Fraunhofer FOKUS
Institut für Offene Kommunikationssysteme

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

Providing Trust Through Efficient Cloud Security Certification

The EU-SEC Project

Jürgen Großmann

IoT Week in Aarhus June 17-21, 2019

Fraunhofer
FOKUS

Cloud Platforms: **Certification is Key for Trust in Cloud Security**

- Shift in control and governance over security and privacy to an indirect form
- CSC have to rely on statements and confirmations of CSPs
  - Code of conducts
  - Attestations
  - Certifications
- Annual or bi-annual third party audits and certifications have become the most effective solution to increase the level of trust

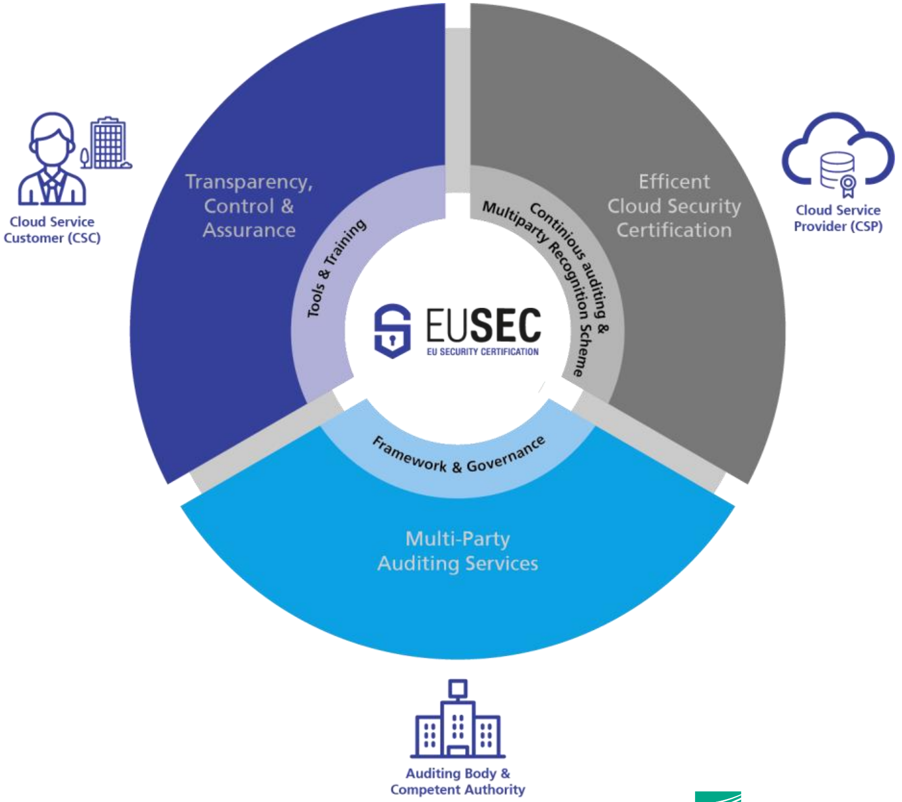
- **Certification and attestation have become a relevant cost factor,** while in the same time **interim changes** in infrastructures, applications and environments **go unaudited.**

Trust in Cloud by Certification:

The European Security Certification Framework (EU-SEC)

Innovation project with an aim to create a framework under which existing certification and assurance approaches can co-exist. It has a goal to improve the business value, effectiveness and efficiency of existing **cloud security certification schemes**.

- **Multiparty Recognition Framework (MPRF)** for cloud security certifications and
- **Continuous Auditing Based Certifications (CABC)**
- **Governance Structure** for trustful and compliant use of cloud computing



Cloud Service Customer (CSC)
Transparency, Control & Assurance
Tools & Training
EUSEC
EU SECURITY CERTIFICATION
Efficent Cloud Security Certification
Continious auditing & Multiparty Recognition Scheme
Cloud Service Provider (CSP)
Framework & Governance
Multi-Party Auditing Services
Auditing Body & Competent Authority

EU-SEC grant agreement no 731845

Project Set Up and Partners

A successful cooperation under the hood of a common project

Funded by **EU Horizon 2020**, a funding programme created by the European Union to support and foster research in the European Research Area

