNHOFER AISEC

Fraunhofer AISEC is part of the Fraunhofer-Gesellschaft and thus contributing to research projects and providing consulting services for the private and public sector. Within EU-SEC Fraunhofer AISEC was primarily responsible for the overall design of the technical architecture (WP3) as well as providing the necessary tooling for continuous auditing-based certification in the WP5 pilot. During the course of the project, the prototype Clouditor was improved in its technology readiness level and eventually made open source to provide its code base to a larger community. The exploitation plan is mainly based on the continuous auditing-based certification.

1.4.1 CABC BASED EXPLOITATION

Within the project Fraunhofer AISEC has gained the necessary knowledge to support partners within the private and public sector to implement the technical measures needed for continuous based auditing. This expertise is vital for Fraunhofer AISEC to attract more customers in its field of Cloud Security research and already has led to new projects, especially in domains with similar high regulations such as the medical domain. The expertise gained from the financial pilot can be leveraged to handle the special requirements of those fields. Furthermore, Fraunhofer AISEC is planning to participate in further public funded research projects in the field of cloud security and certification on a European as well as national level.

1.4.2 EXPLOITATION PLAN FRAUNHOFER AISEC

Table 2: Detailed exploitation plan Fraunhofer AISEC

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Define a viable product (Clouditor, Methodology, consulting and development services) and its business requirements 2. Spread and announce the innovation and its potential 3. Get community involved in specification and development	R&D activities Improvement of the technology on the basis of the EU-SEC use cases and pilots. Launch as an open source project (see detailed actions in columns below)	Getting contributions from the open source community	**Success** (published on GitHub)
	1. Raising awareness on conferences and workshops 2. Increase acceptance at the industry and open source community	Participation in industrial or academic conferences, workshops and fairs	Publication and adoption at conferences and workshops	**Success** (WETICE 2019) **Running** (more tutorials on conferences and workshops)

	1. Acquisition of future projects in the context of continuous auditing	Application for H2020 and national follow up programs	Project application is successful	**Running** (Fraunhofer AISEC applied for several H2020 calls related to cyber security e.g. SU-ICT-02-2020)
	1. Collecting user feedback	Tool evaluation with project partners.	Partner shows interests and provides feedback.	**Success** (Pilots succeeded)
Market Evaluation phase: During 2 years after the project	1. Establishing a customer base for consultancy in the (continuous) certification market 2. Establishing an active open source community around Clouditor 3. Achieving TR-Level 8 for the Audi API	R&D activities Improvement of the technology on the basis of customer experiments. Acquisition of additional funding. Acquisition of customers for continuous based auditing. Active open source development of Clouditor. (see detailed actions in columns below)	Reaching TR-Level 8 for Clouditor An initial customer base for consultancy in the (continuous) certification market has been established. Managing the development of Clouditor (see detailed criteria in columns below)	**To be started**
Market Establishing phase: During 4 years after the project	1. Establishing Clouditor-as-Service as stand-alone product and service	Improvement of the technology on the basis of customer relationships and internal use. Establishment of a spin-off company outside of	A solid customer base for Certification-as-a service has been established. An initial customer base has been established.	**To be started**

		Fraunhofer Acquisition of customers for Certification as a service. Acquisition of customers for the service.		
	1. Establishing initial customer contact	Initiation of marketing activities Contacting existing customers in the critical cloud domain	Customer is interested in certification services from spin-off company	**To be started**

1.5 CSA

CSA, as a non-profit organisation, is the reference organisation for assurance in the cloud, providing tools that fit all types of organisations and risks. By being the first organisation offering a CABC framework and a solution for GDPR compliance, CSA will strengthen its lead in the assurance market. CSA aims to extend its assurance and certification program (STAR) on the basis of the results of the EU-SEC project and release: a Continuous Audit Based Certification (CABC) and a solution for GDPR compliance. Currently CSA already offers four types of assurance tools:

- Cloud security self-assessments based on the Consensus Assessment Initiative (CAIQ) or the Cloud Control Matric (CCM).
- Cloud security Continuous self-assessments based on the Consensus Assessment Initiative (CAIQ) or the Cloud Control Matric (CCM). This option represents already an exploitation of the results of the EU-SEC project.
- "Traditional" third party-certifications or attestations for cloud security, through the CSA STAR program. The proposed certification is founded on ISO27001, while the attestation is based on SOC 2.
- CSA Code of Conduct for GDOR compliance, which an evidence-based self-assessment derived from the Privacy Level Assessment Code of Conduct (PLA CoC).

For all these existing tools, CSA acts as a Certification Authority, defining the relevant assurance criteria, certification mechanisms, auditor qualification requirements, program oversight and governance mechanisms. It also maintains the STAR Registry: a freely accessible database of cloud services that have successfully applied these assurance tools, as a vehicle for transparency and trust.

1.5.1 MPRF & COC BASED EXPLOITATION

By exploiting the project results, an additional tool for GDPR compliance will likely appear in 2020, with the release of the CSA third-party certification. Such a new compliance option will to satisfy the requirements of the Article 42 of the GDPR. It will be based on the work done on the PLA CoC (D2.3). Additionally, on the privacy / GDPR front, CSA is currently working on:

- obtaining the approval of the its Code of Conduct by the European Data Protection Board (at this purpose a meeting to discuss the final review from the French Data Protection Authority – CNIL took place on the 17th of December in Paris) under the requirements of Article 40 of the GDPR.
- Finalising the CSA GDPR scheme and obtaining the approval of the EDPB (the scheme has been completed and will be submitted to CNIL for an initial assessment before the end of 2019) under the requirements of Article 42 of the GDPR.
- Defining the go-to-market strategy for both CSA GDPR CoC and Certification.

In order to support a quick uptake of both the Code of Conduct and the Certification, CSA has already:

- the CSA GDPR Code of Conduct as not-approved solution for GDPR alignment (nine (9) submissions have been already received)
- the CSA Code of Conduct and Certification Lead Auditor and Consultant training (three (3) successful training sessions already took place)
- translated the Code of Conduct into ten (10) languages
- signed an agreement with the company OneTrust for the inclusion of the controls within the CSA GDPR CoC (PLA Code of Practice) into their tool "Vendor Risk Management".

1.5.2 CABC BASED EXPLOITATION

CSA aims to add Continuous Audit Based certification (CABC) to this list of assurance tools, with the 3 assurance levels defined in the EU-SEC project. And in this context, CSA will naturally play the role Certification Authority as well. It shall be noticed that while the "Continuous Self-Assessment" option has been already made available, CSA is currently finalising the internal scheme, the supporting material and branding of the "Extended Certification with C Continuous Self-Assessment" which will be made available in February 2020.

The task at hand is to provide a set of best practices and guidance supporting continuous audit-based certification, from a more practical point of view. The main issue is to define a set of industry standard cloud metrics that can be used as starting point for cloud service providers for audit-based assurance. While the EU-SEC project already defined a dozen metrics, a substantially broader catalogue needs to be available to auditors and auditees. CSA has started contacting cloud security monitoring tool vendors in order to establish a working group in early 2020 that would aim to create such a catalogue based on existing technical offerings.

1.5.3 EXPLOITATION PLAN FOR CABC

Table 3: Detailed exploitation plan CSA for CABC

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	Engage with various stakeholders (i.e. CSA, cloud customers, auditing and consulting companies, security solution providers) in order to extend the scope of the CSA Open Certification Framework Working Group and build a certification scheme for CABC.	Use CSA network to connect with relevant stakeholders.	Define the final draft of the scheme for the CABC. Set up a dedicated sub-group within OCF for the definition a metrics catalogue	**Running**
	Build supporting standards and best practices for cloud security metrics.	Use CSA working group to produce consensus. Biweekly working sessions.	Production of first version of metrics catalogue and guidance for CABC.	**To be started**
	Technical integration with CSA infrastructure.	Work with the CSA dev team to merge EU-SEC specific changes to STARWatch into mainstream platform, and update STAR Registry.	Updated and tested platform is operational.	**To be started**
	CABC scheme final version	Achieve consensus on the	Publish the final scheme and	**To be started**

		final scheme and metrics catalogue	supporting material for the CABC.	
Market Evaluation phase: During 2 years after the project	Full scale CABC "Third party certification" pilot with a specific CSP and set of tools.	Select a volunteer CSP and Auditor, working in cooperation with CSA.	First CABC "third-party certification" entry	**To be started**
	Full scale CABC "Self-assessment" pilot with a specific CSP and set of tools.	Select a volunteer CSP and Auditor, working in cooperation with CSA.	First CABC "Self-assessment" entry	**To be started**
	Establish accreditation and train certified bodies for CABC.	Create an accreditation program. Create a training program.	The existence of at least 1 accredited Certified Bodies with a presence in EMEA, North America and APC.	**To be started**

1.5.4 EXPLOITATION PLAN FOR CSA GDPR CODE OF CONDUCT AND CERTIFICATION FOR GDPR COMPLIANCE

Table 4: Detailed exploitation plan CSA for CSA GDPR Code of Conduct and Certification for GDPR Compliance

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6	Seek for the approval of the European Data Protection	Work with National DPAs (the French CNIL and the	Approval from the EDPB.	**Running**

month) after the project	Board (EDPB) for the CSA Code of Conduct for GDPR Compliance based on the requirement	Italian Garante Privacy in particular) at the review of the current version of the CoC		
	Translation of the CSA CoC in several EU languages.	Use partner for the translation and publish the draft version for peer review. Engaging CSA National Chapters. Biweekly working sessions.	Final translation	**Running**
	Embed the CSA CoC for the GDPR Compliance into third party solution providers product to facilitate adoption.	Work with CSA corporate members to identify security and privacy tools providers interested in leveraging the template of the GDPR CoC.	At least one vendor using the CSA GDPR CoC.	**Running**
	Definition of the CSA GDPR Certification	Working within the OCF WG to define the final certification scheme in accordance with the Article 42 requirements and EDPB Guidelines	Final GDPR Certification scheme published	**Running**
	Submission of the GDPR Certification scheme to the relevant DPAs	Leverage connection already established for the review of the GDPR CoC	Approval of the CSA GDPR Certification scheme by the EDPB	**Running**
	Launch of the CSA GDPR	Create the training course	Training launched and	**Running**

	CoC and Certification Lead Auditor and Consultant training	and establish a go-to-market strategy	strategy in place	
Market Evaluation phase: During 2 years after the project	Implement the GDPR Code of Conduct and Certification go-to-market strategy	Engage with the CSA community and other relevant stakeholders in ensure that awareness and adoption are maximised	Achieve at least 100 submissions within 12 months from the approval of the CSA Code of Conduct and/or Certification by the EDPB	**To be started**
	Implement the GDPR Code of Conduct and Certification go-to-market strategy	Engage with the auditor and consultant community to maximise the uptake of the CSA GDPR training	Train at least 100 auditor and consultant before the end of 2020	**To be started**
	Create a sustainable approach to the implementation of the internal monitoring body	Establish an internal monitoring body to oversee the implementation of the CSA Code of Conduct and Certification	Establish an internal monitoring body	**Running**
	Extend the scope of the PLA Code of Practice to cover the requirements of GDPR Article 46 on international data transfer	Extend the scope of the CSA Privacy Level Agreement (PLA) WG	New version of the PLA Code of Practice	**Running**
	Extend the scope of the PLA	Extend the scope of the CSA	New version of the PLA	**Running**

	Code of Practice to cover the requirements from other relevant data protection regulation around the world so to create a tool for global privacy compliance. transfer	Privacy Level Agreement (PLA) WG	Code of Practice	

1.5.5 EXPLOITATION PLAN FOR MPRF

Table 5: Detailed exploitation plan CSA for MPRF

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	Include the results of the MPRF into the European Certification scheme that ENISA will create in the context of the EU Cybersecurity Act.	Participate in the Ad hoc expert group established by ENISA	MPRF results (repository of controls and governance framework partially leveraged by ENISA	**Running**

Market Evaluation phase: During 2 years after the project	Seek for the approval of the US General Services Administration (GSA) for the mutual recognition between CSA STAR and FedRAMP Moderate	Run a real-life pilot with 4 different FedRAMP Moderate compliant cloud services.	Approval from US GSA.	**Running**

1.6 CAIXA BANK

CaixaBank, as a Cloud Service Customer in a highly regulated sector such as the banking sector, aims at relying on Cloud services continuously certified. Therefore, considering the positive evaluation of the approach deployed in EU-SEC, CaixaBank plans to continue providing support in the following steps given by the rest of EU-SEC partners for the commercial exploitation and widespread uptake of the solution. The adoption of Cloud Services is becoming a fundamental step to achieve a truly digital transformation of any business and assure security and compliance requirements is one if not the most important challenge because the traditional ways to certify and audit services are not working for Cloud Services. In the Cloud paradigm the point in time audit or certification is not enough, a continuous certification is necessary to assure reliability of strategic assets now outside our infrastructure and owned by a third party.

