EU-SEC Awareness Workshop
Continuous Auditing-based Certification

Barcelona

9th Apr 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.

Agenda

Time	Session	Speaker(s)
9:30 – 10:00	**Presentation and EU-SEC Introduction**	Jürgen Großmann
10:00 – 10:50	**Description of the pilot and CA theoretical model**	Ramon Martín de Pozuelo
10:50 – 11:10	***Coffee Break***	
11:10 – 12:20	**CA technical architecture and demo**	Christian Banse, Dorian Knoblauch, Björn Fanta, Cristóvão Cordeiro, Alain Pannetrat
12:20 – 13:15	**Round-table discussion (Questions and Answers)**	Ramon Martín de Pozuelo
13:15 – 14:30	***Lunch Break***	
14:30 – 15:30	**Hands-on Lab**	Christian Banse, Dorian Knoblauch, Björn Fanta, Cristóvão Cordeiro, Alain Pannetrat
15:30 – 16:00	**Closing**	Jürgen Großmann

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

Introduction to EU-SEC

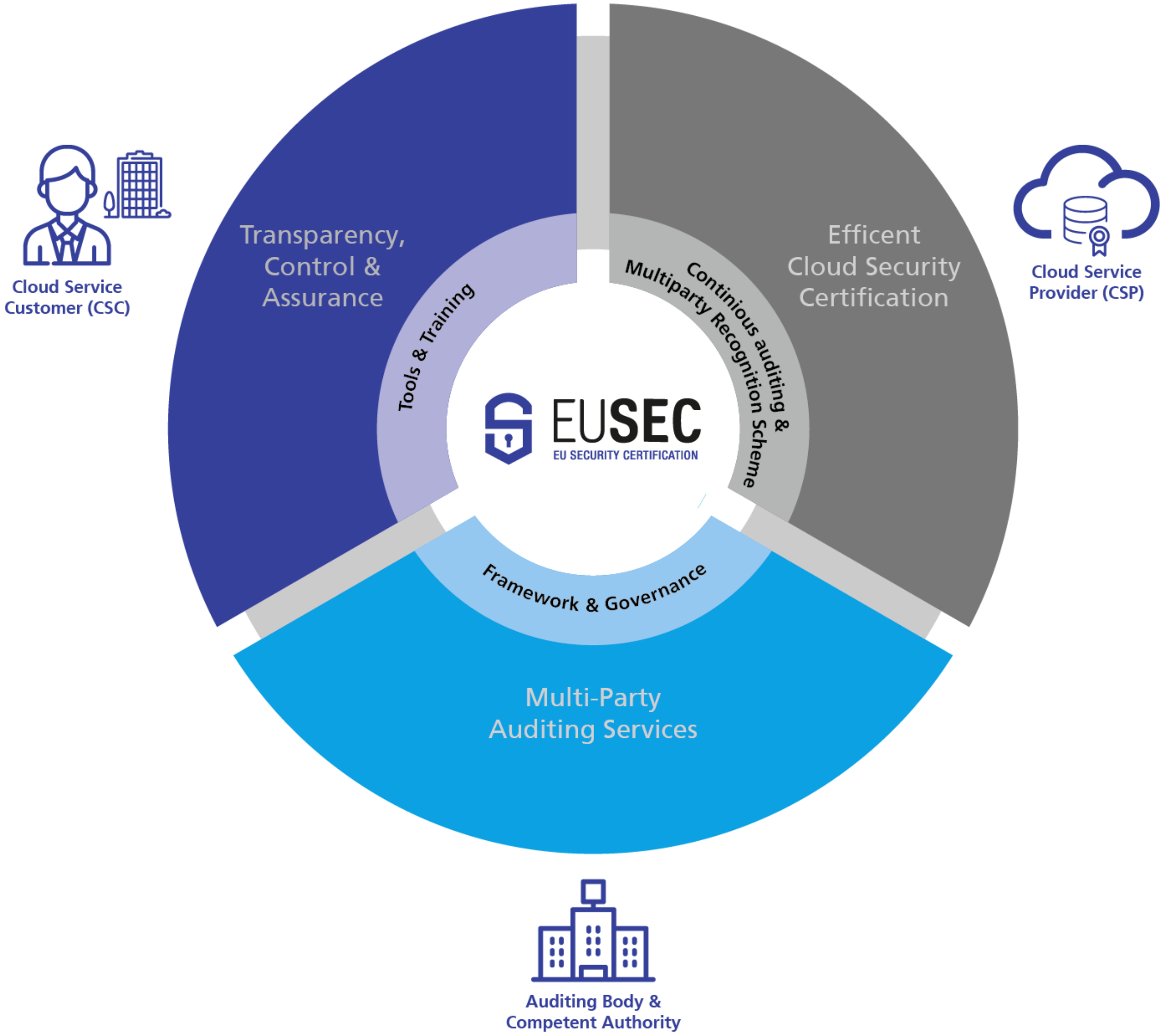
Jürgen Großmann (FRAUNHOFER)

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

Trust in Cloud by Certification
The European Security Certification Framework (EU-SEC)

EU-SEC aims 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 Certification (CAC)**
- **Governance Structure** for trustful and compliant use of cloud computing


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

9th April 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.

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.
- Stream line governance, risk management and compliance of cloud service delivering a reference architecture, mechanisms and tools for continuous auditing and certification reducing human interaction.
- Initiate 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 to support EU-SEC's long term sustainability.

CC0 1.0 Universal (CC0 1.0) Public Domain Dedication

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

EU-SEC Challenges

Achieving applicability, flexibility and tool support

- Ensure broad and international and cross-industry applicability of EU-SEC framework.
- Demonstrate a high level of security and privacy assurance and control while the CSP enhances the Cloud Service continuously.
- Provide a framework which can be adapted to new technical, compliance and market requirements, easily and promptly.
- Generate a flexible and functional architecture and tools for cloud security governance, risk management and compliance.

The U.S. National Archives

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

EU-SEC Activities
Define, evaluate, improve and maintain the framework

- Collect and maintain security and privacy requirements relevant to the public and private sector.
- Define the continuous auditing and certification framework and enable it for mutual recognition of existing certification and assurance approaches.
- Develop a governance structure to support trans-European EU-SEC framework adoption. Provide architecture and adapt existing tools to facilitate continuous auditing and control of security and privacy level service.
- Validate the framework with pilot use cases executed by public and private sector partners to ensure its effectiveness, efficiency and market readiness in large-scale demonstrators.
- Strengthen the value proposition, market uptake and long-term sustainability of EU-SEC framework through commercial exploitation, influencing other standardization initiatives and performing strategic awareness and training activities.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under 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 (including CSPs, Cloud Users, Auditors, Scheme Owners and Researchers)

Duration: January 2017 - December 2019

Web: https://www.sec-cert.eu/
Contact: *contact@sec-cert.eu*
Twitter: @EU_SEC

CaixaBank

cloud security alliance® CSA

Fabasoft

Fraunhofer FOKUS

Fraunhofer AISEC

MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

nixu cybersecurity.

pwc | Deutschland

sixsq

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

EU-SEC Goes Public

Workshops and trainings planned throughout the year

EUSEC
EU SECURITY CERTIFICATION
Workshop on
Multi-Party Recognition between
Cloud Security Certifications
May 13
Amsterdam

Workshop on Multi-Party Recognition on 13 May 2019!
Date: Mon., May 13, 2019
Location: Amsterdam, Netherlands

EUSEC
EU SECURITY CERTIFICATION
Workshop on
Continuous Audit Based Certification
APR 09
Barcelona

Workshop on Continuous Auditing Based Certification
Date: Tue., Apr. 09, 2019
Location: Barcelona

Date	Topic	Location
13/05/2019	Training Workshop **MPRF**	Amsterdam
08/10/2019	Training Workshop **MPRF**	Berlin
09/10/2019	Training Workshop **CAC**	Berlin
18/11/2019	Joint Training Event **MPRF, CAC** at CSA EMEA Congress	Berlin
Q4/2019	Joint Training Event **MPRF, CAC**	Helsinki,
Q3 & Q 4 2019	Individual Training Events for **MPRF, CAC**	tba.
Q3 & Q 4 2019	Webinars **MPRF, CAC**	tba.