9 Partners (amongst them CSP, Cloud Users, Auditors, Scheme Owners and Researchers)

Duration: January 2017 – December 2019
Contact:
Twitter: @EU_SEC

CaixaBank

CSA cloud security alliance®

Fabasoft

Fraunhofer FOKUS

Fraunhofer AISEC

MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

nixu cybersecurity.

pwc | Deutschland

sixsq

EU-SEC Objectives: Increasing trust, efficiency and sustainability

- Increase user trust in Cloud Service Providers by
  - **defining principles, rules and processes for mutual recognition** between different certification schemes indicating security and privacy level.
  - **defining an approach for higher frequency security audits** for high security applications
- Support EU-SEC's long term sustainability by initiating the process for the **trans-European adoption of the EU-SEC framework and of the format used to express security requirements, controls and audit results**.

Photo by Noah Busher on Unsplas

EU-SEC grant agreement no 731845

EU-SEC Achievements: Applicability, flexibility and tool support

- **Cross-industry applicability** of the EU-SEC framework.
- **High level of security and privacy assurance and control** while the CSP enhances the Cloud Service, continuously.
- Consolidated framework which can be **adapted to new technical, compliance and market requirements**, easily and promptly.
- **Flexible and functional architecture and tools** for cloud security governance, risks management and compliance.

The U.S. National Archives

Business Drivers: Value Proposition – Cloud Service Providers

- **Saving money:** MPRF reduces compliance costs
- **Increased efficiency:** MPRF streamlines the compliance approach
- **Improved security**: Reducing security risks (higher audit frequency, less auditors approaching your data)
- **Transparency and clarity to the cloud customer**: One standard of reference to enable comparison and integration between many different ones.

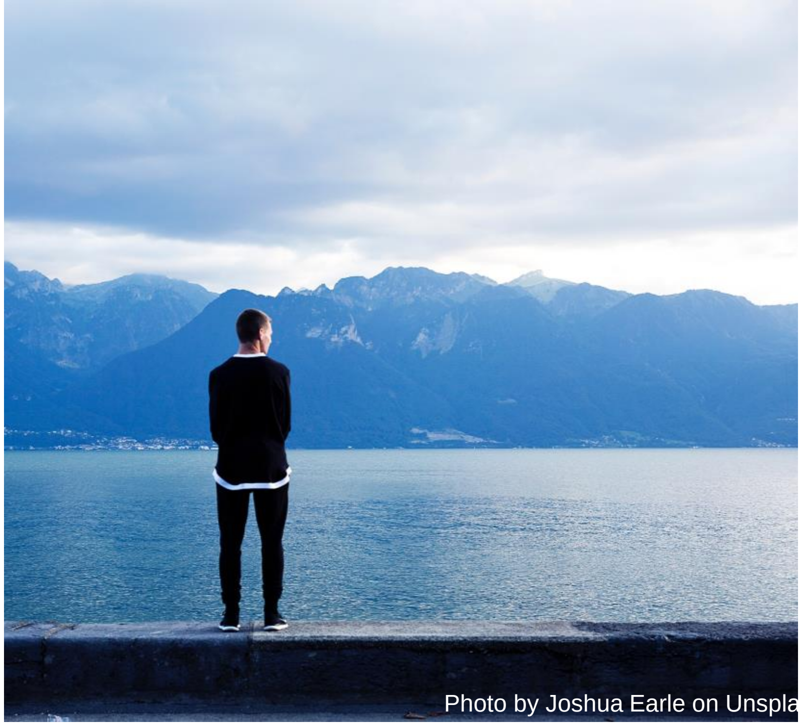


Photo by Joshua Earle on Unspla

The EU-SEC Multi Party Recognition Framework

1

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

Fraunhofer
FOKUS

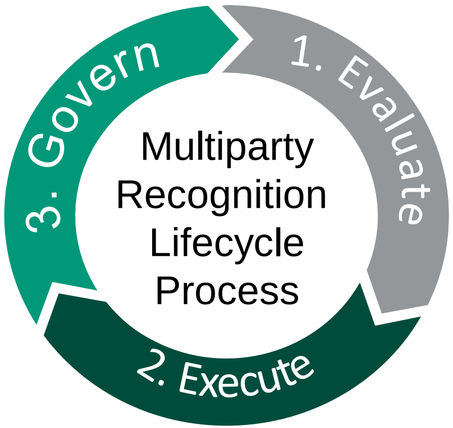
Multi Party Recognition Framework: Problem Statement