1.6.1 CABC BASED EXPLOITATION

The pilot has demonstrated a promising approach for enhancing the control of the CSPs in very sensitive sectors, having a more exhaustive and automated control of privacy and security features while migrating services to the cloud. Aligned with the recently released (7th June 2019) *CSP CERT WG Recommendations for the implementation of the CSP Certification scheme,* which included that, "*considering the ever-evolving threat landscape for cloud services, a continuous certification process (which may include a continuous monitoring component) should be adopted as part of the requirements for a substantial and high certification.*", CaixaBank plans to be an early adopter of cloud services Continuous Certification, pushing their cloud providers to be certified by such certification methodology. To that end, the plan of CaixaBank consist on establish a strong collaboration with CSA as financial sector advisor for the definition of the Continuous Certification, continue dissemination (internally and externally) for the adoption of CABC type of approaches, and deploy further proof-of-concept pilots with other CSPs and cloud services which CaixaBank is already working with.

The pilot is also focusing on protecting information exchange, through a Cloud Service. In CaixaBank we have several examples of this use case, such as information exchange with Regulators, Providers, Auditors, or other Financial institutions, Caixabank will propose to these third parties the use of the outcome of the EUSEC pilot.

1.6.2 EXPLOITATION PLAN CAIXA BANK

Table 6: Detailed exploitation plan CAIXA Bank

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Raising awareness on conferences and workshops. 2. Spread and announce the innovation and its potential. 3. Increase acceptance at the industry and open source community.	Participation in industrial or academic conferences, workshops and fairs.	Publication and adoption at conferences and workshops.	**Success** (ETSI Security Week, FS-ISAC) **Running** (more tutorials on conferences and workshops)
	4. Evaluate CABC concept and potential adoption	Definition of the CABC framework	CABC framework defined	**Success** (Framework defined)
	5. Identify the business value CABC as a cloud customer	Creating a Business Model Canvas for CABC.	Business canvas validated	**Success** (Canvas created)
	6. Evaluate EU-SEC CABC reference architecture	Pilot definition, deployment and evaluation of the different tools and the architecture as a whole	CABC pilot demo and evaluation completed	**Success** (CABC pilot successfully evaluated)
	7. Acquisition of future projects for extending	Application for H2020 and	Project application is	**Running** (CaixaBank applies for several H2020 projects

	and specializing the CABC concept.	national follow up programs	successful	related to cyber security e.g. CONCORDIA)
Market Evaluation phase: During 2 years after the project	1. Establishing a customer CABC community	Contacting potential customers in the critical cloud domain for exchanging experiences.	Customer are interested in certification services	**To be started**
	2. Raising awareness on conferences and workshops. 3. Spread and announce the innovation and its potential. 4. Increase acceptance at the industry and open source community.	Participation in industrial or academic conferences, workshops and fairs.	Publication and adoption at conferences and workshops.	**To be started** (more tutorials on conferences and workshops)
	5. Acquisition of future projects for extending and specializing the CABC concept.	Application for H2020 and national follow up programs	Project application is successful	**To be started** (CaixaBank applies for several H2020 projects related to cyber security e.g. CONCORDIA)
	6. Evaluate further proof-of-concept pilots with other CSPs and cloud services which CaixaBank is already working with.	Deploy new pilots with existing cloud services.	Successful evaluation of the pilots.	**To be started**

Market Establishing phase: During 4 years after the project	1.	Widespread adoption of Continuous Certification of cloud services in CaixaBank.	Set up the continuous certification process for any cloud service in CaixaBank.	Continuous certification running in several cloud critical services in CaixaBank	**To be started**

1.7 SIXSQ

SixSq is an SME that provides neutral solutions allowing companies and institutions to benefit from cloud and edge computing while avoiding lock-in. Its smart solution-in-a-box appliance, NuvlaBox, is a simple plug & play edge solution which brings customers a private infrastructure at an affordable price as well as playing an intrinsic part of smart city and IoT strategies. SixSq's smart multi-cloud and edge management platform, Nuvla, offers application deployment from a single, simple dashboard. In context of EU-SEC, CABC shows business potential to further develop and extend SixSq's Nuvla service in providing more transparency and better compute infrastructure profiling.

1.7.1 CABC-BASED EXPLOITATION

Nuvla has been extended to support the management of raw continuous auditing evidence, by allowing the tools involved in the Continuous Auditing process to ingest the raw evidence records into Nuvla, as JSON documents, via a REST API. These tools are mapped into Nuvla users, which can also programmatically manage these evidence records once they have been registered in Nuvla. Apart from the standard CRUD operations, the evidence record managers can also make these available for other Nuvla users (and even anonymous users), with very fine-grained access control policies.

This functionality could potentially lead to the implementation of new features in Nuvla, that would allow its users to automatically and dynamically be assigned to the best fitting CSP, based on their user criteria and application requirements.

1.7.2 EXPLOITATION PLAN SIXSQ

Table 7: Detailed exploitation plan SixSQ

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	Engage with 3rd party continuous auditing tools (like Clouditor) in order to establish a communication protocol between those tools and Nuvla's REST API	Through the partners involved in the EU-SEC project	Add Nuvla API support to the chosen tools	**Success** (Clouditor can publish its results to Nuvla)
	Run scale tests to confirm that the 3rd party tools being used match well with the evidence management schemes defined in Nuvla	Through pilot projects	Be able to automatically generate evidence and publish it into Nuvla	**Success** (through the CABC pilot in EU-SEC)
Market Evaluation phase: During 2 years after the project	Continue engaging and researching 3rd party tools that are capable of doing continuous security audits/checks	Research and involvement in other cybersecurity projects	Identification of additional tools that serve the purpose and can be integrated with Nuvla	**To be started**
	Integrate more of these tools with Nuvla	Through internal development at SixSq or collaboration with the	Full integration with Nuvla	**To be started**

		institution providing the 3rd party tool		
	Announce this Nuvla capability to the market	Create dissemination material through SixSq's website and documentation	Have the dissemination material in place and proof of interest from SixSq's users	**To be started**
	Implement data analysis algorithms to give users relevant information about Nuvla	Through internal development at SixSq or collaboration with the data analysis experts	Have a working functionality in Nuvla that provides user-friendly information about the security status of an infrastructure and advises on the best ones to use	**To be started**

1.8 FABASOFT

Fabasoft is a European software manufacturer and cloud provider. The software products and cloud services from Fabasoft ensure the consistent capture, sorting, process-oriented handling, secure storage and context-sensitive finding of all digital business documents. These functions are used in both on-premises installations in customer data processing centres, as well as in SaaS and cloud services. The Fabasoft eGov-Suite, which was developed in this manner, is the leading application for electronic records management in the public sector within the German-speaking region. Regarding the cloud strategy to foster trust in this important technology and in the light of EU initiatives like CSP-Cert and the DSM, Fabasoft undertakes great efforts to take a pioneering role for their customers in the fields of cybersecurity, privacy and trust. Therefore, the two approaches, MPRF and CABC, yield valuable results, to streamline the current audit processes and to aim for more efficiency and transparency.

1.8.1 MPRF BASED EXPLOITATION

The shear potential to streamline certification and attestation efforts, given by the MPRF approach is something that caught Fabasoft's attention in the first place and led to the project participation. The results from the pilot phase of WP4 and the Requirements Repository are directly exploitable, as Fabasoft, holding a BSI C5 Type 2 attestation, uses them to aim for a SOC 2 attestation for English speaking regions.

1.8.2 CABC BASED EXPLOITATION

Fabasoft will use the results of the continuous audit pilot (WP5), to build an internal control assurance approach. This will be done by using the current available tools like *app.telemetry*[1] and the proof of concept, provided by the pilot and the established EU-SEC Audit-API specification. A first approach will be built around requirements of the BSI C5 scheme and aim to satisfy the requirements of the EU cybersecurity act with the level "high".

[1] https://www.fabasoft.com/en/products/fabasoft-apptelemetry

1.8.3 EXPLOITATION PLAN FABASOFT

Table 8: Detailed exploitation plan Fabasoft

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Streamline compliance activities within Fabasoft for multiple certification / attestation 2. Extend (internal) Control Matrix 3. Establish process for compliance prog. Extension	Directly apply the EU-SEC results to the internal processes and materials.	Sub-steps 1 – 3 successful	**Running**
	Identify the business values of MPRF and CABC	Creating a Business Model Canvas for MPRF & CABC	Business canvas created	**Success** (Canvas created)
	Apply the WP4 pilot findings to new compliance schemes within the Fabasoft group	Select at least one additional new compliance scheme (e.g., SOC2) and in the process apply (at least partially) the MPRF Framework.	Effort for new attestation significantly reduced.	**Running**
	Evaluate the Requirements Repository and verify / extend the internal Control Matrix.			**To be started**

Market Evaluation phase: During 2 years after the project	1. Further explore and develop the EU-SEC concept 2. Map the current Audit API findings to internal monitoring processes	R&D activities	Sub-steps 1 – 2 successful	**Running**
	Participate in funded projects to further develop the EU-SEC CABC proof of concept.	Identify calls and consortia	Active consortium member of a funded project in Austria, Germany or Europe.	**Running**
	Extend the EU-SEC proof of concept by working on the Audit API from a BSI C5 point of view.	Formalize selected BSI C5 requirements according to the EU-SEC Audit API. Implement these requirements in the Fabasoft VDE.		**To be started**

1.9 SI-MPA

One of the main responsibilities of the Slovenian Ministry of Public Administration (SI MPA) is the maintenance of the state-owned private communication network, maintenance of horizontal IT systems and providing support to the development of electronic services for civil servants, citizens and the business entities. By December 2015, SI MPA has built the Slovenian Government Cloud (SGC) to support a new way of delivering IT services. New infrastructure was put in place and the software layers for setting up IaaS, PaaS and SaaS services were designed and successfully implemented. The traditional IT solutions are slowly being migrated to the SSC infrastructure. The goal is not only to migrate the existing applications, but also to transform them into proper cloud services (SaaS). Regarding the use of the new IT infrastructure and transition to the cloud services as new business model, information security, privacy and trust are an increasingly pressing topic which must be addressed in systematic way. Last but not least, frequent information security and privacy revisions of the SGC, hosting the sector-specific applications of public authorities, is required by them. The use of different audit standards and certification methods requires a lot of efforts and resources, which is becoming increasingly challenging for SI MPA.

Participating on the project EU SEC gives SI MPA opportunity to reduce the audit efforts and resources. The exploitation plans are based on the two innovations multi-party recognition framework as well as the continuous auditing-based certification. The EU-SEC project has developed a model architecture which aims to tackle the certification schemes' proliferation side effects to benefit all cloud-based stakeholders. The method which was developed to achieve this goal, multiparty recognition, and is realized as a well-defined layered architecture called: the multiparty recognition framework (MPRF), will be the SI MPA main dissemination or / and exploitation focus.