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

Description of the pilot and Continuous Auditing-based Certification theoretical model

Ramon Martín de Pozuelo (CAIXABANK)

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

Continuous Auditing-based Certification

Challenges of Cloud Certifications

- “Point-in-time” / “period-of-time” approaches to security certification do not provide the high assurance and transparency required by cloud stakeholders with high risk profiles .

- Currently, security audits are usually performed at intervals of 6 or 12 months
  - This 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 developed addresses this issue by providing a way of continuously assessing compliance status.

Designed by fullvector / Freepik

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

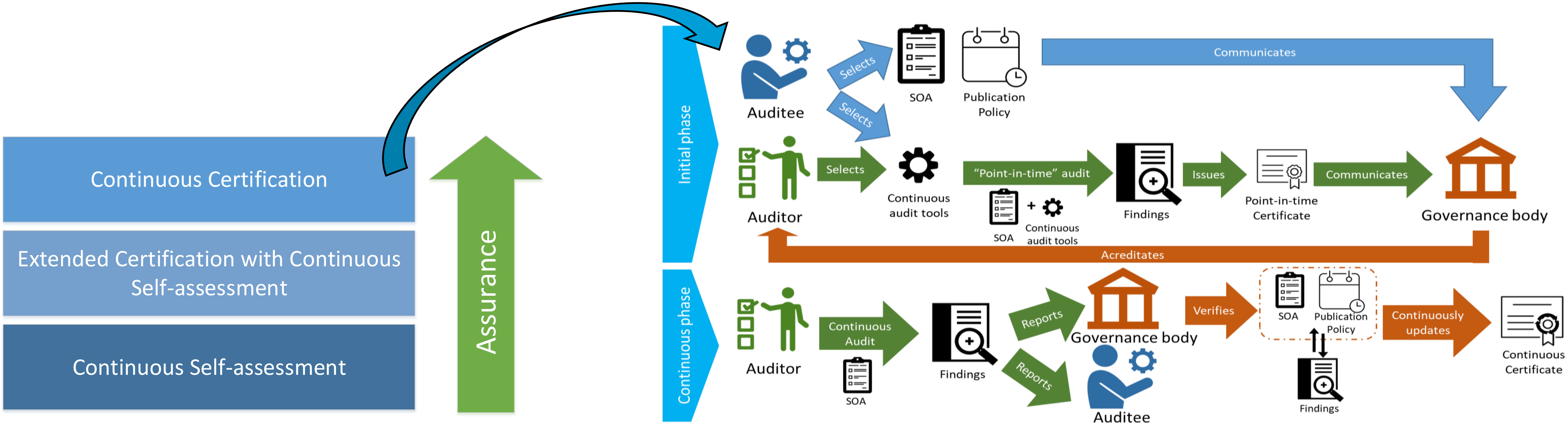
Continuous Auditing-based Certification
Models

Continuous Auditing: An **ongoing assessment process** that aims to determine the fulfilment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.

Continuous Certification: An information system is said to be the state of continuous certification if it **meets a predefined set of SQOs and SLOs**, which have been **verified through continuous auditing**.

EU-SEC project proposes a framework that contains **three models** for Continuous Auditing-based Certification.

Each of these models provides a **different level of assurance** by meeting requirements of continuous auditing with various levels of scrutiny.

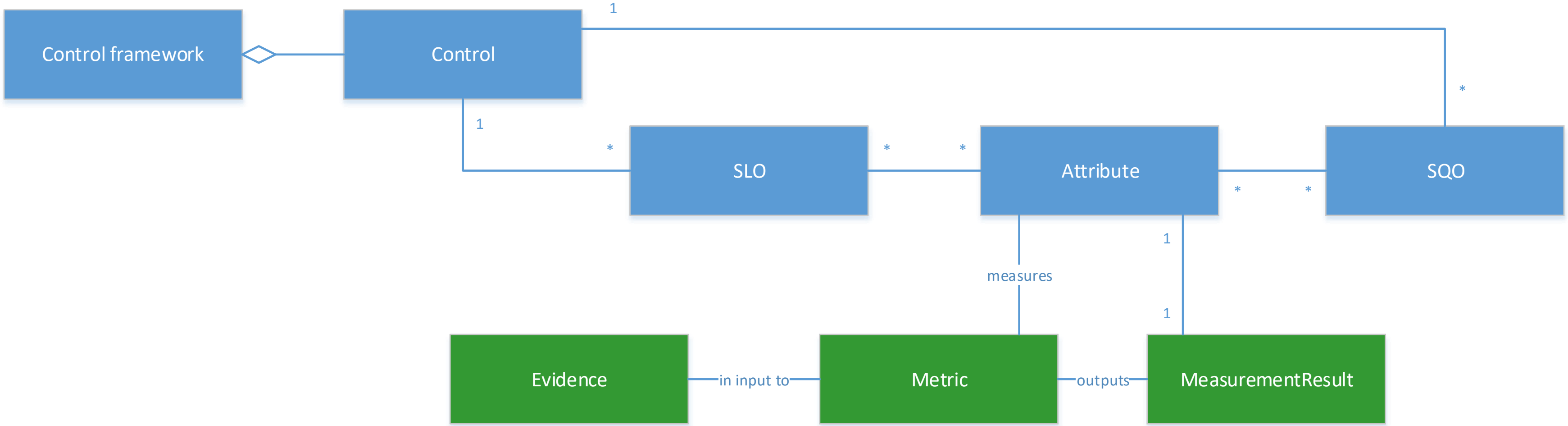


9th April 2019

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

Continuous Auditing-based Certification
Methodology – Control Breakdown

- The window between audits/check is reduced and matches with the nature of the requirement/security property to be verified.
- Controls can 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