- CSPs pushed to invest in compliance audits
- Proliferation of certification schemes with
  - Increased assessment costs
  - Confusion of users
  - Market barriers for SMEs

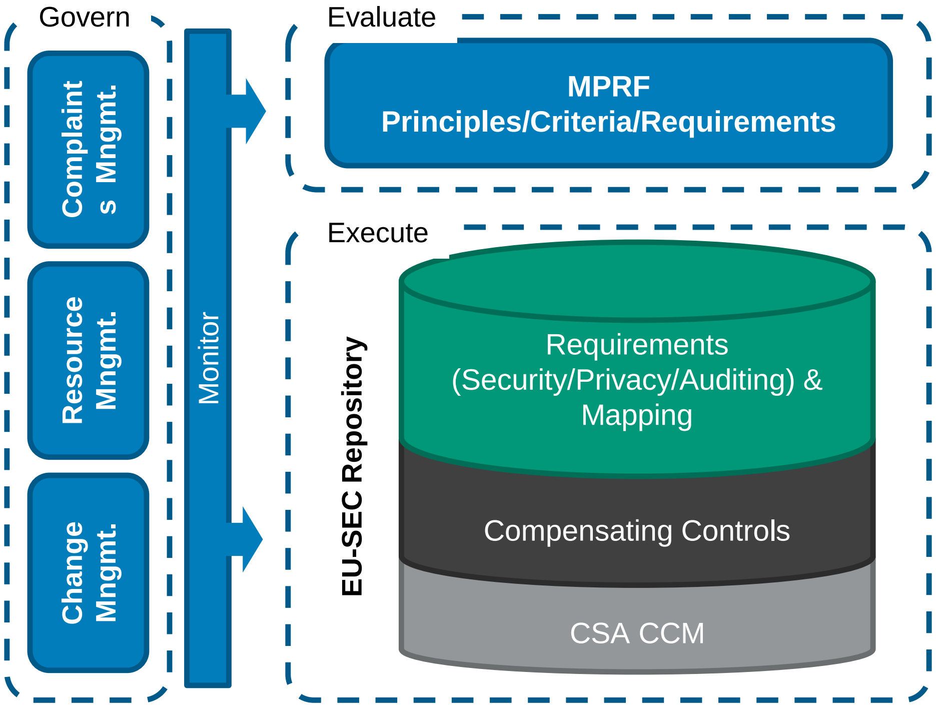
Argentina PDPA
Canadian Privacy Laws
CCSL (IRAP)
CDSA
China DJCP
China GB 18030
China TRUCS
CJIS
CS Mark (Gold)
CSA STAR Attestation
CSA STAR Certification
CSA STAR Self-Assessment
DoD
ENISA IAF
EU Model Clauses
EU-U.S. Privacy Shield
FACT
FDA CFR Title 21 Part 11
FedRAMP
FERPA
FIPS 140-2
FISC
GxP
HIPAA/HITECH
HITRUST CSF Certified
HITRUST
IRS 1075
ISO 22301
ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
IT Grundschutz Compliance Workbook
ITAR
Japan My Number Act
Centers for Medicare & Medicaid Services
MARS-E
MeitY
MPAA
iDA
MTCS
NIST 800-171
NZCC Framework
PCI-DSS
SHARED ASSESSMENTS
SHARED
AICPA SOC
AICPA SOC
AICPA SOC
ens
GOV.UK

- **Objectives**
  - **Minimize the effort** of obtaining certification "Y", when there is already certification "X".
  - **Streamline the cloud compliance** process, bring efficiency, increase assurance and reduce re-assessments cost