1.9.1 MPRF BASED EXPLOITATION

SI MPA will exploit the EU SEC MPRF for further development of the EU-SEC Requirements and Controls Repository, which is internally developed by SI MPA in Oracle APEX environment. Further extension of EU-SEC Requirements and Controls Repository will be done by inclusion of security requirements defined in the Decree on information security in the State

Administration[2], which came into force in 2018. Increasing the efficiency and effectiveness of the audit process will be facilitated by designing of compliance evidence repository, which must be confidential. This repository should be used by the auditors from different auditing companies.

Linked to development of MPRF as the main part of simplifying the certification process of cloud services, SI MPA has presented EU-SEC project at any occasion were possible to disseminate the project's activities and results, which will stay the permanent task of the ministry, and will gradually progress into recognized center for increasing awareness, improving understanding and building confidence concerning cloud services and MPRF.

1.9.2 CABC BASED EXPLOITATION

CABC provides assurance based on continuous auditing. This requires the knowledge of breaking down certification goals in to measurable artefacts. As the SI MPA is not classical CSP on the market, the SGC users are in trusted environment, connected with state-owned private communication network, the CACB innovation is not in the SI MPA main dissemination or / and exploitation focus. However, SI MPA will monitor further development of CACB within other EU SEC participants and broader.

[2] Decree on information security in the State Administration

1.9.3 EXPLOITATION PLAN SI-MPA

Table 9: Detailed exploitation plan SI-MPA

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Presenting the MPRF and EU-SEC framework to the respectable audience	Participation on industrial, government and academic conferences, workshops and fairs	Monitor the audience response and collecting feedback	**Running**
	2. Raising awareness and acceptance of MPFR in real audits	Presenting the MPRF to the internal auditors from SI-MPA and to state institutions, like Budget Supervision Office and Court of audit.	Level of acceptance of MPRF in audit process to SGC.	**Planned**
	3. Monitoring the development of the MPRF in terms of implementation of other stakeholders (industry, academia, etc.) for simpler use of EU SEC repository	Tracking the EU SEC web page, social media, academic articles, participation of new stakeholders.	Numbers of stakeholders involved	**Planned**
	4. Further development of EU-SEC requirements and controls repository	Development of SI-MPA internal application EU-SEC Requirements and Controls	Application deployed in production environment	**Planned**

		Repository based on Oracle APEX		
Market Evaluation phase: During 2 years after the project	1. Establishing the base for increasing awareness, improving understanding and building confidence concerning cloud services and MPRF	Improvement of the MPRF and internal application based on cloud providers and customer experience.	Cloud providers and customers feedback	**Planned**
	2. Extend the EU SEC Requirements and Controls repository	The inclusion of security requirements defined in the Decree on information security in the State Administration	Extended EU SEC Requirements and Controls repository	**Planned**
Market Establishing phase: During 4 years after the project	1. Make audits easier and more efficient	Designing the compliance evidence repository of confidential nature as input for auditors from Budget Supervision Office, Court of audit and other Slovene auditing companies	Number of auditors which will use the MPRF	**Planned**

1.10 MFSR

MFSR is one of the founding organization who built the government cloud in Slovakia. Our cloud consists of 2 separate areas. One is Private cloud which is provided by the Ministry of interior of the Slovak Republic, and second is the hybrid/commercial environment. The basis of the hybrid environment is a catalogue of services. Services which are signed in the catalogue of services are proved by Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization (from now on "UPVII"), and government bodies and institutions are eligible to use only cloud services signed in the catalogue of services.

Participating in the project allows us to bring more quality for proving services in entering phase for CSPs services. The method which was developed to achieve this goal, multiparty recognition, and realized as a well-defined layered architecture called: The multiparty recognition framework (MPRF), will be used by UPVII and MFSR with primary dissemination or/and exploitation focus.

1.10.1 MPRF BASED EXPLOITATION

The MFSR, in cooperation with UPVII, has developed a separate set of questions to assess the maturity of service in a hybrid environment. Based on the results of the EU-SEC project, we have created a mechanism to recognize other publisher certificates to speed up the process of procuring cloud services.

The project outputs significantly helped us to progress the whole creating process of introducing a hybrid cloud in the Slovak government cloud environment. More than 40 external CSP services are currently included in the catalogue[3], and approximately 50 other services are accredited.

1.10.2 CABC BASED EXPLOITATION

By definition, the CABC assumes that it is a tool for auditors to more effectively audit individual services. For the needs of government cloud, we think that when individual CSPs provide

[3]https://www.vicepremier.gov.sk/sekcie/informatizacia/egovernment/vladny-cloud/katalog-cloudovych-sluzieb/index.html

sufficient evidence for monitoring, we will include certificate monitoring in the management of hybrid cloud services. However, MFSR will monitor further development of CACB within other EU SEC participants and broader.

1.10.3 EXPLOITATION PLAN MFSR

Table 10: Detailed exploitation plan MFSR

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Raising awareness and acceptance of MPRF	Participation on industrial, government or academic conferences, workshops and fairs	Monitor the audience response and collecting feedback	**Running**
Market Evaluation phase: During 2 years after the project	1. Establishing the base for increasing awareness, improving understanding and building confidence concerning cloud services and MPRF	Improvement of the MPRF and internal application based on cloud providers and customer experience as a part of national government hybrid environment.	Cloud providers and customers feedback	**Running**
	2. Extend the EU SEC Requirements and Controls repository	The inclusion of security requirements defined in the Decree on information security in the State Administration	Extended EU SEC Requirements and Controls repository	**Planned**

1.11 NIXU

Nixu is a cybersecurity services company helping organizations to embrace digitalization securely. Partnering with its clients, Nixu provides practical solutions for ensuring business continuity, easy access to digital services, and data protection. Besides various types of consultation services, Nixu offers information security auditing services. Nixu Certification Ltd, a subsidiary to Nixu, is an accredited certification body and provides certifications for multiple standards such as ISO/IEC 27001 and CSA STAR. By focusing only on information security auditing services, they offer one of the broadest portfolios of security audits in the Nordics such as Katakri, VAHTI, KANTA, PCI DSS, PCI PA-DSS, PCI 3DS and Mirrorlink. In context of EU-SEC, both project outcomes, MPRF and CABC, show business potential to further develop and extend Nixu's services in consultation and auditing.

1.11.1 MPRF-BASED EXPLOITATION

Nixu is interested in creating a new service based on MPRF. For auditors the benefits of MPRF are quite self-explanatory: It is a competitive advantage against "traditional" audits because the MPRF-based approach might be more tempting for CSP's. MPRF-based approach streamlines the audit process when mutual recognition of security requirements can be used to reduce the amount of audited controls. MPRF also allows the auditor to conduct a combined audit where multiple standards can be audited in a single audit by using the same evidence for equivalent requirements in different standards. In addition to auditing services, MPRF would create opportunities for consultation and training when Nixu's clients aim to take MPRF into use and require assistance to achieve their goals.

1.11.2 CABC-BASED EXPLOITATION

Continuous Auditing Based Certification is a great new addition to the traditional point-in-time audits because it enhances the auditor's ability to ensure the auditee's compliance to standards throughout the certification life cycle. CABC allows Nixu to provide auditing more as a continuous service which is in line with Nixu's strategic goals. This service would extend the existing service portfolio and would create a more involved and closer relationship with auditees, which would help Nixu to gain a better position in the market. Like in MPRF, there is need for both auditing and consultation services.

1.11.3 EXPLOITATION PLAN NIXU

Table 11: Detailed exploitation plan NIXU

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	Identify the business value of MPRF and CABC for auditors	Create a business model canvas for MPRF and CABC	Business model canvas validated	**Running**
		Define auditing and consultation services utilizing MPRF	Service concepts ready to be piloted	
	Define and finalize business cases for both innovations	Define auditing and consultation services utilizing CABC and prepare pilot implementation		
Market Evaluation phase: During 1 year after the project	Gather a potential customer base for all services	Contact potential customers and spread awareness of new services	Initial customer base for each service identified and established	**To be started**
		Arrange a service pilot with potential customers	Service pilots finished for all services	
	Pilot all services with potential customers			
Market Establishing phase: During 2 years after the project	Establish MPRF-based auditing service	Service concepts updated based on pilot feedback	Market interest in all four services (growth potential)	**To be started**
	Establish MPRF-based	Services up and running	First client assignments of	

	consultation service	each service running
	Establish CABC-based auditing service	
	Establish CABC-based consultation service	

1.12 PWC GERMANY

When it comes to auditing and advisory, PwC supports clients of all industry fields to reach their goals. We advise corporations as well as family-owned companies, industry- and service companies, global players and local heroes, the public sector, organisations and NGOs. With our know-how and our expertise, around 600 partners and nearly 12,000 experts in 21 locations in Germany support our clients in terms of finding solutions for complex questions in a world changing rapidly – in line with our purpose statement "Build trust in society, solve important problems".

The exploitation plans are based on the two innovations multi-party recognition framework as well as the continuous auditing-based certification. For us and our clients, these topics are of high importance as they can drive the quality and sustainability of compliance.

1.12.1 MPRF BASED EXPLOITATION

PwC plans to leverage the MPRF concept in consulting and certification/attestation engagements. This will support our clients and us to prepare and execute certification/attestation engagements more efficiently and effectively. We will deepen our understanding and expertise over time and strive to work on real-world MPRF projects and respective proof of concepts and implementations.

1.12.2 CABC BASED EXPLOITATION

The CABC concept stands for increasing the efficiency and reliability of automated compliance testing. PwC plans to work on the testing-related requirements as well as the processes and procedures in order to design these in a way that they provide the basis for building continuous trust. Like MPRF, CABC will be a future enabler for increasing the compliance processes' efficiency as well as effectiveness and a building block for generating trust in Cloud.

1.12.3 EXPLOITATION PLAN PWC GERMANY

Table 12: Detailed exploitation plan PWC Germany

WHEN	WHAT (GOALS)	HOW (ACTIONS)	SUCCESS CRITERIA	CURRENT STATUS
Market Initiation phase: During project or shortly (6 month) after the project	1. Define a viable product (Audit API, Methodology, consulting and development services, CABC package) and its business requirements 2. Spread and announce the innovation and its potential 3. Get community involved in specification and development	R&D activities Improvement of the technology on the basis of the EU-SEC use cases and pilots. Launch as an open source project (see detailed actions in columns below)	Getting contributions from the open source community	**Running**
	On 1: Establish a vision and high-level plan of how the CABC can be established	Create a Roadmap incl. possible applications of CABC in the community	Roadmap developed	**To be started**
	On 2: Raise awareness for and acceptance of CABC in the Cloud community	Explain CABC in client conversations and on conferences/workshops as well as similar occasions	Increased awareness	**To be started**

	On 3: Demonstrate that CABC can be implemented and will deliver added value	Realise proof of concept for CABC	PoC has been implemented and results have been analysed	**To be started**
Market Evaluation phase: During 2 years after the project	1. Establishing a customer base for consultancy in the (continuous) certification market 2. Establishing an active open source community around the Audit API 3. Achieving TR-Level 6 for the Audi API	R&D activities Improvement of the technology on the basis of customer experiments. Acquisition of additional funding. Acquisition of customers for continuous based auditing. Active open source development of the Audit API. (see detailed actions in columns below)	Reaching TR-Level 6 for the Audit API An initial customer base for consultancy in the (continuous) certification market has been established. Managing the development of the Audit API. (see detailed criteria in columns below)	**To be started**
	On 1: Build a community of CABC users	R&D activities incl. feasibility test with CABC users	An initial user base for CABC	**To be started**

	On 2: no action planned	n/a	n/a	**n/a**
	On 3: no action planned	n/a	n/a	**n/a**
Market Establishing phase: During 4 years after the project	1. Establishing the Audit-API as stand-alone product and service	Improvement of the technology on the basis of customer relationships and internal use. Acquisition of customers for security testing as a service. Acquisition of customers for the Audit API.	A solid customer base for security testing as a service has been established. An initial customer base for the Audit API and CABC has been established.	**To be started**
	On 1: no action planned	n/a	n/a	**n/a**

2 DISSEMINATION

This section outlines the key dissemination activities across a variety of channels and includes progress against associated key performance indicators (KPIs) for year 3, as well as the three-year lifespan of the project.