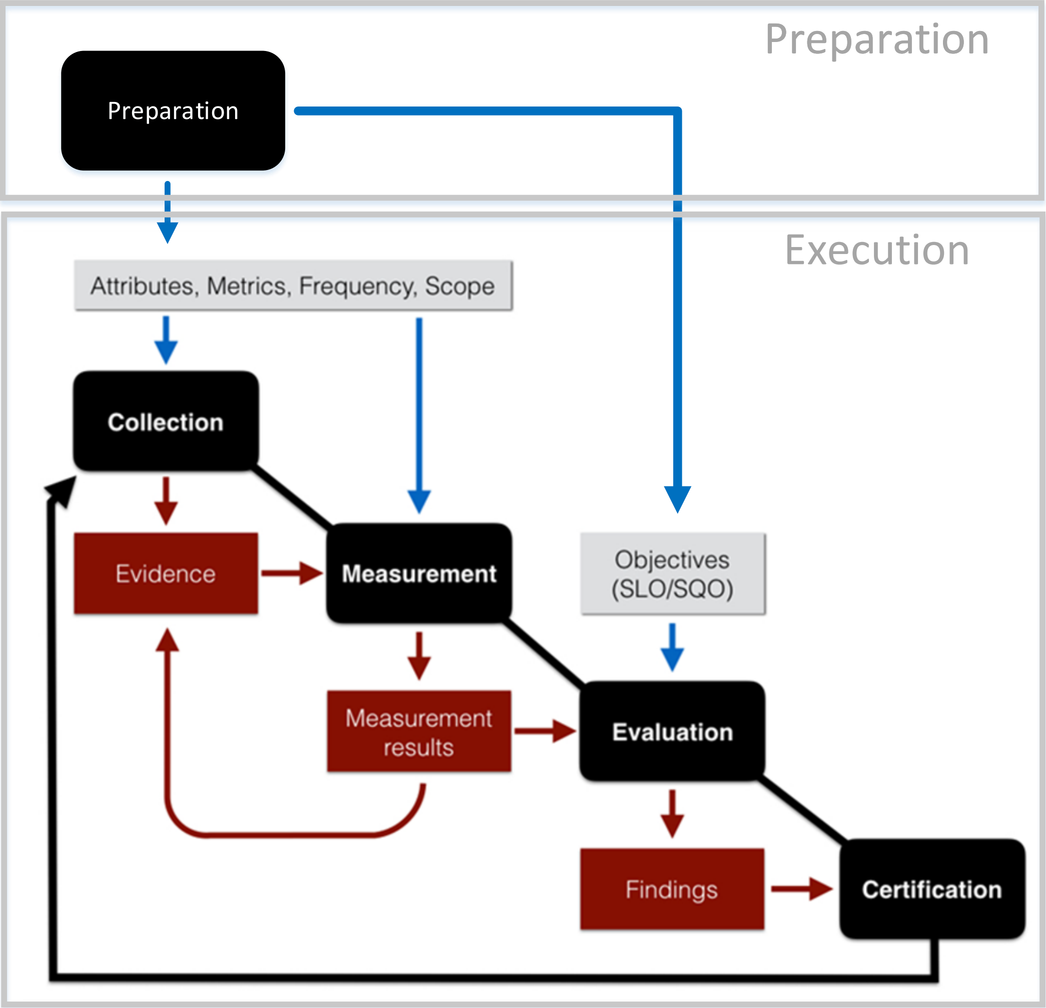


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification
Methodology – phases

- Continuous Auditing-based Certification consists of 5 phases:

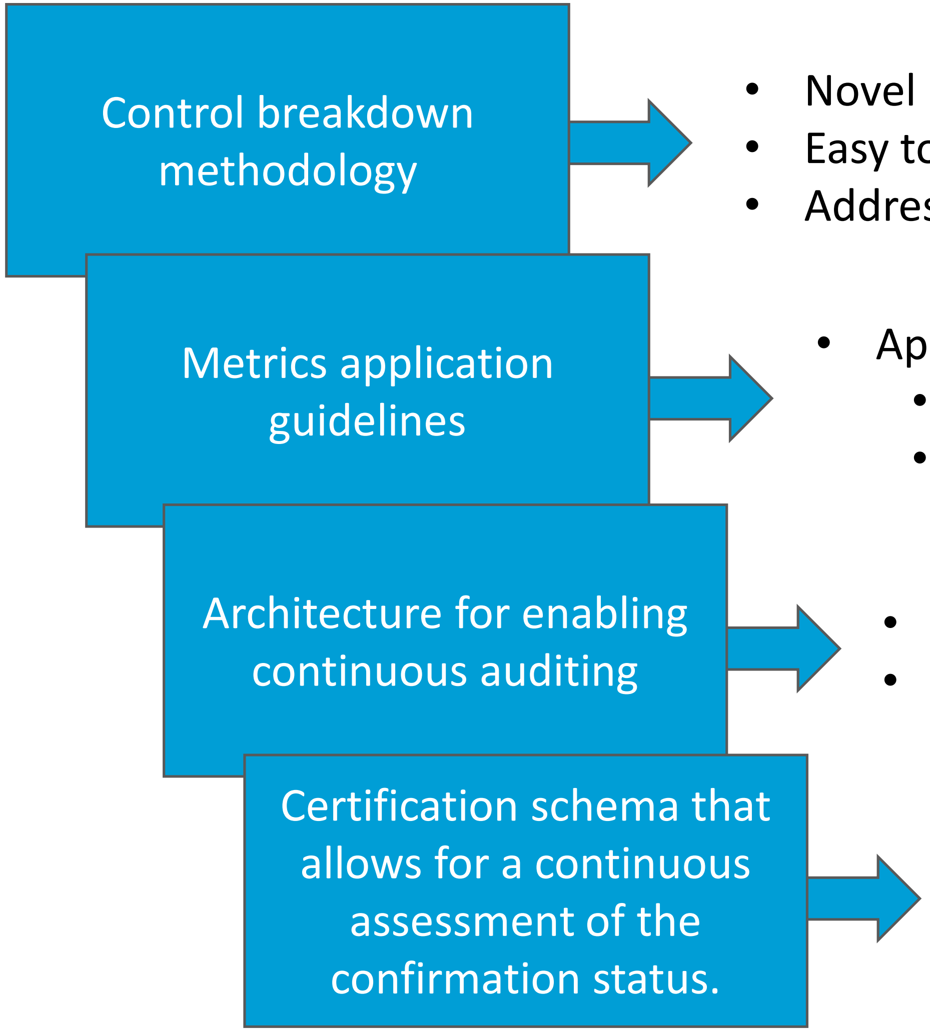
1. Preparation: mainly devoted to the operationalisation of the controls
   - This initial setup is performed once
   - SLO's and SQO's are defined to describe controls
   - The output are:
     - Objectives = constraints on attributes
     - Metrics for assessing the attributes
     - Objective assessment frequency
     - Scope of the assessment.
2. Collection: devoted to the collection of evidence
3. Measurement: the metrics are applied to the collected evidence.
4. Evaluation: it checks if an objective is fulfilled.
5. Certification: according to the result of the evaluation, a certificate is granted or not.



