EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

# D6.4 TRAINING AND AWARENESS PLAN

VERSION 1.1

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

|  |  |
|---|---|
| DUE DATE: 31.12.2018 | DELIVERY DATE: 21.1.2019 |
| AUTHOR:<br>CSA | PARTNERS CONTRIBUTED:<br>SixSq, Fabasoft |
| DISSEMINATION LEVEL:*<br>Public | NATURE OF THE DELIVERABLE:**<br>R |
| INTERNAL REVIEWERS:<br>Fabasoft, Fraunhofer |  |

*PU = Public, CO = Confidential

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

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

# VERSIONING

| Version | Date | Comment | Name, Organisation |
|---|---|---|---|
| 1.0 | 21/01/2019 | Initial Version | Damir Savanovic, CSA<br>Louise Merifield, SixSq |
| 1.1 | 24/05/2019 | Updated descriptions of educational activities | Damir Savanovic, CSA<br>Louise Merifield, SixSq |

# EXECUTIVE SUMMARY

This deliverable presents the activities the consortium intends to carry out to spread knowledge of project results to internal and external parties, both within academic and industrial domains. These activities will raise awareness and support the market uptake of the EU-SEC results. The document outlines the strategy and target audiences for its training and awareness activities and indicates the methodologies and tools the consortium intends to use. In addition, it includes a calendar which will be updated as necessary during the course of 2019.

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

© Copyright in this document remains vested with the EU-SEC Partner

# ABBREVIATIONS

| | |
|---|---|
| CSA | Cloud Security Alliance (Europe) LBG |
| CSC | Cloud Service Customer |
| CSP | Cloud Service Provider |
| DSM | Digital Single Market |
| e.g. | For example |
| EC | European Commission |
| etc. | et cetera |
| EU | European Union |
| EU-SEC | European Security Certification Framework |
| i.e. | id est (It is) |
| ICT | Information and Communication Technology |
| MPRF | Multi-Party Recognition Framework |
| n.a. | not applicable |
| NIS | Network and Information Security |
| NIST | National Institute of Standards and Technology |
| PwC | PricewaterhouseCoopers GmbH WPG |
| SIXSQ | SixSq Sàrl |
| SME | Small and Medium-sized Enterprise |
| tbd. | To be defined |
| WP | Work Package |

## TABLE OF CONTENTS

# LIST OF TABLES

# TERMINOLOGY AND DEFINITIONS

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

*Table 1. Terms and definitions*

| Term | Definition | Source |
|---|---|---|
| Audit | A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled | ISO/IEC 19011:2011, 3.1 |
| Audit criteria | Set of policies, procedures or requirements used as a reference against which *audit evidence* is compared<br>Note 1: Policies, procedures and requirements include any relevant Service Qualitative Objectives (SQOs) or Service Level Objectives (SLOs). | ISO/IEC 19011:2011, 3.2 |
| Auditee | Organization being audited. | ISO 9000:2005, definition 3.9.8 |
| Auditor | Person who conducts an audit. | ISO/IEC 19011:2011, definition 3.8 |
| Authorized Auditor | An auditing organization/auditor authorized by the certification authority/scheme owner to conduct assessments against the requirements of the scheme. A certification body is considered as an authorized auditor. | |
| Certification | The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. | https://www.iso.org/certification.html |
| Certification scheme | The set of rules, requirements and mechanisms that govern the process of certifying a process or a product.<br>**NOTE**: In this document we use interchangeably "certification scheme" and "compliance scheme" noting that in the real term practice often the term "certification scheme" is used when referring to ISO-based certification while the term "compliance scheme" is used when referring to ISAE 3000 audits. | EU-SEC D1.4 [1] |
| Cloud Control Matrix | Provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains *(CSA, 2016)*. Cloud Control Matrix is used as a central cloud service requirement scheme. | |
| Cloud service | A software service available in a cloud. | |