2.1 SCIENTIFIC AND TECHNICAL PUBLICATIONS

The project published five articles in scientific publications and technical journal, as shown in the table below. A complete list of the of the project's publications can be found in the Annex of this document.

Table 13 Publications in 2019

Year	Author(s)	Title	Type	Journal/Conference	Place / Country	Date	Published in	Publisher
2019	Martin Labaj, Karol Rástočný, Daniela Chudá	Towards Automatic Comparison of Cloud Service Security Certifications	PRP	SOFSEM 2019: 45th International Conference on Current Trends in Theory and Practice of Computer Science	Slovak Republic, Nový Smokovec, A trium Hotel	01/27-30/2019	Conference proceedings	Springer
2019	Anton Ujčič, Damir Savanović	Okvir medsebojnega priznavanja EU-SEC / EU-SEC Multiparty Recognition Framework	J	27th International Conference on Information Systems Auditing and Control	Kranjska gora, Slovenia	24.9.-25.9.2019	SIR*IUS 5/2019	Slovenian auditors institute
2019	Jürgen Großmann, Dorian Knoblauch	Neue Wege in der IT-Sicherheitszertifizierung von Cloud Infrastrukturen	J	Objektspektrum: Online-Themenspecial zum Thema "Cloud Computing - Dynamische IT- Leistung aus der Wolke"	Deutschland	June 2019	Objektspektrum: Online-Themenspecial zum Thema "Cloud Computing - Dynamische IT-Leistung aus der Wolke"	SIGS Datacom
2019	Dorian Knoblauch, Jürgen Großmann, Linda Strick, Alain Pannetrat	Europäisches Rahmenwerk für Continuous Auditing based Certification	PRP		Germany		Tagungsband zum 16. Deutschen IT-Sicherheitskongress, ISBN: 978-3-922746-82-9	SecuMedia Verlag
2019	Dorian Knoblauch & Jim de Haas	Cloud Provider Continuous Assurance: EU SEC Framework for Continuous Assurance in the Cloud	J	ISSA Journal Oct 2019	Netherlands	Okt 19	Issa Journal October 2019 Volume 17 Issue 10	ISSA
2019	André Koot	EU-SEC helpt auditors	J	de IT-Auditor	Netherlands	Sep 10	IT Auditor 2-2019	NOREA

2.2 DISSEMINATION AND COMMUNICATION ACTIVITIES

2.2.1 PROJECT WEBSITE

The website has acted as one of the central dissemination channels and sources of information for the project. In May 2019, the design of the website was updated to improve the message regarding the objectives and benefits of the project's innovations. This resulted in a significant improvement in the website visits, with 4,150 visits in 2019 and 450 resource downloads.

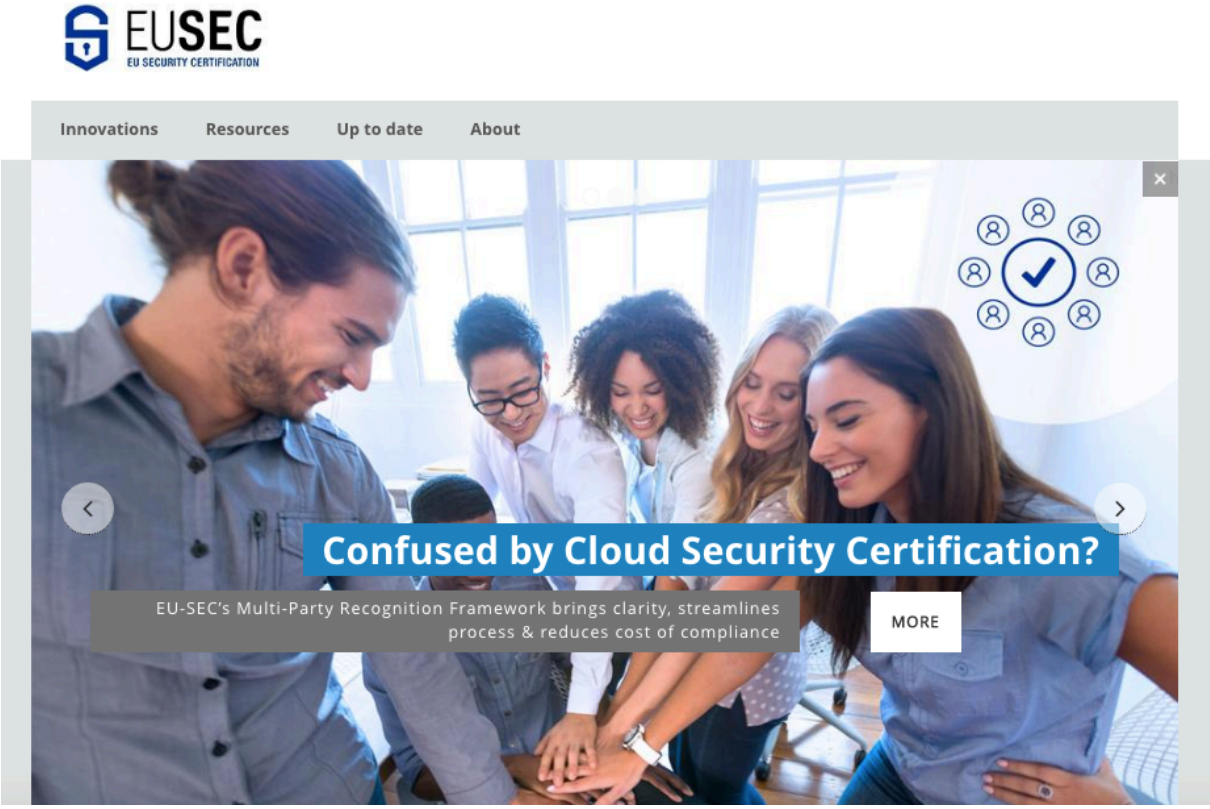


Figure 7: Snapshot from the EU-SEC website

The site is updated on a regular basis with news, deliverables, and events. It features an overview of the project's three innovations, information about the partners, a section for news, workshops and events, and the following set of downloadable resources:

- How to documents
- Slide decks
- White papers

- Deliverables
- Papers & publications
- Newsletters

Website traffic was monitored by Fraunhofer FOKUS. Most people who visited the site went to the home page and the news section. The website will be maintained for at least two years after the end of the project to ensure the ongoing transfer of knowledge and results.

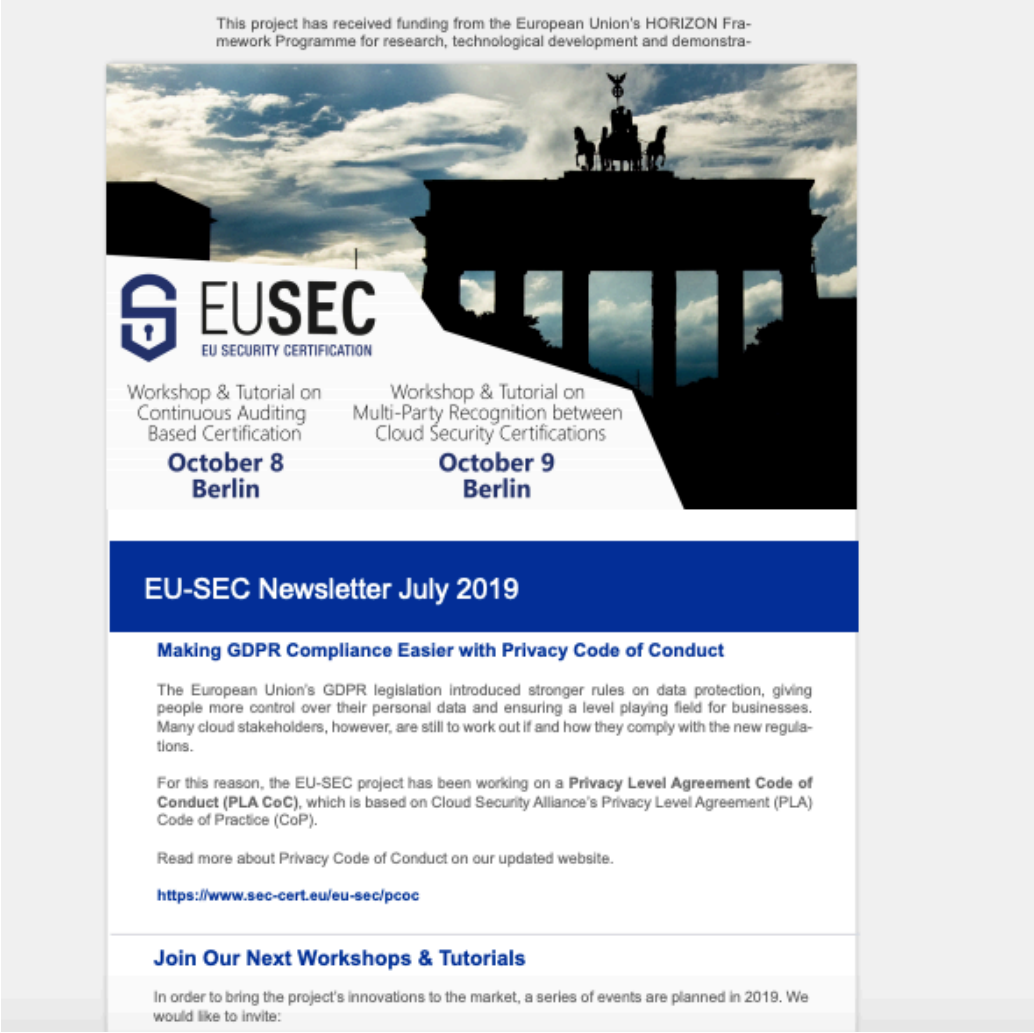
2.2.2 NEWS ITEMS

The project published 16 news items on the website [4]in 2019, covering mainly events attended by partners and publicising the workshops and training events. By disseminating the news items via the social media accounts, they provided a way to drive traffic to the site and raise awareness of the project's innovations.

2.2.3 NEWSLETTERS

Four newsletters were published in 2019. The idea was to bring together the latest activities and provide a digest to email to registered subscribers, as well as be available for website visitors.

[4] https://www.sec-cert.eu/eu-sec/news


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstra-

EUSEC
EU SECURITY CERTIFICATION

Workshop & Tutorial on Continuous Auditing Based Certification
October 8
Berlin

Workshop & Tutorial on Multi-Party Recognition between Cloud Security Certifications
October 9
Berlin

EU-SEC Newsletter July 2019

Making GDPR Compliance Easier with Privacy Code of Conduct

The European Union's GDPR legislation introduced stronger rules on data protection, giving people more control over their personal data and ensuring a level playing field for businesses. Many cloud stakeholders, however, are still to work out if and how they comply with the new regulations.

For this reason, the EU-SEC project has been working on a **Privacy Level Agreement Code of Conduct (PLA CoC)**, which is based on Cloud Security Alliance's Privacy Level Agreement (PLA) Code of Practice (CoP).