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

Continuous Auditing-based Certification

Scheme definition



Control breakdown methodology

- Novel methodology
- Easy to use
- Addresses automation and non automation

Metrics application guidelines

- Applicable for:
  - automatable measurements
  - manual measurements

Architecture for enabling continuous auditing

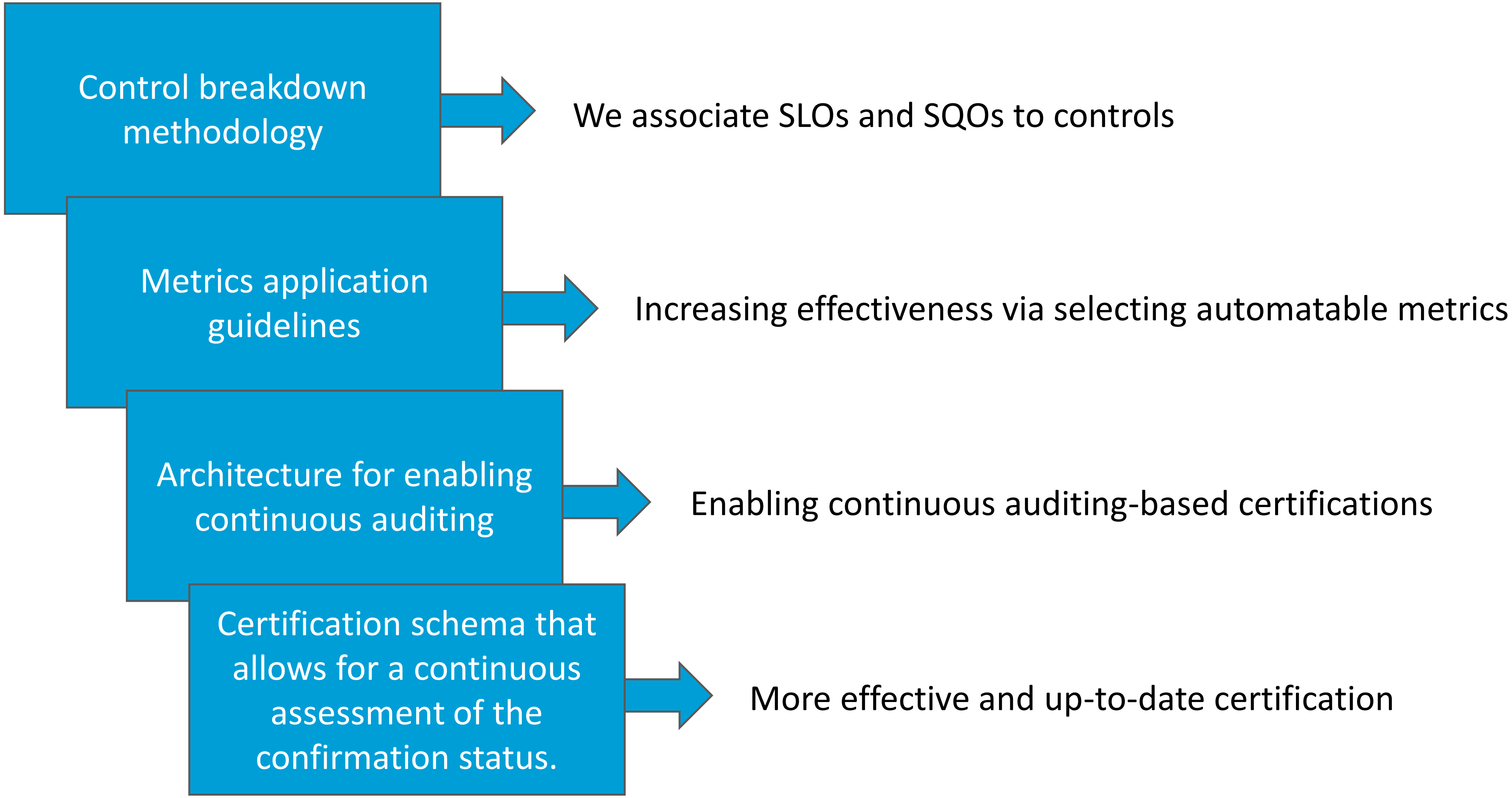
- Easy to implement phases
- Highly automatable process

Certification schema that allows for a continuous assessment of the confirmation status.

- User gets a constantly updated compliance status
- 3 Models with different degrees of assurance

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

Continuous Auditing-based Certification
Scheme definition



Control breakdown methodology → We associate SLOs and SQOs to controls

Metrics application guidelines → Increasing effectiveness via selecting automatable metrics

Architecture for enabling continuous auditing → Enabling continuous auditing-based certifications

Certification schema that allows for a continuous assessment of the confirmation status. → More effective and up-to-date certification

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

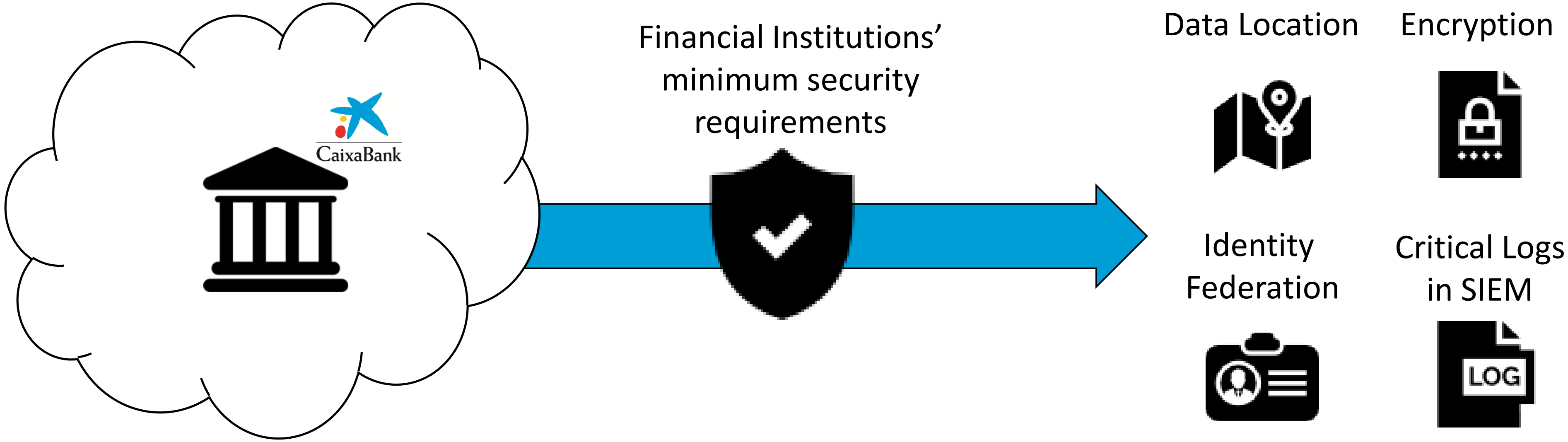
Description of the Pilot
Introduction

EUSEC
EU SECURITY CERTIFICATION

Trusted information sharing — Financial institutions need to report sensible information to the regulators in a reliable and trusted way.

Collaboration — In some cases, this exchange of information can involve multiple entities and organisations.

Industrial gap motivation: Lack of a continuous auditing service that verifies that the cloud provider running the information sharing service actually complies with Financial Institutions' requirements.



CaixaBank

Financial Institutions' minimum security requirements

Data Location

Encryption

Identity Federation

Critical Logs in SIEM

Goal: Continuous auditing of security requirements in a **Financial Information SHaring (FISH)** application with EU-SEC platform.

9th April 2019

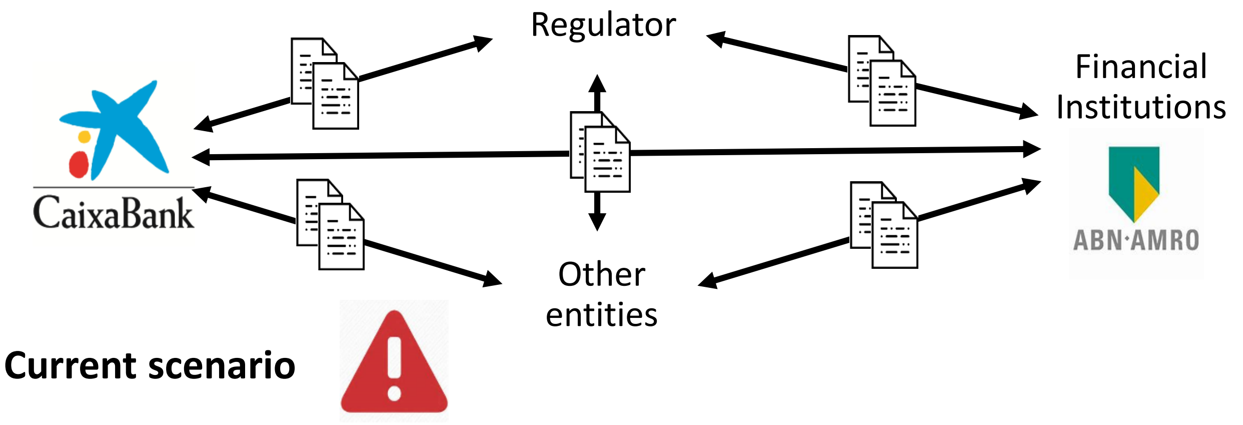
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Description of the Pilot
Introduction

Current scenario and problem statement:

- Regulatory entities **require banks to share information.**
- **Regulators may ask CaixaBank for confidential information** of accounts:
  - **Incident reporting** with information of mule accounts for fraud and money laundering, terrorism, etc.
  - **Periodic reports** about security and privacy projects and procedures.