| Term | Definition | Source |
|---|---|---|
| Cloud service customer | A body that contracted a cloud service. | |
| Cloud service provider | A third-party company offering a cloud service. | |
| Continuous auditing | Continuous auditing is an automatic method used to perform auditing activities, such as control and risk assessments, on a more frequent basis. | |
| EU-SEC Security Requirements Repository | A repository of all collected requirements mapped against the CSA CCM, making it a native control framework to address the identified requirements | EU-SEC D1.2 v1.2 [2] |
| Information Security | Maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.<br>Note: The terms "continuous" and "on-going" in this context mean that security and privacy controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. | NIST SP 800-57 |
| Management system | System to establish policy and objectives to achieve those policies. | ISO 9000:2005, definition 3.2.2 |
| Multiparty recognition | A process for establishing a mutual agreement between certification and compliance scheme owners for recognition of the full or partial equivalence between the certification and/or attestation they govern. | EU-SEC D1.4 |
| Requirement | A need or expectation that is stated in a standard, law, regulation or other documented information, generally implied (i.e. it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied), or obligatory (usually stated in laws and regulations) | ISO/IEC 27000:2016 |
| Scheme Owner | The organization (individual, for-profit corporation, not-for-profit corporation, certification body, government department, agency or other body, trade association, group of certification bodies or other just about any other body or group of bodies) that is responsible for the development and maintenance of the scheme and owns the intellectual property, copyright, trademarks and other rights to a certification scheme. | |

# 1 INTRODUCTION

Promoting and implementing results is a major objective of the EU-SEC project. The project has already produced substantial results that include the realization of the first version of the EU-SEC framework (D2.4[1]) and the related validation works using the two representative work package four and five pilots: a) pilot 1: the multiparty recognition scheme for national/sectorial/international security, and b) pilot 2: continuous auditing-based certification[2] for the banking sector.

The conclusions and recommendations given by the partners who participated in the real-life pilots (i.e., CSPs and auditors) are representative of the greater efforts that are needed to be made to increase awareness among cloud stakeholders with respect to the usability of the EU-SEC framework, as well as the impact it has and the benefits it brings to the cloud security certification landscape.

The framework's maturity, when taking into consideration the feedback obtained from the pilots and also its expected future update to version D2.5, is continuously increasing. Recognition and awareness of the achieved results across the shareholder community are a key enabler for its future wide scale adoption. In this context, strategic awareness and training activities for users and providers of cloud services as well as the auditors and scheme owners/authorities are being planned in order to increase user trust in ICT services, and by such means maximize the EU-SEC framework's value proposition, market uptake and long-term sustainability.

This deliverable presents a training and awareness plan that will support the market uptake of the aforementioned results of the EU-SEC project and homonymous framework. The plan includes training events, educational online portals and material (e.g., webinars, booklets, quizzes), physical or virtual events (e.g., conferences, training workshops/tutorials and educational training sessions) and educational guidelines (e.g., presentations, white papers, reports, etc.) addressed to all the relevant stakeholders (auditors, CSPs, CSCs, and governmental institutions).

The following sections present the planned educational activities, including awareness-raising events and the training material that will be used under a well-defined timeframe.

[1] https://cdn0.scrvt.com/fokus/c375da367703d004/e78fe75a3771/9EU-SEC-Framework---Draft.pdf, accessed on 20/12/2018.

[2] https://cdn0.scrvt.com/fokus/ed7adf549baf0c9f/371b9af7dd9f/Pilot-preparation-v1.1_draft.pdf, accessed on 20/12/2018.

## 1.1 SCOPE AND OBJECTIVES

The objectives of this deliverable include the formulation of a training and awareness plan that will support the market uptake of the results of the EU-SEC project. The plan will include:

- The production and distribution of training and awareness material about the project's results
- The organization of training sessions and workshops to discuss the project's results with stakeholder communities

The scope of activities involves the transformation of the EU-SEC project's innovative content and results into awareness-raising material that is to be distributed throughout the established communication channels, as well as educational sessions and trainings. Mechanisms for effective communication and outreach need to be established in order to ensure that information is shared with relevant target audiences on a timely basis and by the most effective means to a broadest possible outreach. The produced educational material and planned events should be addressed to the relevant stakeholders listed below.

Finally, the organization of future educational activities into a calendar with well-defined milestones is to be used as the planning method towards achieving the two objectives of this deliverable.

## 1.2 DOCUMENT STRUCTURE

The planned educational activities are presented in chapter 2, including training sessions (virtual or physical), e.g., webinars, conferences, training workshops/tutorials, while chapter 3 introduces the educational material that is to be developed (e.g., presentations, white papers, reports, guidelines, etc.).

Finally, chapter 4 introduces a comprehensive calendar with planned events and defined milestones of educational activities.

# 2 EDUCATIONAL ACTIVITIES

The innovative nature of the project's activities necessitates a range of educational activities to ensure that potential users and beneficiaries are aware of how, why and when to benefit from the project results and thereby promote the market uptake. The activities will include awareness workshops, training sessions and associated supporting material, with a mixture of face-to-face and online formats.