Read more about Privacy Code of Conduct on our updated website.

https://www.sec-cert.eu/eu-sec/pcoc

Join Our Next Workshops & Tutorials

In order to bring the project's innovations to the market, a series of events are planned in 2019. We would like to invite:

Figure 8: Snapshot from 5th Newsletter

2.2.4 HOW-TO DOCUMENTS & TRAINING PACKAGES

In support of the training and awareness workshops, the partners developed comprehensive how-to guidelines[5]:

- Implementing Continuous Audit-Based Certification
- Implementing Multi-Party Recognition for Cloud Security Certifications

The guidelines include sections targeted at specific audiences including standard owners, cloud service providers, auditors and auditees and provide a convenient handbook for anyone

[5] https://www.sec-cert.eu/how-to-documents-e935cc5175e0fa0d

wishing to implement the project's innovations.

In addition, the project has published a full set of resources for each innovation in package[6] form, bringing together all relevant documentation in one place to facilitate the uptake of the project outcomes.

2.2.5 VIDEOS

In order to make the results accessible to a wider audience, 5 videos[7] have been produced which showcase the main aims and benefits of Continuous Audit-Based Certification and the Multi-Party Recognition Framework. The videos gave the partners chance to present the results in a storytelling format and reach a wider audience.

2.2.6 WORKSHOPS & WEBINARS

As stated in the D6.4 training and awareness plan, the project organised one awareness workshop and two training workshops in 2019. The workshops and training sessions were supported by the presentation material and practical how-to guidelines referred to in section 3.2.5. To ensure the sustainability of the results beyond the end of EU-SEC, the materials have been made available online.

In addition, a webinar [8]about the Multi-Party Recognition Framework was published on BrightTalk in May 2019.

2.2.7 EVENT PARTICIPATION

In a continued effort to raise awareness of the project's results, EU-SEC partners presented the project at a significant number of industry and research events, as shown in the following table. A complete list of all attended workshops and conferences can be found in the Annex of this document.

[6] https://www.sec-cert.eu/cabc-training-and-awareness-package-3944d470f60a5ae5

[7] https://www.sec-cert.eu/videos-fbb262b58aaf62e7

[8]https://www.brighttalk.com/webcast/16947/358154?utm_campaign=viewing-history&utm_source=brighttalk-portal&utm_medium=web

Table 14: List of attended events

Date	Location	Name of conference/workshop/event	Contributing partner	Form of the contribution	Title
27-30.01.19	Nový Smokovec, Slovak Republic	SOFSEM 2019: 45th International Conference on Current Trends in Theory and Practice of Computer Science	MFSR	Paper & presentation	Towards Automatic Comparison of Cloud Service Security Certifications
10.01.19	Aalto University, Helsinki, Finalnd		Nixu	Presentation	EU-SEC EU Security Certification presentation
15.01.19	Amsterdam, Netherlands	CSA Netherlands Cloud Journey Event	Nixu	Presentation	EU-SEC EU Security Certification presentation
04-08.03.19	San Francisco, USA	RSA Conference	CSA	Presentation	CSA Star: The leading cloud trust & accountability program
12-14.03.19	Milan, Italy	Cloud Security Summit	CSA	Presentation	CSA Star: The leading cloud trust & accountability program
12-14.06.19	Capri, Italy	28th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative	Fraunhofer	Presentation	Reducing implementation efforts in continuous auditing

		Enterprises (WETICE-2019)			certification via an Audit API
21-23.05.19	Bonn, Germany	16th BSI German IT Security Congress	Fraunhofer	Presentation	Europäisches Rahmenwerk für Continuous Auditing based Certification
04.06.19	Brussels, Belgium	Cyberwatching.eu concertation meeting	Fraunhofer	Presentation	Standards and Certification for Cybersecurity
17-21.06.19	Aarhus, Denmark	IoT Week 2019	Fraunhofer	Presentation, panel discussion	5G, IoT and End-to-End Security
01.05.19	Bratislava, Slovakia	Slovak Government IT conference	MFSR	Presentation	Onboarding Cloud Services with MPRF approach
09.05.19	Vienna, Austria	European Cyber Crime and Fraud Investigators Conference (ECCFI)	Nixu	Presentation	True stories of cyber-crime and insight on how to prevent
13.05.19	Amsterdam, Netherlands	Cyber Security Conference	Nixu	Presentation	
23-27.06.19	Tel Aviv, Israel	Cyber Week	CSA	Presentation	Trust in Cloud by Certification
21.06.19	Sophia Antipolis,	ETSI Security Week 2019	Fraunhofer	Presentation	Continuous Auditing Certification

	France				
21.06.19	Sophia Antipolis, France	ETSI Security Week 2019	CSA	Panel discussion	Panel discussion on Cyber Security Act & policy actions
28.08.19	Tallinn, Estonia	Nixucon19 security conference	Nixu	Presentation	EU-SEC: What's in it for us?
19.09.19	Helsinki, Finland	EU ICT proposers day	Nixu	Booth presence	Dissemination, networking at EU ICT proposers day, Helsinki
24. – 25. 9. 2019	Kranjska Gora, Slovenia	27th International Conference on Auditing and Information Systems Controls	SIMPA & CSA	Presentation and e-publication	EU-SEC Multiparty Recognition Framework
26.09.19	Helsinki, Finland	NGI Conference	Nixu	Booth presence	NGI Conference
9-10.10.19	Berlin, Germany	Automotive Cyber Security 2019	Fraunhofer FOKUS	Presentation	Security Certification for Future Automotive Cloud Architectures
12.11.19	Bratislava, Slovakia	ITAPA 2019	CSA	Presentation	The impact of EU Security Act on Cloud Computing
13.11.19	Warsaw, Poland	Advanced Threat Summit 2019	CSA	Presentation	The impact of EU Cyber-Security Act on Cloud

18-19.11.19	Brussels, Belgium	2019 International Conference on EU Cybersecurity Act	CSA	Presentation	The EU-SEC Framework
18-21.11.19	Berlin, Germany	CSA EMEA Congress 2019	CSA	Presentation	Trust in Cloud Certification

2.2.8 SOCIAL MEDIA

The social media strategy was designed to deliver visibility and engagement for the project, communicate key outputs from the project, and to leverage the pre-existing social network accounts of EU-SEC partners. Twitter and LinkedIn were selected as the most appropriate channels for the project. The Twitter account was launched in August 2017 and had 427 followers at 19 December 2019. It has been particularly effective in promoting the EU-SEC workshops, and has resulted in collaboration with other similar H2020 projects. For example, a connection made with Cyberwatching.eu resulted in EU-SEC being featured in their project hub and promoted as Project of the Week[9]. Cyberwatching.eu is developing a single gateway to innovative and trustworthy ICT products, services and software and provides another window of exposure for EU-SEC.

Figure 9: Snapshot of Twitter statistics for June 2019

The LinkedIn[10] account has 137 followers. This page has been effective in attracting views from members in the IT industry and driving visitors to the website.

[9] https://cyberwatching.eu/projects/1046/eu-sec/news-events/project-week-eu-sec

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

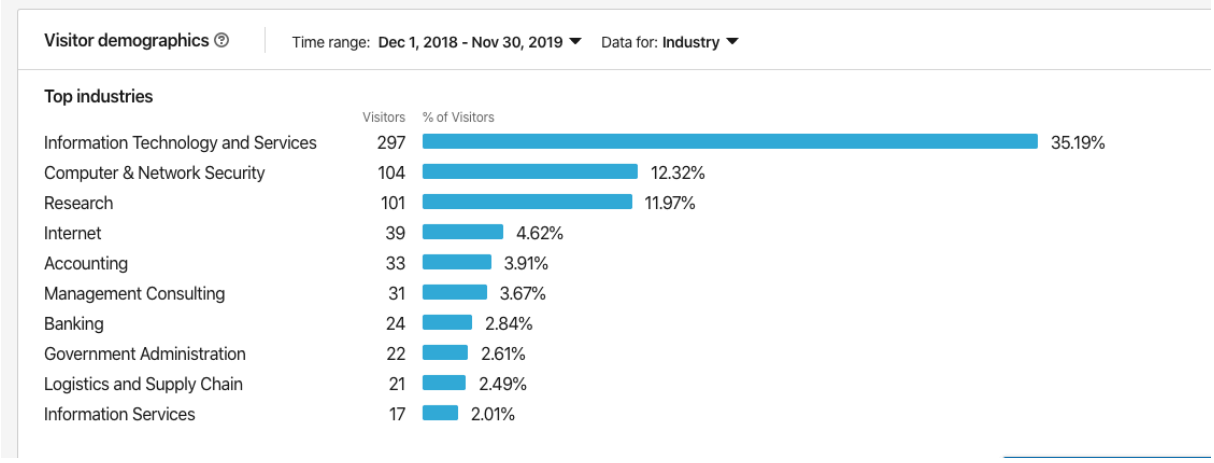


Figure 10: LinkedIn visitor demographics by industry over 12 months

2.3 KEY PERFORMANCE INDICATORS

The following table shows progress against the KPIs defined at the beginning of the project for 2019 and the total project duration.

Table 15: Achievement against KPIs

Area of impact	Description	KPI	Achieved to 2019	Achieved total project duration
Visibility of the project	Number of website visitors per year	1500	4,150	10,999
	Number of press release/website news issued per year	4	11	23
	Number of domain exhibitions per year	>5	6	10
	Number of project hosted external workshop (per year)	>1	4	5

	Number of external workshops/seminars etc participation	>10	0	4[11]
Knowledge impact creation	New training seminars (project duration)	>3	6	6
	Posters, flyers, exhibitions (project duration)	>5	2	6
	Number of journal publications	>5	1	5
	Number of conference papers & presentations (project duration)	>15	21	52
	Number of events attended (project duration)	50	35	50
Impact on Europe's technology leadership	Number of market consultation meetings	>6	9	13
	Number of trainings with industry/SMEs	>6	6	6
	Number of trainings with certification authorities	>3	2	2

3 STANDARDISATION

The standardisation effort within the EU-SEC project focused on:

[11] In fact, the project partners were present at a much larger number of workshops. However, as we count presentations separately, they are not listed here.

1. standards to consider within the project,
2. opportunities for providing contribution to new and ongoing standardisation activities.

The detailed approach is described in the D6.1 Dissemination and Standardisation plan (D6.1).

During the life-time of the project, we monitored the standardisation and policy landscape to identify:

1. standards that might not have been originally considered by the project,
2. new standardisation initiatives, and
3. changes in the policy, legal and regulatory requirements.

We focused specifically at the opportunities within ISO/IEC, CEN-CENELEC, ETSI, ENISA, European Commission and EDPB from the perspective of cloud assurance frameworks and technical standards for:

- process-based 3rd party audit certification schemes,
- semi-automated continuous auditing certification schemes
- GDPR compliance code of conducts.

The event with the greatest impact on the EU-SEC standardization effort has been certainly the approval of the EU Cybersecurity Act (EUCA)[12] in June 2019.

The EUCA introduces the EU wide rules for the cybersecurity certification of products, processes and services. Under the EUCA, a European cybersecurity certification scheme is envisioned as a comprehensive set of rules, technical requirements, standards and procedures, agreed at European level for the evaluation of the cybersecurity properties of a specific product, service or process. The EUCA gave ENISA a permanent mandate with current tasks, such as supporting policy development and implementation. New tasks have been added, most prominently regarding cybersecurity certification to:

- increase the transparency of cybersecurity assurance levels in information and communication technology (ICT) products, services, and processes;
- improve trust and help end users make informed choices; and
- lower costs by avoiding conflicting or overlapping national certifications.

[12] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

The other important event from the legal and regulatory standpoint with significant impact on the EU-SEC project, has been the entering into force of the GDPR and the issuing of new guidelines from the EDPB on Code of Conducts[13] and Certifications[14] for GDPR compliance.