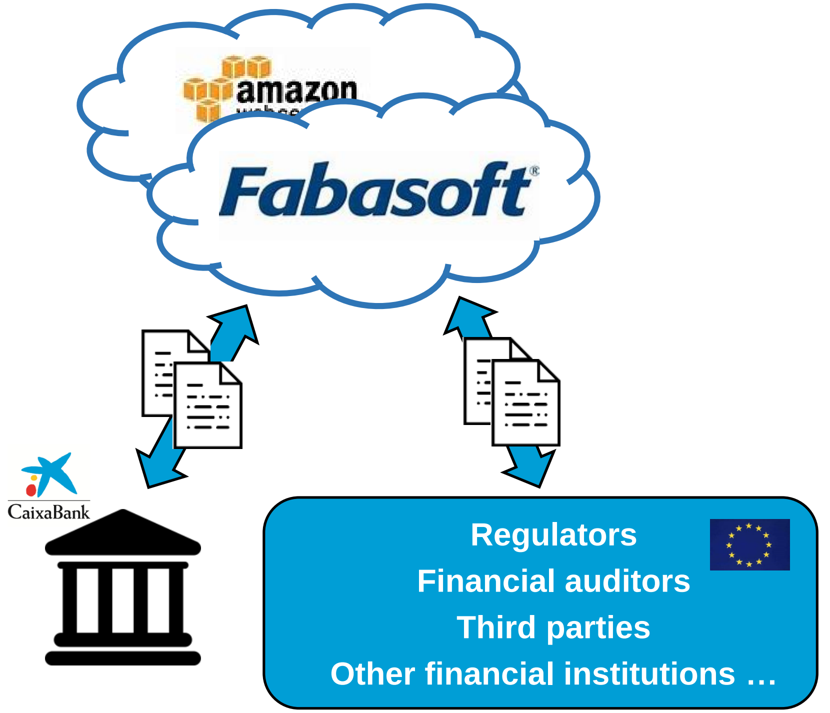
- Information is **shared across groups of regulators/banks**:
  - A simple repository hosted by a bank cannot be trusted by others.
- This may lead to **bad practices and/or onerous document management**:
  - Report sensitive information via mail, physical sharing of information,…



FISH: Neutral European service used by both financial entities and regulators.

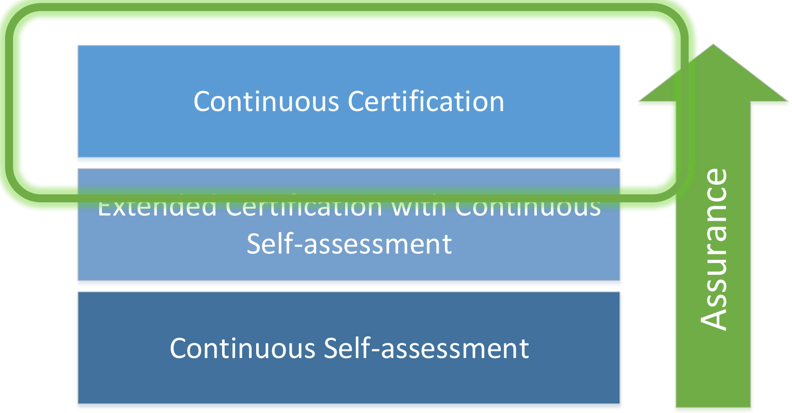
Pilot 2 different approaches:

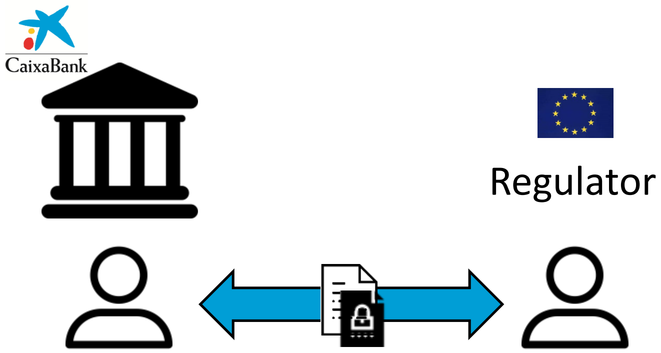
- Custom-tailored FISH over commercial cloud provider (IaaS).
- Fabasoft as a cloud platform for information sharing (SaaS).