## 2.1 TARGET AUDIENCE

EU-SEC reaches out to a broad number of stakeholders to raise awareness of activities and outcomes. The project's dissemination activities are wide-ranging and designed to address multiple audiences, including the general public. The educational activities, however, will be targeted at more specific groups of interest. Focus will be directed at the following communities:

- Auditors
- Cloud Service Providers
- Cloud Service Customers
- Government institutions

The aim is to support participants in understanding the work of the EU-SEC project with a view to adopting its framework and combining the novel approach with traditional certification methods.

## 2.2 WORKSHOPS & TRAINING

EU-SEC plans to leverage related conferences, such as ISACA EuroCACS, CSA EMEA Congress and the Digital Single Market (DSM) cloud stakeholder meetings, by co-locating its workshops and training events. The organisation of the events will include:

- Planning and preparation
    - The core topics, place, venue and agenda will be established. Announcements and invitations will be drafted and issued, with associated social media activity. Registration will be possible online via Eventbrite. Training material, a mixture of presentations and hands on, will be prepared, based on the outcomes of WP4

and WP5. This will take into account the need to familiarise attendees with the topics in hand using with the appropriate level information.

- Delivery
    - The workshop/training takes place, delivered by relevant work package experts. Participants will be provided with the associated material.
- Evaluation and follow up
    - Participants will be asked to evaluate the event and will be asked for consent to receive project updates on an ongoing basis.

After each event, partners will evaluate the process and examine feedback, which will be fed into the planning stage for the next workshop to continually improve quality.

The objectives relating to EU-SEC workshops and training are the following:

- Promote the use of the EU-SEC framework in the certification community
- Promote the use of the EU-SEC repository as a central point for finding information regarding certification and auditing schemes.

### *2.2.1 AWARENESS WORKSHOPS*

The project's overall plan is to deliver 4 workshops, 2 based on the Multi-Party Recognition Framework (MPRF) and 2 on Continuous Auditing based certification. The first of these, on MPRF, took place in September 2018. The content will be updated for the second workshop in each series, based on analysis of the project findings. The EU-SEC team will gather the findings of WP4 and WP5 and transfer them into material suitable for awareness raising activities.  The workshops will include practical demonstrations and recommendations.

The workshops will be full-day events, targeting all main target audiences defined in section 2.1.
The multiparty recognition framework (MPRF) workshops will provide an insight into the functionality of the framework, its tools and requirements comparison methodology, as well as the benefits offered to the cloud certification community and market. The main learning objectives for the MPRF awareness workshops will be to acquire an understanding of:

1. The purpose and objectives of the MPRF.
2. MPRF's life-cycle and its processes.
3. The business drivers for and benefits of the adoption of the MPRF
4. How to use the MPRF in real life (with practical, dedicated tips for the different target audiences, i.e. CSPs, Customers, Auditors & Consultant and scheme owners & regulators)

The Continuous Auditing workshops will show how Continuous Auditing Based Certification can address concerns about security, privacy and regulatory requirements, which are known to hinder cloud adoption. It will include showing participants how to perform a Continuous Auditing Based Certification which allows them to retrieve information on applied controls in an automated and near real time way. In addition, the workshops will demonstrate the technical architecture proposed to provide this service, its preliminary testing, the evaluation already undertaken and the different approaches deployed in the framework of EU-SEC project. The main learning objectives for the Continuous Auditing awareness workshops will be to acquire an understanding of:

1. the purpose and objectives of EU-SEC's Continuous Auditing Based Certification scheme
2. the purpose and objectives of the Pilot
3. EU-SEC's Continuous Auditing technical architecture, including use cases
4. business benefits of adopting Continuous Auditing model
5. how the scheme is applied in real life via a hands-on demo
6. how to fulfil security, privacy and regulatory requirements by applying a continuous and semi-automated audit on Cloud Services.

The project will attempt to organise the workshops in conjunction with relevant partners and events to optimise attendance by targeted stakeholders. They will be planned and announced in advance, including to the EC PO, to allow enough time to promote them with target groups and increase interest in participating. Moreover, they will be held in different European cities to reach as many stakeholders as possible.

### *2.2.2 TRAINING WORKSHOPS*

Training workshops will be the follow-up to the Awareness Workshops. They will be delivered to both internal and external partners, in the form of two to four-hour workshops, based on audience requirements. They will be delivered by EU-SEC domain experts and targeted at industry and SMEs as well as certification authorities. Participants will be given the opportunity to discuss idea for application of the project results and be given concrete support on how to use them in their business environment.

The educational materials as described in section 2.2.6 will be used for the delivery of the training workshops. In addition, a presentation pack will be developed which will allow EU-SEC partners to deliver shorter training sessions to colleagues and interested partners.