The EUCA has created standardisation opportunities both for the MPRF and the Continuous Auditing certification approach. We first contributed to the preparatory work done by the expert group CSPCert under the auspices of the European Commission. The CSPCert had the goal to provide recommendations to ENISA for the creation of the European cloud certification scheme. Concretely, the CSPCert produced the Milestone 3 report "Recommendations for the implementation of the CSP Certification scheme"[15]

Lately, with the official mandate[16] from the EC to ENISA to focus on cloud computing certification scheme as priority, the EU-SEC consortium started to engage directly with the Agency and offer our result as contribution to the upcoming EU cybersecurity certification framework and more specifically, the cybersecurity certification for cloud services.

As ENISA was represented in the project advisory board at the beginning of the project, we had a continuous communication with the Agency throughout the course of the project. Even after they withdrew from the advisory board to avoid potential conflict of interest with their new mandate, we continued with the strategic and proactive collaboration with ENISA, which resulted in EU-SEC presenting the final results on MPRF and CABC to ENISA in recent meetings (four in December), where have received feedback that EU-SEC contribution will be important and significant for their efforts, providing them with a very good start for maintenance and mutual recognition for the EU cybersecurity certification scheme. They also believe that continuous auditing-based approach is the future of compliance, especially where high level of assurance is required. However, at this moment the market still needs to mature for them to embrace it.

From the GDPR perspective, we used the clarifications and guidance from EDPB on CoC and Certification as well as the direct feedback from the French CNIL and the Italian Garante Privacy

[13] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under-0_en

[14] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[15] https://cspcerteurope.blogspot.com/2019/06/final-public-private-recommendation-for.html

[16] https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa

for improving the PLA Code of Conduct and better align it with the GDPR Articles 40 and 41.

In order to update our understanding of existing practices and impact the future approach to certification and assurance, to feed into the development of key European initiatives regarding common cybersecurity requirements and evaluation criteria, we lunched in final quarter of the project a survey, to collect the feedback on the approach to cybersecurity certification and compliance.

More specifically, from October 31st 2019 to November 27th 2019 we conducted a survey within the context of the EUCA and the EU-SEC project, aiming at the auditors, regulators, cloud service providers and cloud users that are involved in standards.

We have received 14 opinions, out of which CSPs represented 43 percent, Auditors 29 percent, Standards owners 21 percent and cloud users 7 percent. Majority of respondents were from EU/EEA (79%), the rest (21%) were from Americas.

71 percent of respondents use ISO-based approach for achieving compliance, while 29 percent use ISAE-based approach. NIST was also mentioned and one respondent expressed interest to use the EU-SEC approach.

64 percent are adhering to up to 5 compliance schemes/frameworks/regulatory frameworks, while 14 percent are adhering to up to 10.

Some of the standards not included in the EU-SEC requirements repository are relevant NIST standards, ISO/IEC 27701:2019, COBIT, HITRUST, GDPR, Shared Assessments Program Tools - SIG and SCA, and upcoming AUDITOR data protection certification.

Standards leveraged within the organisations are ISO27001/27017/27018, CSA STAR, SOC2, BSI C5, PCI-DSS, relevant NIST standards, Shared Assessment Program and NEN-7510 (Dutch healthcare based on 27001).

When asked about the potential barrier to the continued adoption of (additional) standards, 93 percent believe it would increase cost, 64 percent indicated lack of resources and 29 percent believe it would confuse the cloud customers. All respondents find MPRF approach as beneficial and 64 percent do not see any barriers to using the MPRF for achieving compliance to several standards. Other 5 respondents (each representing 7%) are not familiar with it; their auditor cannot provide such a service; believe that the customers have low awareness; believe the auditors and regulators will be sceptical to true mutual recognition; mention preconditions that need to be met for mutual agreement.

When asked if using any means of continuous monitoring/auditing, only 36 percent answered

positively, using different commercial monitoring tools and internal control frameworks. 93 percent find Continuous auditing-based certification beneficial for achieving a higher level of assurance in high risk environments, while 7 percent answered no with the argument that it would need customization, knowledge and resources.

While 21 percent do not see any potential barriers to use the continuous auditing-based certification, 29 percent do not have the technical ability for it, 21 percent believe the cost would be too high, 21 percent state both reasons and 7 percent see the limited number of auditors to support this service due to capability and knowledge as the main barrier.

Given the low number of responses the conclusions cannot be statistically relevant, however we were able to confirm some of the conclusions from the project. The most common approaches for achieving compliance continue to be ISO and ISAE-based approaches, where ISO-based approach is being prevalent. By that said, usually a CSP would still adhere to more than one compliance scheme. MPRF-based turns out to be beneficial, tackling some of the main barriers in the proliferated compliance landscape, such as increased cost, lack of resources and confusion of customers.

When it comes to the continuous auditing-based certification, the maturity of the market or the lack of thereof, represents different barriers for the adoption of a such an approach. Organisations might not have technical ability for it or believe the cost will be too high, or do not have enough resources. Based on the survey results and the conversations we had with the stakeholders both inside and outside the EU-SEC consortium, we believe that while there is a clear need and interest in continuous auditing-based certification. However, the market of tool providers needs to mature in order to make such a service more accessible and drive adoption by providing the technical ability for their customers and ultimately lowering the cost for the continuous auditing.

3.1 KEY PERFORMANCE INDICATORS

The following table shows progress against the KPIs defined at the beginning of the project for 2019 and the total project duration.

Table 16: Achievement against KPIs

Area of impact	Description	KPI	Achieved to 2019	Achieved total project duration
Policy impact	Number of contributions to standards/best-practices	>5	2	6
	Number of contributions to roadmaps, discussion papers (per year)	>2	3	5
	Number of contributions to policy-makers	>5	1	5

4 SUMMARY AND CONCLUSION

During the second half of the project (M19-M36), the EU-SEC project increased the intensity of its dissemination, exploitation and standardisation activities to ensure increased awareness of its results and optimise their uptake. The project has proactively managed its activities to ensure compliance with its year three KPI's and overall project KPIs. As shown in Tables 15 and 16, the KPIs set at the onset of the project were achieved, and in many cases exceeded. Each of the consortium partners developed the short- and long-term exploitation plans for the project innovations.

One of the key dissemination activities performed during the third year was the update of the website to bring a clearer, more focused message to stakeholders. The project also participated in a large number of EU, industrial and academic events to ensure a full spectrum of engagement and impact.

Standardisation activities focused, especially during the last 12 months, on participating in the expert group established by the European Commission, CSPCert, and in engaging with ENISA. The objective has been to contribute the MPRF and CABC certification approaches to the European Cloud Certification scheme currently under development. The results of the project have fed into the work of EC and ENISA and serve as a valuable contribution for further development of the EU cybersecurity certification scheme. Additionally, from the GDPR perspective, the PLA Code of Conduct has matured as a comprehensive framework for complying with the GDPR. From this perspective we have received positive feedback from the French Data Protection Authority (CNIL) and review meeting has been scheduled with them for the 16th of January 2020.

Finally, the consortium is very proud of the rich set of materials left at the disposal of cloud stakeholders and the website will remain active to promote the outputs of the project and to ensure the widest possible reach and adoption of the innovations developed.

ANNEX A

Table 17 Journal articles and peer reviewed publications

Year	Author(s)	Title	Type	Journal/Conference	Place / Country	Date	Published in	Publisher	Link
2017	Immanuel Kunz and Philipp Stephanow	A process model to support continuous certification of cloud services	PRP [17]	31st IEEE International Conference on Advanced Information Networking and Applications	Taipei, Taiwan	27.-29.3.2017	Conference proceedings	IEEE	https://doi.org/10.1109/AINA.2017.106
2017	Philipp Stephanow and Koosha Khajehmoogahi	Towards continuous security certification of Software-as-a-Service applications using web application testing techniques	PRP	31st IEEE International Conference on Advanced Information Networking and Applications	Taipei, Taiwan	27.-29.3.2017	Conference proceedings	IEEE	https://doi.org/10.1109/AINA.2017.107
2017	Philipp Stephanow and Christian Banse	Evaluating the performance of continuous test-based cloud service certification	PRP	2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing	Madrid. Spain	14.-17.5.2017	Conference proceedings	IEEE	https://doi.org/10.1109/CCGRID.2017.134
2017	Anton Ujčič,	The European Security Cerification Framework EU-ESC	PRP	IJU 2017 Informatics in Public administration	Brdo pri Kranju,	4.-5.12.2017	Conference proceedings	Slovenian Socie	https://event.meetpoint.si/konferenca.iju-2017

[17] Peer reviewed publication

	Darja Lihteneger				Slovenia			ty informatika	
2017	Philipp Stephanow, Mohammad Moein, Christian Banse	Continuous location validation of cloud service components	PRP	2017 IEEE 9th International Conference on Cloud Computing Technology and Science	Honk Kong	11.-14.12.2017	Conference proceedings	IEEE	https://doi.org/10.1109/CloudCom.2017.29
2018	Anton Ujčič, Bojan Pohar	Development of the new EU-SEC certification framework for cloud computer services	PRP	DSI 2018 Days of Slovenian Informatics	Portorož, Slovenija	17.-18.4.2018	Conference proceedings	Slovenian Society informatika	https://dsi2018.dsi-konferenca.si/
2018	Martin Labaj, Karol Rástočný, Daniela Chudá	Semiautomatizované porovnávanie certifikačných schém cloudových služieb	PRP	DaZ & WIKT 2018	Czech Republic, Brno, Hotel Santon	11.10.18	Conference proceedings	Vysoké učení technické v Brně	http://daz2018.fit.vutbr.cz/DaZ_WIKT_2018_Sborník.pdf
2018	Anton Ujčič, Bojan Pohar	EU-SEC pilot use case, from ISO 27001 to ISO 27017	PRP	IJU 2018 Informatics in Public Administration	Brdo pri Kranju, Slovenia	10.-11.2018	Conference proceedings	Slovenian Society informatika	https://iju-2018.meetpoint.si/
2019	Martin Labaj, Karol Rástočný, Daniela Chudá	Towards Automatic Comparison of Cloud Service Security Certifications	PRP	SOFSEM 2019: 45th International Conference on Current Trends in Theory and Practice of Computer Science	Slovak Republic, Nový Smokovec, Atrium Hotel	01/27-30/2019	Conference proceedings	Springer	https://beda.dcs.fmph.uniba.sk/sofsem2019/

2019	Anton Ujčič, Damir Savanović	Okvir medsebojnega priznavanja EU-SEC / EU-SEC Multiparty Recognition Framework	J[18]	27th International Conference on Information Systems Auditing and Control	Kranjska gora, Slovenia	24.9.-25.9.2019	SIR*IUS 5/2019	Slovenian auditors institute	https://si-revizija.si/revija-sirius/sirius-2019#t240
2019	Jürgen Großmann, Dorian Knoblauch	Neue Wege in der IT-Sicherheitszertifizierung von Cloud Infrastrukturen	J	Objektspektrum: Online-Themenspecial zum Thema "Cloud Computing - Dynamische IT-Leistung aus der Wolke"	Deutschland	June 2019	Objektspektrum: Online-Themenspecial zum Thema "Cloud Computing - Dynamische IT- Leistung aus der Wolke"		
2019	Dorian Knoblauch, Jürgen Großmann, Linda Strick, Alain Pannetrat	Europäisches Rahmenwerk für Continuous Auditing based Certification	PRP		Germany		Tagungsband zum 16. Deutschen IT-Sicherheitskongress, ISBN: 978-3-922746-82-9	SecuMedia Verlag	https://www.bsi.bund.de/DE/Service/Aktuell/Veranstaltungen/IT-Sicherheitskongress/IT-Sicherheitskongress_node.html
2019	Dorian Knoblauch & Jim de Haas	Cloud Provider Continuous Assurance: EU SEC Framework for Continuous Assurance in the Cloud	J	ISSA Journal Oct 2019	Netherlands	Okt 19	Issa Journal October 2019 Volume 17 Issue 10	ISSA	
2019	André Koot	EU-SEC helpt auditors	J	de IT-Auditor	Netherlands	Sep 10	IT Auditor 2-2019	NOREA	2019