Multi Party Recognition Framework: Overview

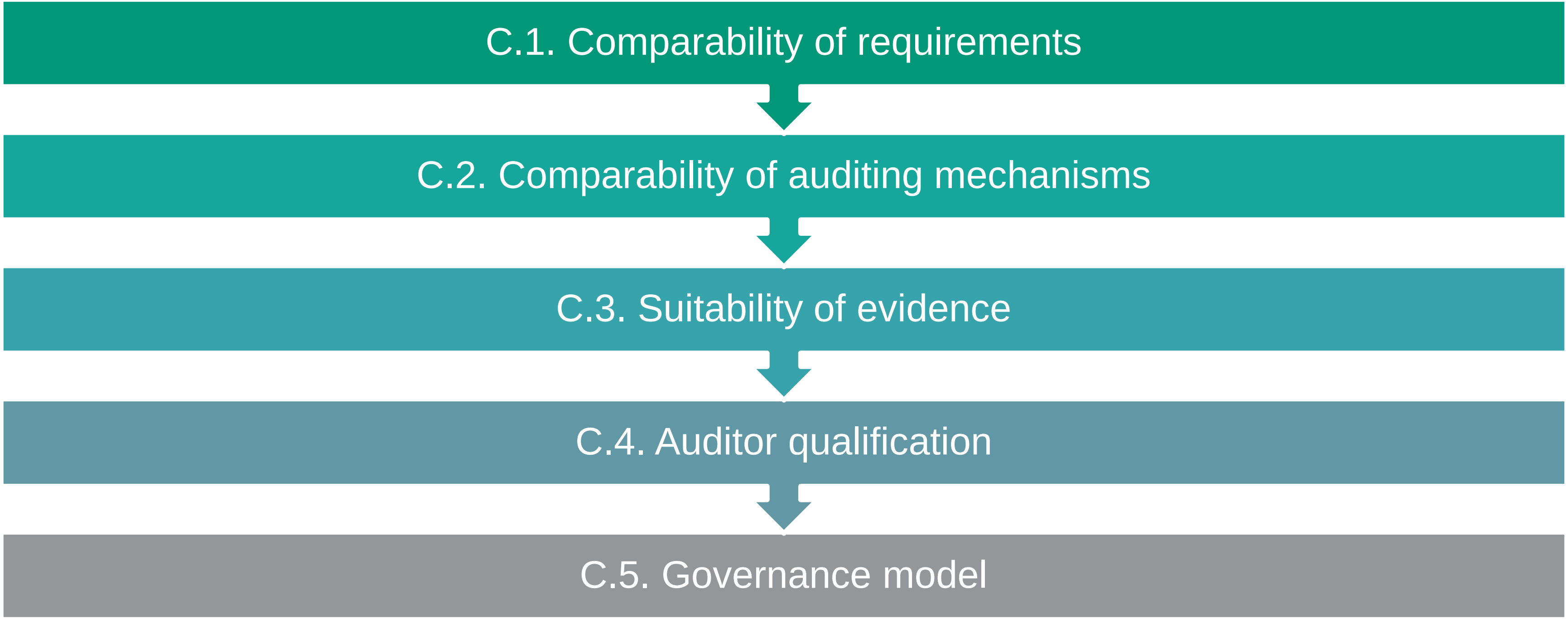


ISO 27000-family and the ISAE 3000 assessments are supported



EU-SEC grant agreement no 731845

Multi Party Recognition Framework: Multiparty Recognition Criteria



C.1. Comparability of requirements

C.2. Comparability of auditing mechanisms

C.3. Suitability of evidence

C.4. Auditor qualification

C.5. Governance model

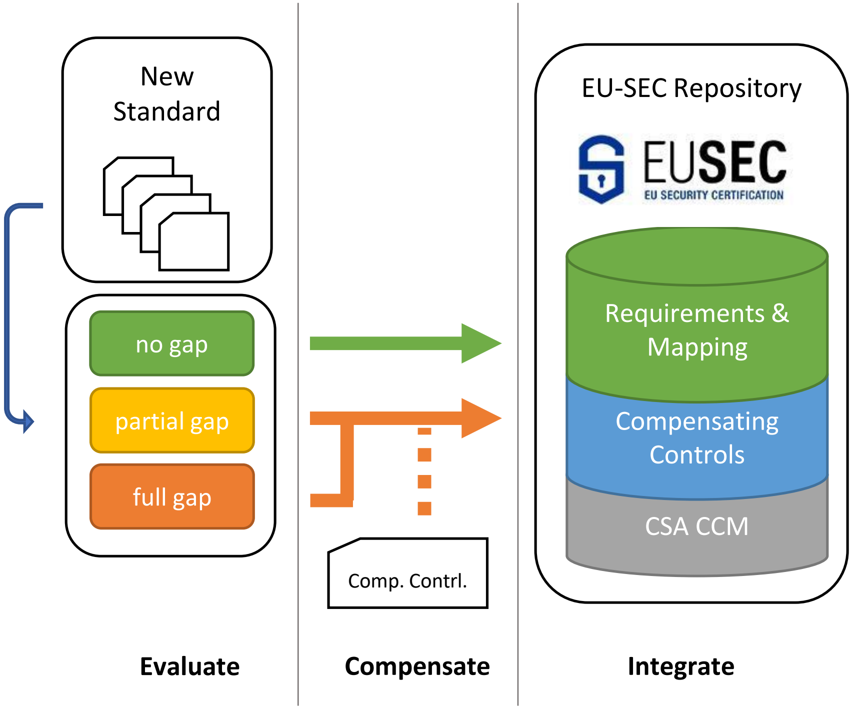
EU-SEC grant agreement no 731845

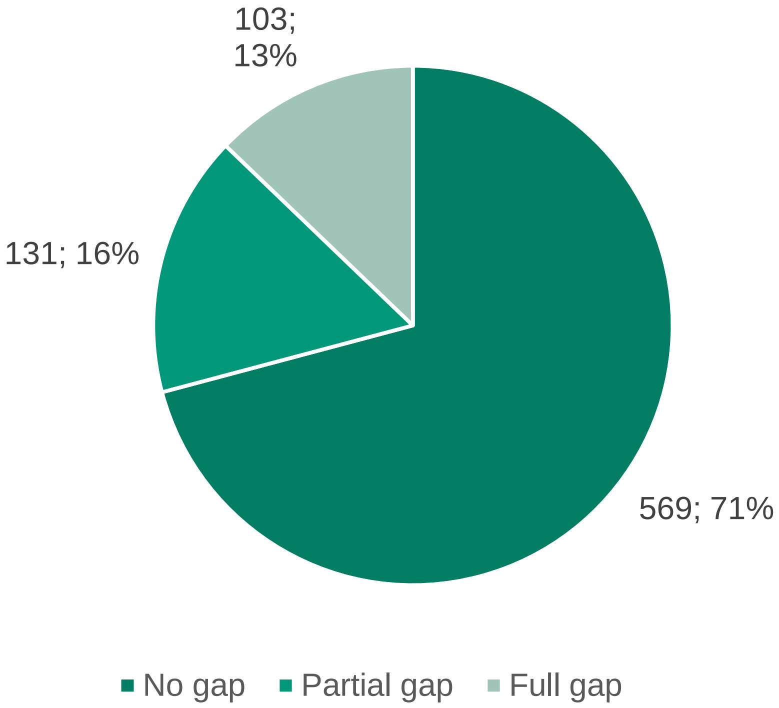
Multiparty Recognition Framework: Principles

	P1. The repeatability principle	P2. The equivalence principle	P3. The relevancy principle	P4. Trustworthiness principle
Certification scheme	Results of two audits of the same security/privacy requirements under the same scope and conditions should be the same.	Assessment of a requirement should provide the equivalent level of security/privacy in different IS.	Requirements and the associated processes used should be selected so as to provide actionable information to the auditee.	Collection, verification and evaluation of evidence against audit criteria should be transparent, unbiased, complete and unambiguous in order to provide a trustworthy representation of the security/privacy.
EU-SEC Framework	Results of a comparison of requirements of two certification schemes, under the same conditions should be the same.	Comparison of requirements between schemes should provide equivalent level of security/privacy.	Not applicable	Comparison of two schemes should be transparent, unbiased, complete and unambiguous in order to provide trustworthy results.