### *2.2.3 JOINT TRAINING EVENTS*

Joint Training will be a lightweight version of the two Training Workshops combined, covering the topics of MPRF and Continuous Auditing Certification in one event.

### 2.2.4 INDIVIDUAL TRAINING EVENTS

Using the presentation pack developed for the training workshops, EU-SEC partners will be able to deliver tailored training to individuals or small groups on request, either in-house or externally.

### 2.2.5 WEBINARS

The project plans to deliver 2 recorded on-line training sessions in the form of webinars on the topics of multiparty recognition framework and continuous auditing-based certification. They will be presented via BrightTalk and will be available free of charge. They will be targeted at an intermediate to advanced level audience and will present the main challenges that the project is addressing, including the objectives and methodology used. Webinars will also present the theoretical model of both innovations and the main conclusions deriving from the project activities.

The consortium will also create videos based on project presentations and demonstrations, making the material available to a wider audience.

### 2.2.6 EDUCATIONAL MATERIALS

The workshops and training sessions will be supported by the development of material such as presentations, practical problem sheets and guidelines. To ensure the sustainability of the results beyond the end of EU-SEC, the materials will be made available online.

There will be dedicated training material for specific audiences, e.g. SMEs, auditors or CSPs. The material will be divided into:

1. Awareness guidance
2. How-to guidance

Awareness guidance will include a description of the purpose and objectives of the MPRF and continuous auditing-based certification and their processes. Additionally, it will include the business drivers for and benefits of their adoption and how to use them in real life from perspective of different target audiences.

Building on top of the awareness guidance, how-to guidance will provide guideline documents for including new security and privacy requirements in the MPRF and adopting the continuous auditing-based certification approach by different target audiences.

How-to guidance for MPRF will be composed of:

1. MPRF operational process overview which will describe the reasons for using the MPRF and its benefits, as well as how to interact with and participate in the MPRF.

2. Instructions on how to engage within each of the MPRF’s operational and governance processes
3. Use-case scenario of an MPRF-based audit.

How-to guidance for continuous audit-based certification will be composed of:

1. Description of the continuous auditing theoretical model with the motivations behind the development of the model, drill-down into the models, methodology and definition of the certification scheme.
2. Instructions on how the continuous auditing technical architecture works, including IaaS and SaaS approaches.
3. Use-case scenario of a continuous audit-based certification.

# 3 TRAINING AND AWARENESS CALENDAR

The following table summarises the current planning for training and awareness events.

*Table 2. Summary of planning for training and awareness events*

| **Location & Date** | **Activity** | **Topic** | **Related WPs** | **Leading & participating partners** |
|---|---|---|---|---|
| **Brussels, 10/09/2018** | Awareness Workshop | Multiparty Recognition Framework (MPRF) | WP2, WP4 | CSA, PwC |
| **Q1 2019** | Develop Educational Materials | Continuous Auditing Based Certification (CaC) | WP3, WP5 | all WP5 partners |
| **Q2 2019** | Develop Educational Materials | MPRF | WP2, WP4 | all WP4 partners |
| **Barcelona, 09/04/2019** | Awareness Workshop | CaC | WP5 | Caixa Bank, CSA |
| **Amsterdam 13/05/2019** | Awareness Workshop | MPRF | WP2, WP4 | CSA |
| **Berlin, 08/10/2019** | Awareness & Training Workshop | MPRF | WP2, WP4 | all partners |
| **Berlin, 09/10/2019** | Awareness & Training Workshop | CaC | WP2, WP5 | all partners |
| **Q3 & Q 4 2019** | Individual Training Events | MPRF, CaC | WP2, WP3, WP4, WP5 | all partners |
| **10/2019** | Webinar | MPRF | WP4 | all WP4 partners |
| **11/2019** | Webinar | CaC | WP5 | all WP5 partners |

# 4 EXPECTED OUTCOMES

The EU-SEC project strives to address the security, privacy and transparency challenges associated with the greater adoption of cloud services. Within this broad scope, the training and awareness plan is expected to establish a strong base of stakeholders aware of and willing to adopt the certification framework, under which existing certification and assurance schemes can co-exist. The main beneficiaries of the activities will be the auditors, CSPs and CSCs, as they will be presented with a tailored architecture and corresponding set of tools to improve the efficiency and effectiveness of their current approach to security, governance, risk management and compliance in the cloud. Their improved awareness of the EU-SEC scheme will equip them inform other potential stakeholders and thereby increase the adoption of the framework in a commercial environment.

It is hoped that the EU-SEC framework and repository will become a reference point for standardisation initiatives.