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

Description of the Pilot
Definition


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

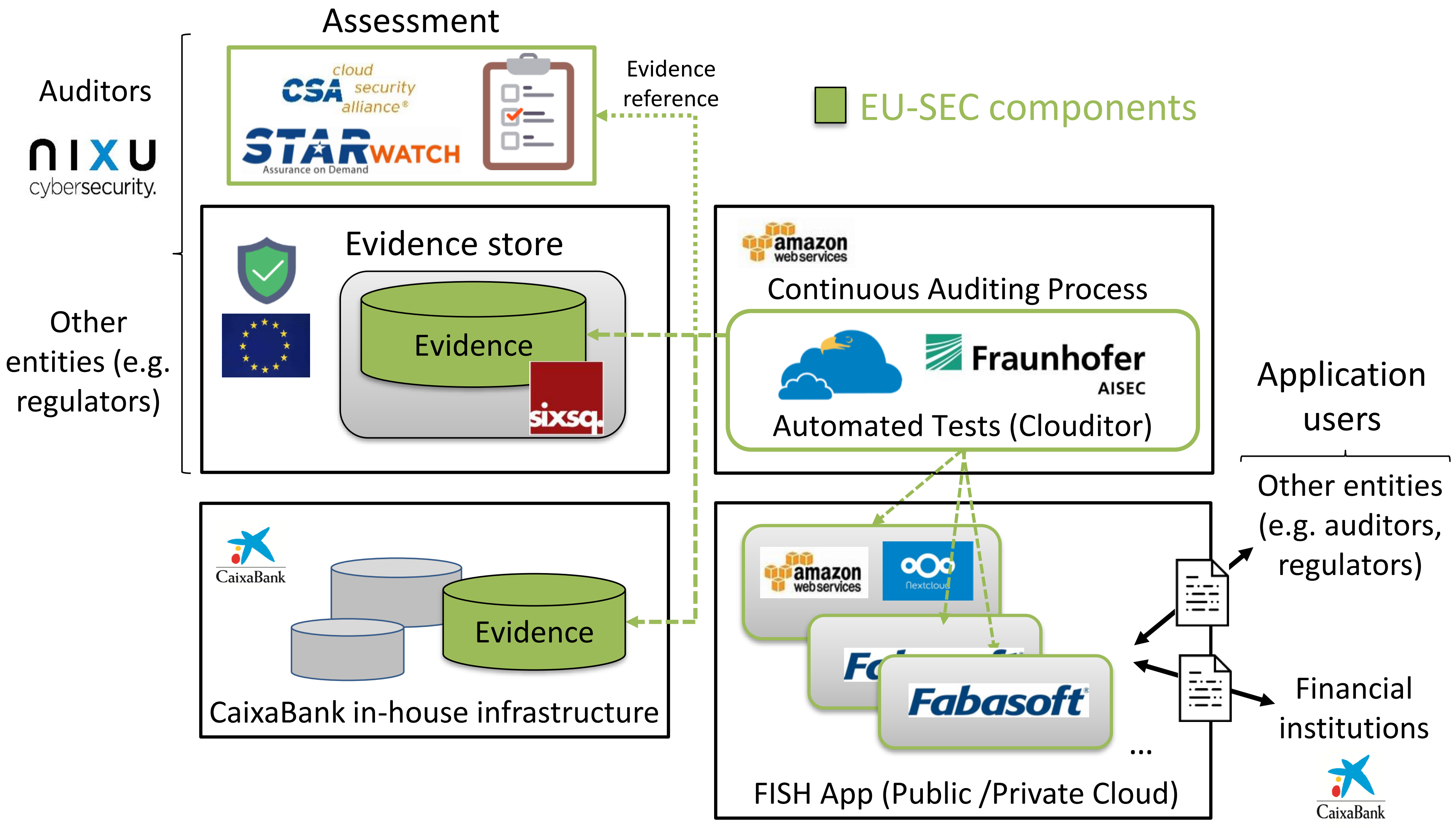


Secure exchange of messages and files

Requirements	Control	CCM code
Data location	The location of all sensitive data and its usage by applications and databases should be known. Moreover, all data should be located within European Economic Space.	CCM-GRM-02, CCM-STA-05
Encryption	All data should be encrypted both at rest and in transit. Cryptographic key management policies and procedures should be defined.	CCM-EKM-04, CCM-EKM-02
Identity Federation	Strong authentication of admin users. Access control and admin profiles should be defined.	CCM-IAM-12
Critical logs in SIEM	All monitoring and evidences logs should be stored in CaixaBank infrastructure.	CCM-IVS-01

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

Description of the Pilot
Architecture



Assessment

Auditors

nixu cybersecurity.

Other entities (e.g. regulators)

cloud security alliance® CSA

STARWATCH Assurance on Demand

Evidence reference

🟩 EU-SEC components

Evidence store

Evidence

sixsq

amazon web services

Continuous Auditing Process

Fraunhofer AISEC

Automated Tests (Clouditor)

Application users

Other entities (e.g. auditors, regulators)

CaixaBank

Evidence

CaixaBank in-house infrastructure

amazon web services

Nextcloud

Fabasoft

…

FISH App (Public /Private Cloud)

Financial institutions

CaixaBank

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

Description of the Pilot
Continuous Auditing API and pilot approaches

- **Continuous Audit API**
  - **CaApiDataLocation**

    GET /{scope}/datalocation/{objectId}/storage/
  - **CaApiEncryption**

    GET /{scope}/encryption/{objectId}/
  - **CaApiIam**

    GET /{scope}/identityfederation/admins/

    POST /{scope}/identityfederation/data/access

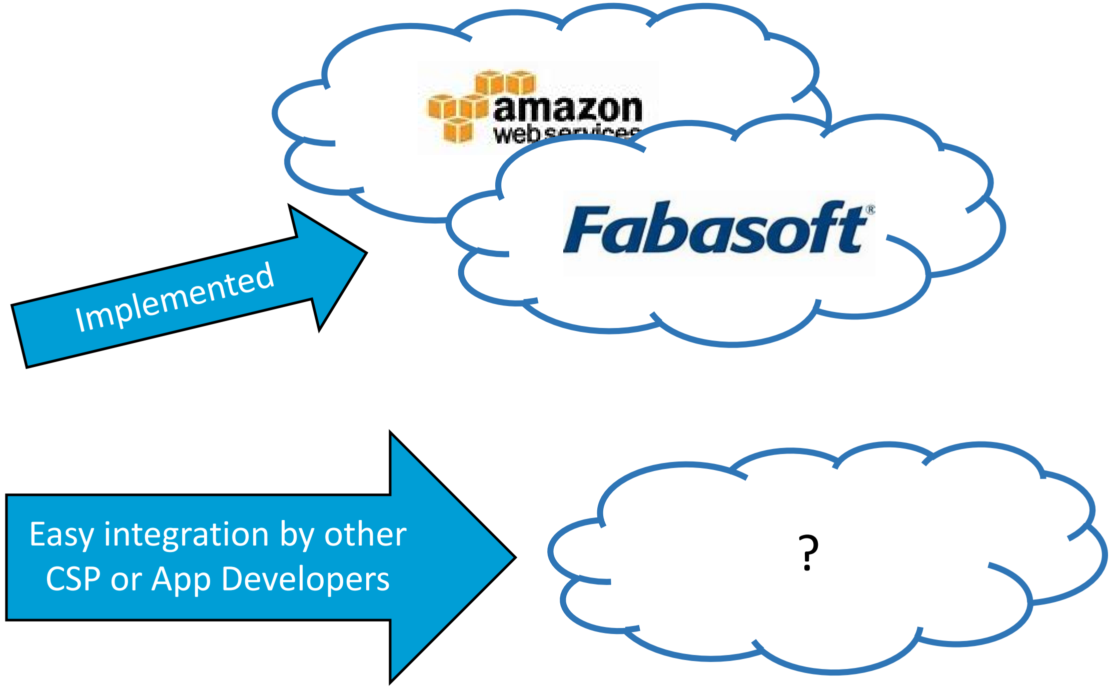
    GET /{scope}/identityfederation/{userId}/logins

    GET /{scope}/identityfederation/{userId}/auth

    GET /{scope}/identityfederation/{userId}/groups
  - **CaApiScope**

    GET /scope/

  …



Implemented

Easy integration by other CSP or App Developers

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

Continuous Auditing-based Certification Pilot
Conclusions

EUSEC
EU SECURITY CERTIFICATION

Value proposition & benefits:

Different actors and perspectives

Scheme Owner

Assurance and transparency

Continuous certification framework

- Methodology
- Implementation guidance
  - - Free material
  - - Paid training

Public registry of excellence

Auditor / Consultant

Computer-assisted, automated auditing

- **Increase productivity**
- **Extend the auditing services**
  - Guidance
  - Support
  - Training

Cloud Service Provider

Real-time & automated security control checking

Save money (on the long run)

Competitive advantage from “big players”

Proof of Trustworthiness

- Quality / Professionalism label
- Easier cooperation / partnerships

Cloud Customer

Certification

- Compliance to regulators

Easier Cloud Service adoption

Cost reduction

Demonstrate trustworthiness to own customers

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

Continuous Auditing-based Certification Pilot
Conclusions

- **First step towards the Continuous Auditing based Certification.**
  - Framework & governance model defined.
  - Reference architecture and modules implemented and deployed.
  - FISH use case tested within EU-SEC partners and external stakeholders.