[18] Article in journal

Table 18 Conference and workshop presentations

Year	Author(s)	Title	Type	Name of Conference / Workshop / Event	Place / Country	Date
2017	Daniele Cattdeddu	Estonian Cloud Security Strategy	Presentation	Estonian Mimnistry of Interior	Tallin	01.03.17
2017	Linda Strick	EU-SEC presentation at Certification Workshop and DSM Stakeholder Meeting	Presentation	DSM Stakeholder Meeting	Brüssel, Rue de la LOI	11.12.17
2018	Linda Strick	EU-SEC Dissemination at ENISA WS Towards the EU Cybersecurity Certification Framework	Presentation	ENISA WS Towards the EU Cybersecurity Certification Framework	Brüssel, Rue Gineste 3	01.03.18
2018	Alain Pannetrat	EU-SEC presemtation at the H2020 Project Clustering Workshop	Presentation	H2020 Project Clustering Workshop	Athens, Greece	31.01.18
2018	Linda Strick	Meeting Security Certification WG	Presentation	Security Certification WG	Brüssel, Rue Phillipe Le Bon	17.04.18
2018	Linda Strick	Presentation EU-SEC and Break out session chair	Presentation		Brüssel, Brussels Marriott Hotel, Rue Auguste Orts 3-7	26.04.18
2018	Daniele Cattdeddu	GDPR, Compliane fatigue and Continuous Assurance	Presentation	CSA Japan Security Summit	Tokio, Japan	23.05.18
2018	Daniele Cattdeddu	GDPR and Mutiparty recognition	Presentation and booth presence	InfoSecurity Europe	London	05-08/06/2018
2018	Linda Strick	Konferenz ICT in Trust - EU-SEC Präsentation	Presentation	Trust in ICT	Graz, Universitätsplatz 3	27.06.18

2018	Jürgen Großmann	Providing Trust Through Efficient Cloud Security Certification The EU-SEC Project		Webinar - Cybersecurity standards and certification - the challenges	Webinar at https://www.cyberwatching.eu/free-webinar-cybersecurity-standards-and-certification-challenges	Wed, Sep 5th, 2018
2018	Jürgen Großmann	The EU-SEC Project in When data becomes action - systematically preventing cyber risks in the IoT	Presentation	T Security Conference of the LKRZV, Cologne 2018	Cologne, Marriot Hotel	Mon, Sep 17th, 2018
2018	Ramon Martín de Pozuelo, Damir Savanovic	Continuous Auditing Based Certification	Presentation	Webinar - CSA FSSP (Financial Services Stakeholder Platform) Working Group Meeting	Webinar	Wed, Nov. 7th, 2018
2018	Jürgen Großmann	Providing Trust in Cloud Security - The EU-SEC Project	Presentation	Automotive Innovation Summit, Neckarsulm, Germany	Audi Forum, Neckarsulm	Tue, Nov. 27th, 2018
2018	Anton Ujčič	Achieving compliance with the requirements of the various information security frameworks	Presentation	Annual Conference ISACA.SI	Ljubljana, Slovenija	06.11.18
2018	Daniele Cattdeddu	Cloud Security Alliance: Where we are &where we are going	Presentation	Cloud Security Summit	Milano, Italy	31.10.18
2018	Damir Savanovic	Continuous audit-based certification	Presentation	Annual Conference ISACA.SI	Ljubljana, Slovenia	06.11.18
2018	Daniele Cattdeddu	CSA CODE OF CONDUCT for GDPR COMPLIANCE	Presentation	EU Cyber Security and Cloud Computing conference	Vienna, Austria	06.12.18
2018	Dorian Knoblauch	Providing Trust Through Efficient Cloud Security Certification	Presentation	Truessec Final Symposium, Lille, 12th December 2018	1 Place Déliot,59000 Lille,France	12.12.2018

2018	Dorian Knoblauch	Increasing the efficiency of cloud certification - Continuous certification	Presentation	Halfway Through the Digital Single Market Strategy	1 Place Déliot,59000 Lille,France	13.12.2018
2019	Niki Klaus		Presentation	Aalto University, Helsinki, Finalnd	Finland	10.01.19
2019	Andé Koot	EU-SEC EU Security Certification presentation	Presentation	CSA Netherlands Cloud Journey Event	Netherlands	15.01.19
2019	Daniele Cattdeddu	CSA Star: The leading cloud trust & accountability program	Presentation	RSA Conference	San Francisco, USA	04-08.03.19
2019	Daniele Cattdeddu	CSA Star: The leading cloud trust & accountability program	Presentation	Cloud Security Summit	Milano, Italy	12-14.03..19
2019	Dorian Knoblauch, Christian Banse	Reducing implementation efforts in continuous auditing certification via an Audit API	Presentation	28th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2019)	Capri, Italy	12-14.06.19
2019	Dorian Knoblauch	Europäisches Rahmenwerk für Continuous Auditing based Certification	Presentation; key note speech	16th BSI German IT Security Congress	Bonn, Germany	21.23.05.19
2019	Niki Klaus	True stories of cyber-crime and insight on how to prevent	Presentation	European Cyber Crime and Fraud Investigators Conference (ECCFI)	Vienna, Austria	09.05.19
2019	Chris van den Hooven		Presentation	Cyber Security Conference	Amsterdam, The Netherlands	13.05.19
2019	Rastislav Neczli	Onboarding Cloud Services with MPRF approach	Presentation	Slovak government		01.05.19
2019	Damir Savanovic	Trust in Cloud by Certification	Presentation	Cyber Week	Tel Aviv, Israel	23-27.06.19
2019	Dorian Knoblauch	Continuous Auditing Certification	Presentation	ETSI Security Week 2019	Sophia Antipolis, France	21.06.19

2019	Tatu Suhonen & Chris Van Den Hooven	EU-SEC: What's in it for us?	Presentation	Nixucon19 security conference	Tallinn, Estonia	28.08.19
2019	Anton Ujčič, Damir Savanović	Okvir medsebojnega priznavanja EU-SEC / EU-SEC Multiparty Recognition Framework	Presentation	27th International Conference on Information Systems Auditing and Control	Kranjska gora, Slovenia	25.09.19
2019	Damir Savanovic	The impact of EU Security Act on Cloud Computing	Presentation	ITAPA 2019	Bratislava, Slovakia	12.11.19
2019	Damir Savanovic	The impact of EU Cyber-Security Act on Cloud	Presentation	Advanced Threat Summit 2019	Warsaw, Poland	13.11.19
2019	Lefteris Skoutaris	The EU-SEC Framework	Presentation	2019 International conference on the EU Cybersecurity Act	Brussels, Belgium	18.11.19
2019	Damir Savanovic	Trust in Cloud by Certification	Presentation	CSA EMEA Congress	Berlin, Germany	20.11.19

Table 19 Press releases and news items

Reported Quarter	Organisation	Author(s)	Title of press release/news item	Date published	Published in	Link
Q1	SixSq	Louise Merifield	SixSq part of H2020 Cloud Security Project	31.01.17	SixSq website	https://sixsq.com/news/2017-01-31-news-eusec-announcement/
Q1	SI-MPA	Anton Ujčič	EU-SEC project	31.01.17	SI-MPA website	https://www.gov.si/zbirke/projekti-in-programi/eu-sec/
Q1	FhG FOKUS	Linda Strick/Jürgen Großman	SixSq part of H2020 Cloud Security Project	31.01.17	FOKUS website	https://www.fokus.fraunhofer.de/de/sqc/projekte/eu-sec
Q7	Fabasoft	Christoph Stangl	Fabasoft Cloud Reconfirmed as World's Most Secure Cloud Service	12.06.18	FAbsoft website	https://www.fabasoft.com/en/news/press/press-releases/fabasoft-cloud-reconfirmed-worlds-most-secure-cloud-service

Q6	SI-MPA	Polona Srebotnjak Verbinc	Uspešno prestali mednarodno neodvisno presojo sistema upravljanja državnega računalniškega oblaka (DRO)	20.06.18	SI-MPA website	http://mju.arhiv-spletisc.gov.si/si/novinarsko_sredisce/novica/9853/
Q6	SI-MPA	Anton Ujčič	Državni računalniški oblak je uspešno preživel presojo (SGC sucsessfuly passed the audit)	23.06.18	DnevneNovice.com	https://www.dnevne-novice.com/14-magazin/1515-drzavni-racunalniski-oblak-je-uspesno-prezivel-presojo
Q7	SixSq	Louise Merifield	Join the Workshop on European Security Certification	04.09.18	SixSq website	https://sixsq.com/news/2018-09-04-news-eusec-workshop/
Q8	SixSq	Louise Merifield	European Security Certification on the Agenda in Linz	10.10.18	SixSq website	https://sixsq.com/news/2018-10-10-news-eusec-linz-meeting/
Q9	CSA	Daniele Catteddu	Cloud Security Alliance Launches STAR Continuous, a Compliance Assessment Program for Cloud Service Providers	04.03.19	CSA website	https://cloudsecurityalliance.org/press-releases/2019/03/04/csa-launches-star-continuous-compliance-assessment-program-for-cloud-service-providers/
Q9	FhG FOKUS	Jürgen Großmann	Join the Workshop on European Security Certification in Barcelona	14.03.19	FOKUS website	https://www.fokus.fraunhofer.de/eusec_barcelona
Q9	CSA	Daniele Catteddu	STAR and EU-SEC: a solution for your compliance fatigue.	27.03.19	Inner Circle - CSA Member Newsletter V2-3	
Q9	FhG FOKUS	Jürgen Großmann	Workshop Multi Party Recognition in Amsterdam	16.04.19	FOKUS website	https://www.fokus.fraunhofer.de/en/news/MPRF_Amsterdam
Q9	FhG AISEC	Christian Banse	Fraunhofer AISEC stellt Tool zur Absicherung von Cloud-basierten Diensten zur Verfügung	31.05.19	Fraunhofer website	https://www.aisec.fraunhofer.de/de/presse-und-veranstaltungen/presse/pressemitteilungen/2019/Clouditor.html
Q10	CSA	Daniele Catteddu	EU SEC	31.05.19	Inner Circle - CSA Member Newsletter V2-5	

Q10	Nixu	Niki Klaus	The first Finnish audit criteria for cloud services released – PiTuKri improves cloud security	05.06.19	Nixu website	https://news.cision.com/nixu-oyj/r/the-first-finnish-audit-criteria-for-cloud-services-released---pitukri-improves-cloud-security,c2834387
Q10	Fabasoft	Christoph Stangl	Fabasoft Cloud Reconfirmed as World's Most Secure Cloud Service	12.06.19	Fabsoft website	https://www.fabasoft.com/en/news/press/press-releases/fabasoft-cloud-reconfirmed-worlds-most-secure-cloud-service
Q6	SI-MPA	Polona Srebotnjak Verbinc	Information about EU-SEC audit	20.06.19	SI-MPA website	http://mju.arhiv-spletisc.gov.si/si/novinarsko_sredisce/novica/9853/index.html
Q11	FhG FOKUS	Jürgen Großmann	EU-SEC Workshops in Berlin	01.11.19	FOKUS website	https://www.fokus.fraunhofer.de/edca4e5fd2544115
Q12	CSA	Damir Savanovic, Louise Merifield	CSA Contributes to Key How-To Guidance Documents for Multi-Party Recognition and Continuous Audit-Based Certification	07.11.19	CSA website	https://cloudsecurityalliance.org/press-releases/2019/11/07/csa-contributes-to-key-how-to-guidance-documents-for-multi-party-recognition-and-continuous-audit-based-certification/
Q12	SixSq	Louise Merifield	European Cloud Security Project Leaves Rich Legacy of Materials for Cloud Stakeholders	18.12.19	SixSq website	https://sixsq.com/news/2019-12-18-news-eusec-final/
	CSA	Damir Savanovic		19.12.19	CSA website	https://cloudsecurityalliance.org/press-releases/2019/12/19/european-cloud-security-project-leaves-rich-legacy-of-materials-for-cloud-stakeholders/
Q12	FhG FOKUS	Jürgen Großmann	Whitepaper on CAC	22.03.2019	FOKUS website	https://www.fokus.fraunhofer.de/7611f85e98dd80db
Q12	FhG FOKUS	Jürgen Großmann	Project results including Training and Awareness Packags, Videos and Howtos	16.12.19	Fraunhofer website	https://www.fokus.fraunhofer.de/en/sqc/news/eusec_final