EU-SEC grant agreement no 731845

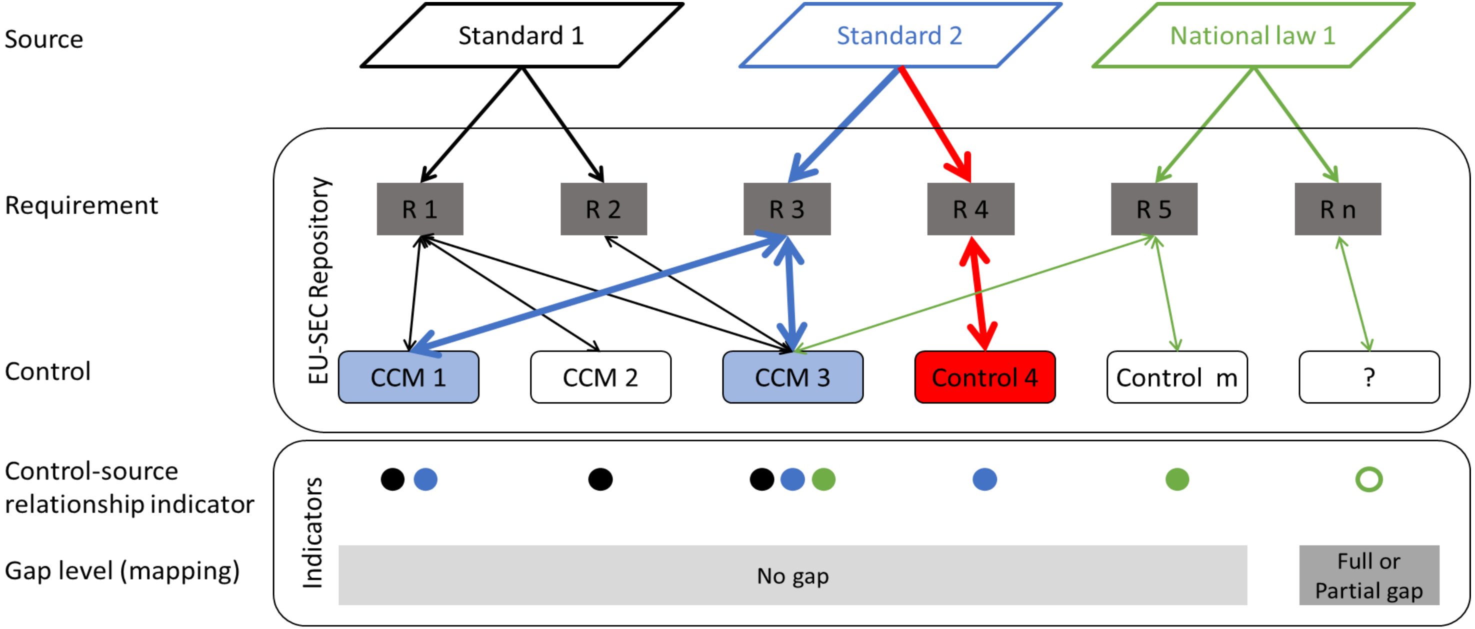
Multi Party Recognition Framework: Requirements Collection Process





EU-SEC grant agreement no 731845

Multiparty Recognition Framework: Application



↔ Requirements are covered by controls that have been implemented under other schemes > **recognition**

↔ Requirements need implementation of controls > **new compliance**

EU-SEC grant agreement no 731845

Multiparty Recognition Framework: Pilot

EUSEC
EU SECURITY CERTIFICATION

ISO auditor

nixu cybersecurity

ISAE auditor

pwc

REPUBLIC OF SLOVENIA
MINISTRY OF PUBLIC ADMINISTRATION

- SI-MPA holds an ISO27001 attestation
- Wants to assess compliance with ISO27017, CSA CCM and SI national requirements
- The audit's scope targets these Slovenian Government Cloud:
  - On-demand self service
  - Broad network access
  - Resource pooling
  - Rapid elasticity