- **Flexibility to define the audit controls and the way to store evidence records.**

- **It does not completely substitute point-in-time auditing.**
- **Still needs some trust on the CSP and the contract with the customer.**

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

Continuous Auditing-based Certification Pilot
Strong partners allow for commercial kick off

- **CSA**: Long term provision and maintenance of the Continuous Auditing-based Certification scheme
- **NIXU, PWC:** Provision of consultancy and audit services dedicated to Continuous Auditing-based Certification
- **Fraunhofer, SIXSQ and CSA**: Provision of tool to drive the operationalization
  - StarRegistry: Mean to publish and maintain Certificates from Continuous Auditing-based Certifications.
  - Clouditor: Cloud Compliance Tool to automatically check the compliance status of a cloud service.
  - Nuvla: Portal for the management and analysis of evidence records, both for supporting the continuous auditing process and for rapid visual assessment of compliance.
  - Continuous Auditing API: Standardized access to Cloud Service Provider security controls information
- **Fabasoft, CAIXA:** Initial adopters of the Continuous Auditing-based Certification

CaixaBank   CSA cloud security alliance®   Fabasoft

Fraunhofer FOKUS   Fraunhofer AISEC   sixsq   nixu cybersecurity.   pwc | Deutschland

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

Continuous Auditing-based Certification Pilot
References

- Deliverables
  - EU-SEC D2.2 – Continuous Auditing Certification Scheme
  - EU-SEC D5.1 – Pilot Definition

- White Paper
  - Continuous Auditing based Certification white paper

- Scientific Papers
  - Continuous Location Validation of Cloud Service Components
  - A Process Model to Support Continuous Certification of Cloud Services
  - Towards Continuous Security Certification of SaaS Applications Using Web Application Testing Techniques
  - Evaluating the Performance of Continuous Test-based Cloud Service Certification

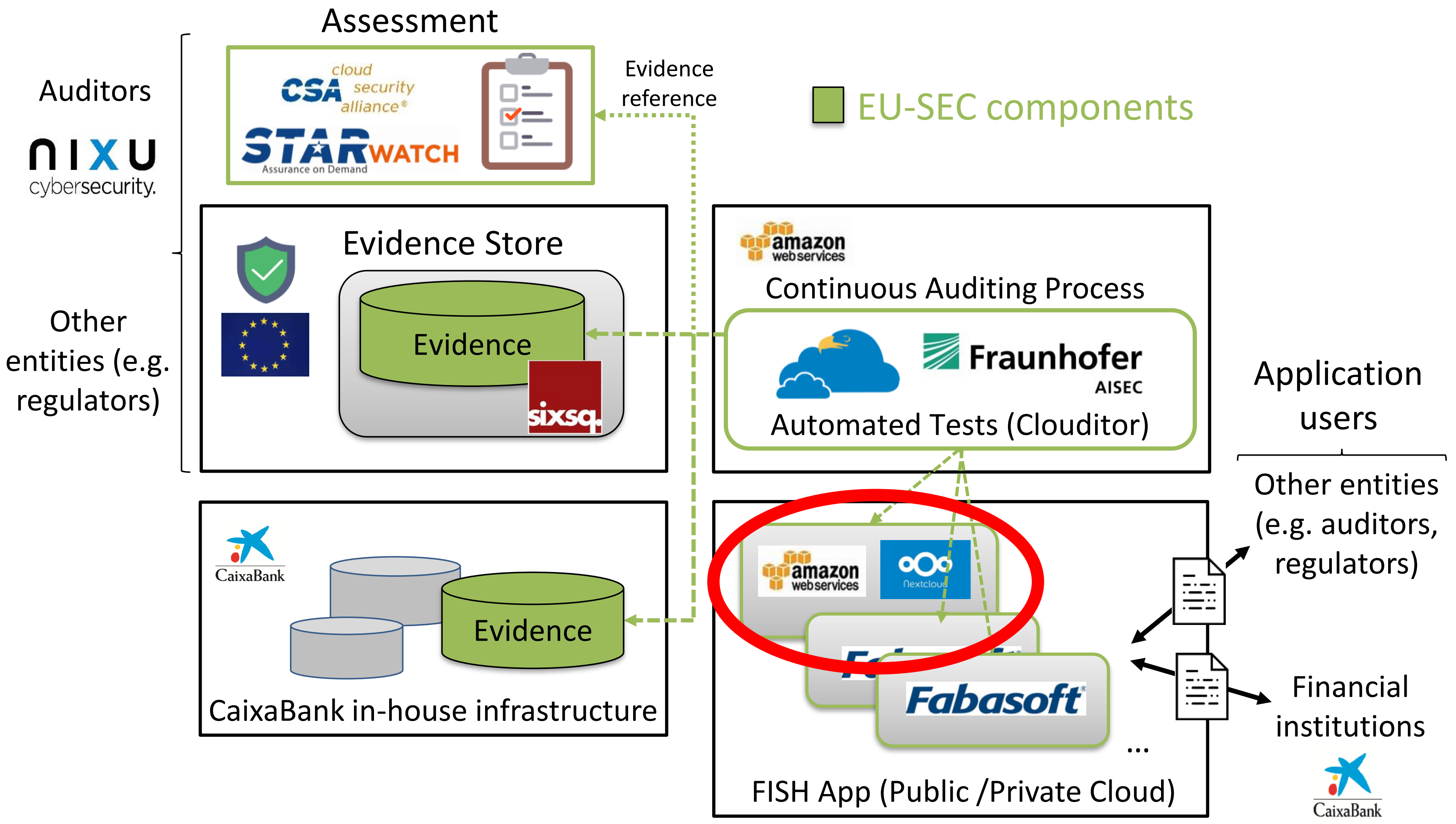
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing Technical Architecture & Demo

Christian Banse (FRAUNHOFER), Dorian Knoblauch (FRAUNHOFER),
Björn Fanta (FABASOFT), Cristóvão Cordeiro (SIXSQ), Alain Pannetrat (CSA)

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

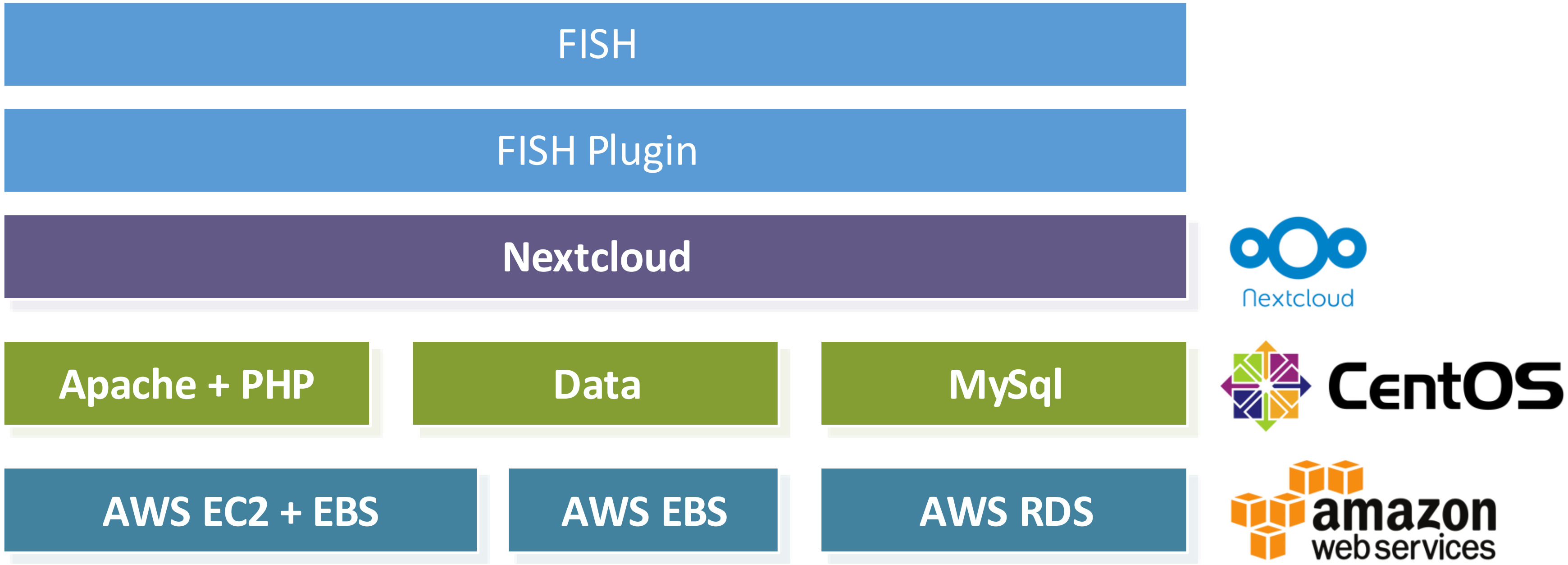
Continuous Auditing Technical Architecture
Introduction