Table 20 Trainings with industry/SMEs

Date	Organisation targeted	Partner involved	Title/subject of training	Location
9.-10.10.19	Automotive Industry & Telecommuication Industry (Volvo, Infineon, Vodafone and Thales)	Fraunhofer FOKUS, Jürgen Großmann	Security Certification for Future Automotive Cloud Architectures, https://bisgrp.com/event/2nd-annual-automotive-cyber-security-forum	Automotive Cyber Security 2019, https://bisgrp.com/event/2nd-annual-automotive-cyber-security-forum, Berlin
11.10.19	Internal seminar at Fraunhofer FOKUS to adress researcher in the quality assurance domain at Fraunhofer FOKUS	Fraunhofer FOKUS, Dorian Knoblauch	The role of MPRF and CABC for future Cloud Security Certification	Fraunhofer FOKUS, Berlin
21.04.19	Internal seminar at CAIXA to explain CABC and EU-SEC developments to Information Security Governance	Internal seminar at CAIXA to explain CABC and EU-SEC developments to Information Security Governance	EU-SEC Demo & Training session - CABC hands-on	Barcelona, Spain
28.03.19	Banco de España	CaixaBank (Ramon Martin de Pozuelo and Mario Maawad), Fraunhofer FOKUS (Dorian Knoblauch), Fraunhofer AISEC (Christian Banse), CSA (Alain Pannetrat)	EU-SEC Demo & Training session - CABC hands-on	Barcelona, Spain
05.12.19	Fabasoft	Internal seminar at Fabasoft to explain MPRF and EU-SEC developments Fabasoft staff responsible for audit processes	EU-SEC Demo & Training session - MPRF: How to use it	Linz, Austria
26.11.19	Slovenian Audit Institute	CSA	EU – SEC Framework – A step to more efficient cloud compliance	Ljubljana, Slovenia

Table 21 Market consultation meetings

Date	Organisation(s) targeted	Partner involved	Topic discussed (CABC, MPRF etc)	Location	Reference
12.12.17	DSM cloud stakeholders	CSA	Cloud certification	Brussels, Belgium	https://ec.europa.eu/digital-single-market/en/news/dsm-cloud-stakeholder-meeting-0
18.04.18		CSA	Meeting Stakeholder workshop on data protection certification mechanisms, seals and marks	Brussels, Belgium	
04.07.18	Cloud Customers (B2B)	Fabasoft	What does dataprotection bring to the table?	Online	Webinar 04.07.2018 "Was bringen Datenschutzzertifzierungen von Cloud-Diensten?" - Text und Verlinkung (Teil 1)
28.02.19	Banco d'España	Caixa Bank, Ramon Martin Pozuelo and Maroi Maaxwad	Meeting with Banco de España, the Spanish regulator of the Financial Sector, presenting EU-SEC project and the potential benefits for enhancing the control of Cloud Service Providers.	Barcelona, Spain	
12.06.19	DSM cloud stakeholders	CSA	Cloud certification	Amsterdam, Germany	https://cspcerteurope.blogspot.com/2019/06/handover-of-cspcert-final-deliverable.html
11.09.19	National authorities	Nixu	Meeting a Finnish authority to discuss certification seals for different applications such as IoT and cloud	Helisinki, Finland	
30.09.19	Cloud security certification for health insurer	Fraunhofer FOKUS	The role of the EU-SEC Frameork for the security certifications in	Leipzig, Germany	https://www.gesundheitsforen.net/portal/de/veranstaltungen/fachsymposien_und_ko

			the eHealth domain (health insurer)		ngresse/fachsymposium_cloud/archiv_5/startseite_cloud_loesungen_2.xhtml
30.09.19	DSM cloud stakeholders	CSA	Cloud certification	Warsaw, Poland	https://www.gov.pl/web/digitalization/releasing-digital-potential-of-the-polish-economy
16.12.19	Hitachi (Japanes delegation)	Fraunhofer FOKUS	The role of the EU-SEC Frameork for the security certifications of Japanese Governmental Cloud.	Berlin, Germany	
16.12.19	Hitachi (Japanes delegation)	Fraunhofer FOKUS`	The role of the EU-SEC Frameork for the security certifications of Japanese Governmental Cloud.	Berlin, Germany	
02.-03.04/2019	DSM cloud stakeholders	CSA	Cloud certification	Berlin, Germany	https://cspcerteurope.blogspot.com/2019/04/outcome-of-berlin-public-plenary-of-2nd.html
26.-27/02/2019	DSM cloud stakeholders	CSA	Cloud certification	Madrid, Spain	https://ec.europa.eu/digital-single-market/en/news/dsm-cloud-stakeholder-meeting-madrid
28-29/06/2017	DSM cloud stakeholders	CSA	Cloud certification	Brussels, Belgium	https://ec.europa.eu/futurium/en/next-generation-internet/net-futures-conference-28-29-june-2017-brussels

Table 22 Domain exhibitions

Date	Organisation	Name of exhibition	Type of participation (booth, poster etc)	Location	Link or other information
5.-8.6.2017	CSA	Infosecurity Europe	Booth, flyer	Olympia, London, UK	https://www.infosecurityeurope.com/
5.-8.6.2018	CSA	Infosecurity Europe	Booth, flyer, presentation	Olympia, London, UK	https://www.infosecurityeurope.com/
20.06.18	Fabasoft	Fabasoft TechSalon	Roll-Up	Vienna, Austria	https://www.fabasoft.com/de/news/events/fabasoft-techsalon-wie-kann-oesterreich-mehr-informatikabsolventen-ausbilden
06.12.18	Fabasoft	DSM Stakeholder Day	Roll-Up + Panel Discussion	Vienna, Austria	https://www.fabasoft.com/de/news/events/cybersecurity-und-cloud-computing-so-erreicht-europa-den-ultimativen-wettbewerbsvorteil
22.01.19	Fabasoft	Fabasoft egovday 2019	Roll-Up	Munich, Germany	https://www.fabasoft.com/de/news/events/fabasoft-egovday-2019-wien
25.01.19	Fabasoft	Fabasoft egovday 2019	Roll-Up	Vienna, Austria	https://www.fabasoft.com/de/news/events/fabasoft-egovday-2019-wien
17-21.06.19	FhG FOKUS	IoT Week 2019, 5G, IoT and End-to-End Security	Presentation; panel discussion	Aarhus, Denmark	https://www.sec-cert.eu/iot-is-continually-challenging-status-quo-and-massively-affecting-our-everyday-lives-357bd66b1be46279
2-3.10.2019	Nixu	Cyber Security Nordic	Ville Koskinen & Matti Leinonen		Booth presence
2.-3. 06 2019	FhG AISEC	Tech Days Munich	Booth, flyer	Munich, Germany	
4.-7.3.2019	CSA	RSA Conference	Booth, flyer, presentation	San Francisco, USA	https://www.rsaconference.com/usa/2019

Table 23 Training with Certification Authorities

Date	Certification authority	Partner involved	Title/subject of training	Location
13.12.19	ENISA	CSA, Fabasoft	EU-SEC MPRF	On-line
18.12.19	ENISA	CSA, Fraunhofer	EU-SEC CABC	On-line

Table 24 Project hosted external workshops

Reported Quarter	year	Organisation (e.g. Company XYZ)	Name of the event	Date	Location	Link
Q7	2018	EU-SEC	EU-SEC Awareness Workshop	11.09.18	BRUSSELS	https://www.sec-cert.eu/eu-sec/event/certification
Q9	2019	EU-SEC	Continuous Auditing Based Certification Workshop	09.04.19	Barcelona	https://www.sec-cert.eu/eu-sec-workshop-on-continuous-auditing-certification-a2bb0e88033e772d
Q10	2019	EU-SEC	MPRF Workshop	13.05.19	Amsterdam	https://www.sec-cert.eu/workshop-on-multi-party-recognition-83de4de4d0701ce0
Q12	2019	EU-SEC	MPRF Workshop & Tutorial	09.10.19	Berlin	https://www.sec-cert.eu/eu-sec/ws_bln9
Q12	2019	EU-SEC	Continuous Auditing Based Certification Workshop & tutorial	08.10.19	Berlin	https://www.sec-cert.eu/eu-sec/ws_bln8

Table 25 Posters, flyers and white papers

Title	Link
EU-SEC Flyer Continuous Auditing Pilot (PDF)	https://cdn0.scrvt.com/fokus/c23b8da26b7c28e7/dd836aa31c7c/EU-SEC_Flyer_CA-PILOT.pdf
EU-SEC Flyer Multi-Party Recognition Framework (PDF)	https://cdn0.scrvt.com/fokus/6facaa36896042b8/bfdf149612d0/EU-SEC_Flyer_MPRF-PILOT.pdf
EU-SEC Flyer Introduction to Project (PDF)	https://cdn0.scrvt.com/fokus/aa1088df93003b7a/736c41bba24d/EU_SEC-Flyer-general-info.pdf
Poster Fabasoft	
EU-SEC CAC White Paper	https://cdn0.scrvt.com/fokus/85f83fc61e693f46/62d46bdb93ec/EU_SEC_Whitepaper_CA.pdf
EU-SEC MPRF White Paper	https://cdn0.scrvt.com/fokus/cd6cd750124ccf71/46442e26d182/MPRF-whitepaper-eu-sec.pdf

Table 26 New training seminars, videos and other material

Training Material	Link/further information
The EU-SEC Continuous Audit-Based Certification Training and Awareness Slide Set	https://cdn0.scrvt.com/fokus/9d6e91d8b5492f45/c2c17c2a261c/EU-SEC_Training_and_Awareness_Slide_Set_Continuous_Auditing_Based_Certification.pdf
The EU-SEC Multi Party Recognition Training and Awareness Slide Set	https://cdn0.scrvt.com/fokus/203c539bc372c6e4/d9ea3668ea9c/EU-SEC_Training_and_Awareness_Slide_Set_Multiparty_Recognition_Framework.pdf
CSA MPRF Webinar	https://www.brighttalk.com/webcast/16947/358154
CSA CABC Webinar	https://www.brighttalk.com/webcast/16947/358149
CABC Howto Document	https://cdn0.scrvt.com/fokus/2dd3c180ea11ea69/1c925e3b6fb9/EU-SEC-Guidelines---Implementing-Continuous-Audit-Based-Certification.pdf
MPRF Howto Document	https://cdn0.scrvt.com/fokus/ccc72dd1f339f01e/440004d502fa/EU-SEC-Guidelines---Implementing-Multi-Party-Recognition-for-Cloud-Security-Certifications---ALL-GUIDES.pdf
CABC explanation videos	https://www.sec-cert.eu/continuous-auditing-certification-2800106f184f06e8
MPRF explanation videos	https://www.sec-cert.eu/multi-party-recognition-fc436dc07a7fbfa2