Ministerstvo financií
Slovenskej republiky

- Starting from ISO27001, MFSR assesses compliance with ISO27017 CSA CCM and SK national requirements
- The SK national requirements are not fully established at the time of the audit
- The audit's scope targets the construction of G-Cloud in Slovakia and its IaaS services

sixsq

- Starting from ISO27001 SixSq assesses compliance with ISO27017 and CSA CCM
- Evidence Store is integrated with Nuvla, so SixSq also tests its readiness
- Being a digital service provider, SixSq has its audit's scope targeting the Development and Operations of software, products and services built inside the company

Fabasoft

- Fabasoft starts from a Star attestation and strives for compliance with BSI C5
- Focus on identifying gaps and non-conformities
- Need to consolidate and trust on the gap analysis

EU-SEC grant agreement no 731845

Fraunhofer
FOKUS

EU-SEC Continuous Auditing Based Certification

2

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

Fraunhofer
FOKUS

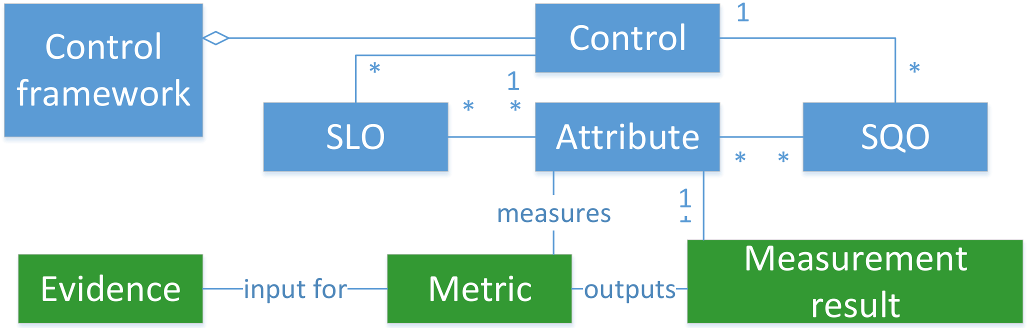
Continuous Auditing Based Certification: Problem Statement

- Security audits are usually performed **in a two year cycle** according to the requirements of the granted certificate.
  - creates a time window of uncertainty where no audit is performed.
  - cloud service customers do not have an up-to-date status on the fulfilment of the requirements, established by the certification goals.

- The continuous audit approach addresses this issue by providing a way of **continuously assessing the compliance status** for
  - regulations
  - requirements
  - controls

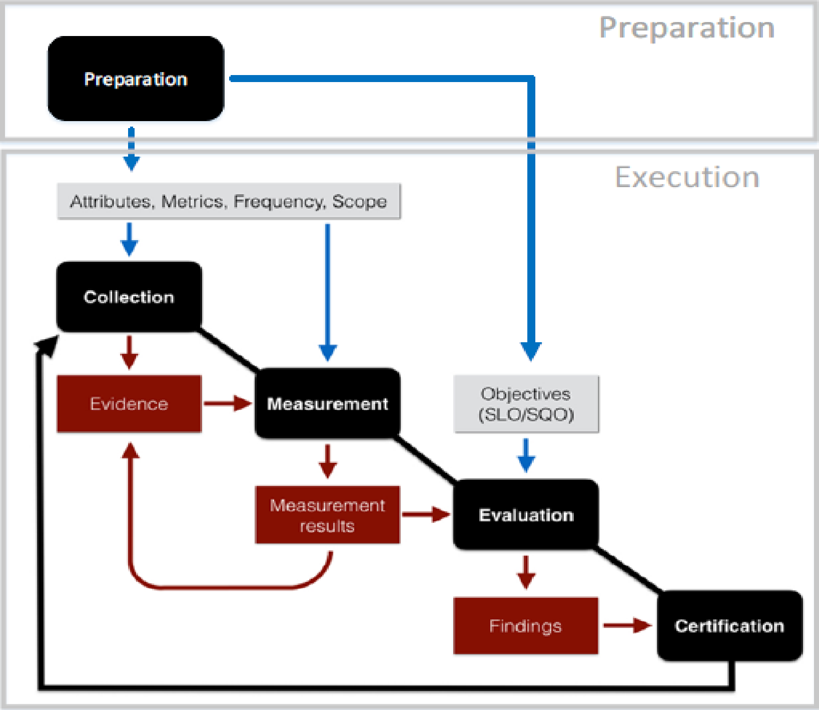
Continuous Auditing Based Certification: Approach (Control breakdown)

- The windows between audits/check is reduced and matches with the nature of the requirement/security property to be verified.
- Controls will be checked on a hourly, daily, weekly or monthly basis depending on their criticality and nature.
- Use automation wherever possible
- Develop fallbacks for human assessments when needed.
- Provide a model for breaking down controls into measurable objectives



Continuous Auditing Based Certification: Process Model

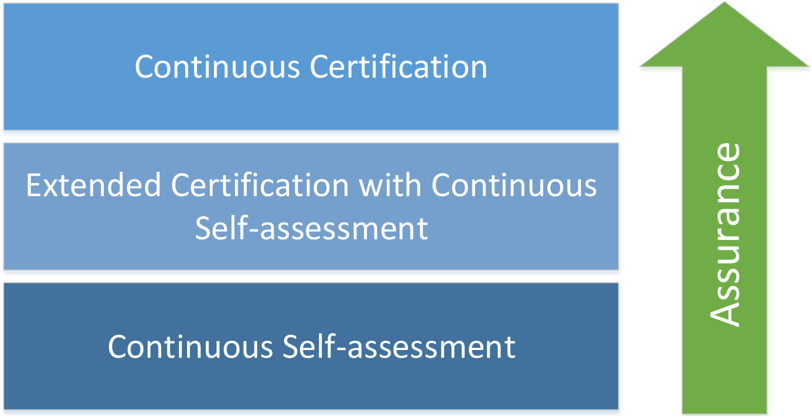
- **Preparation**: Identification of the objectives (SQO, SLO), frequencies, attributes and metrics, as well as the measurements points
- **Collection:** Collection of raw data
- **Measurement:** Transform the collected raw data into usable measurement results
- **Evaluation:** Compile information on controls from attributes and document findings
- **Certification:** Publish results according to the chosen continuous auditing certification scheme (i.e. *Continues Self-assessment*, *Extended Certification with Continuous Self-assessment*, *Continuous Certification*)



EU-SEC grant agreement no 731845

Continuous Auditing Based Certification: **Assurance Level**

EU-SEC project proposes a framework that contains three models for continuous auditing.


Continuous Certification
Extended Certification with Continuous Self-assessment
Continuous Self-assessment
Assurance

Each of three models provides a different level of assurance by covering requirements of continuous auditing with various levels of scrutiny.

EU-SEC grant agreement no 731845

Continuous Auditing Based Certification:

Conclusion and Future Work

- Increased audit frequency with low overhead
- Not bound to a specific standard
- Extremely relevant for specific sectors like banking or health
- Reduction of high implementation efforts by defining a clear and simple API
- *Still more cost intensive that a traditional audit.*
- *Just 25% of the Controls in current standards are fully automatable.*
- **Need for further research and development**
  - Level of automation has to be increased.
  - Natural Language Processing
  - DSL for Security controls and requirements

Thank you for your attention!

EUSEC
EU SECURITY CERTIFICATION

Visit www.sec-cert.eu

- Project deliverables and news
- Invitations to view progress and provide feedback at national and European stakeholder events
- Guidelines and trainings on the European certification framework

Newsletter subscription: www.sec-cert.eu/

Contact: contact@sec-cert.eu

Project Coordinator

Jürgen Großmann

Email: juergen.grossmann@fokus.fraunhofer.de

Fraunhofer FOKUS, Berlin, Germany

Phone: +49 (0)30 3463 7390

Join our Workshops:
CABC, Berlin, October 8th, 2019
MPRF, Berlin, October 9th, 2019

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

Fraunhofer
FOKUS