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

Continuous Auditing Technical Architecture

FISH Application (IaaS approach)



FISH

FISH Plugin

Nextcloud

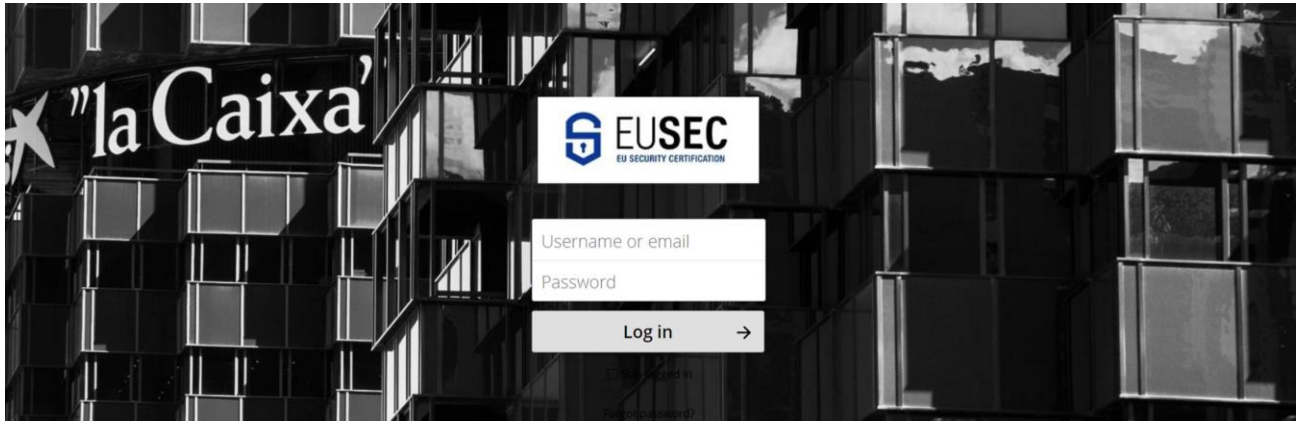
Apache + PHP | Data | MySql

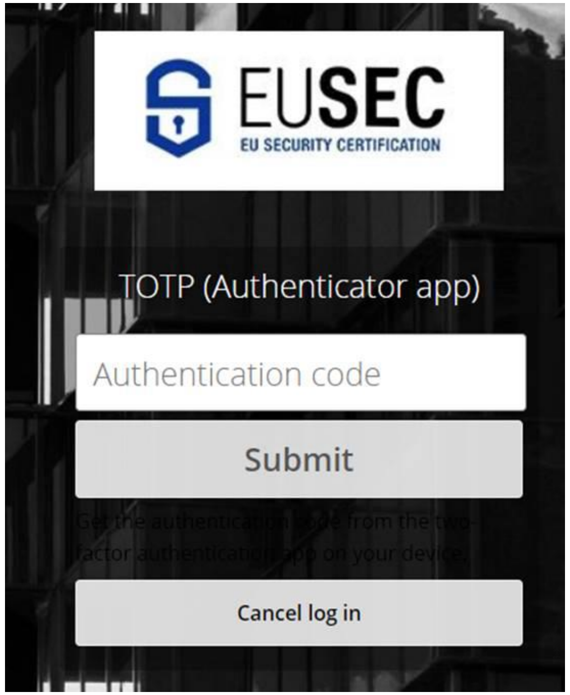
AWS EC2 + EBS | AWS EBS | AWS RDS

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

Continuous Auditing Technical Architecture

FISH Application (IaaS approach)





Get the authentication code from the two-factor authentication app on your device.

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

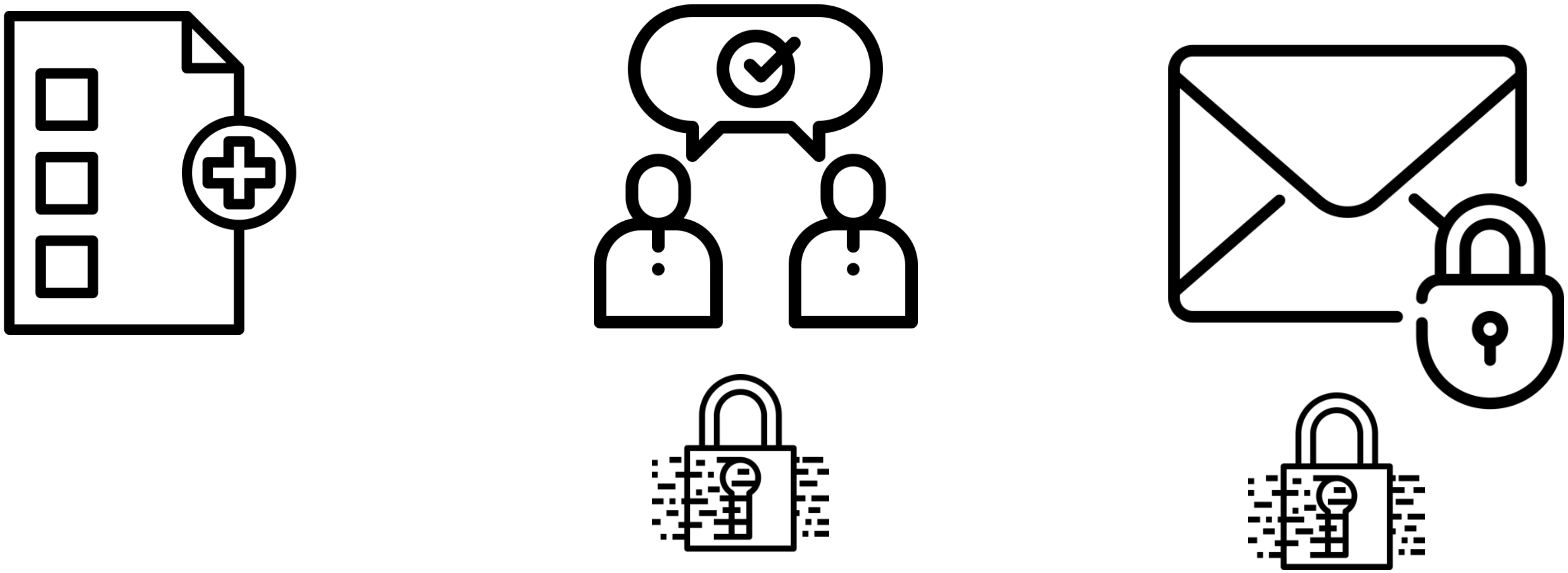
Continuous Auditing Technical Architecture

FISH Application (IaaS approach)

New case

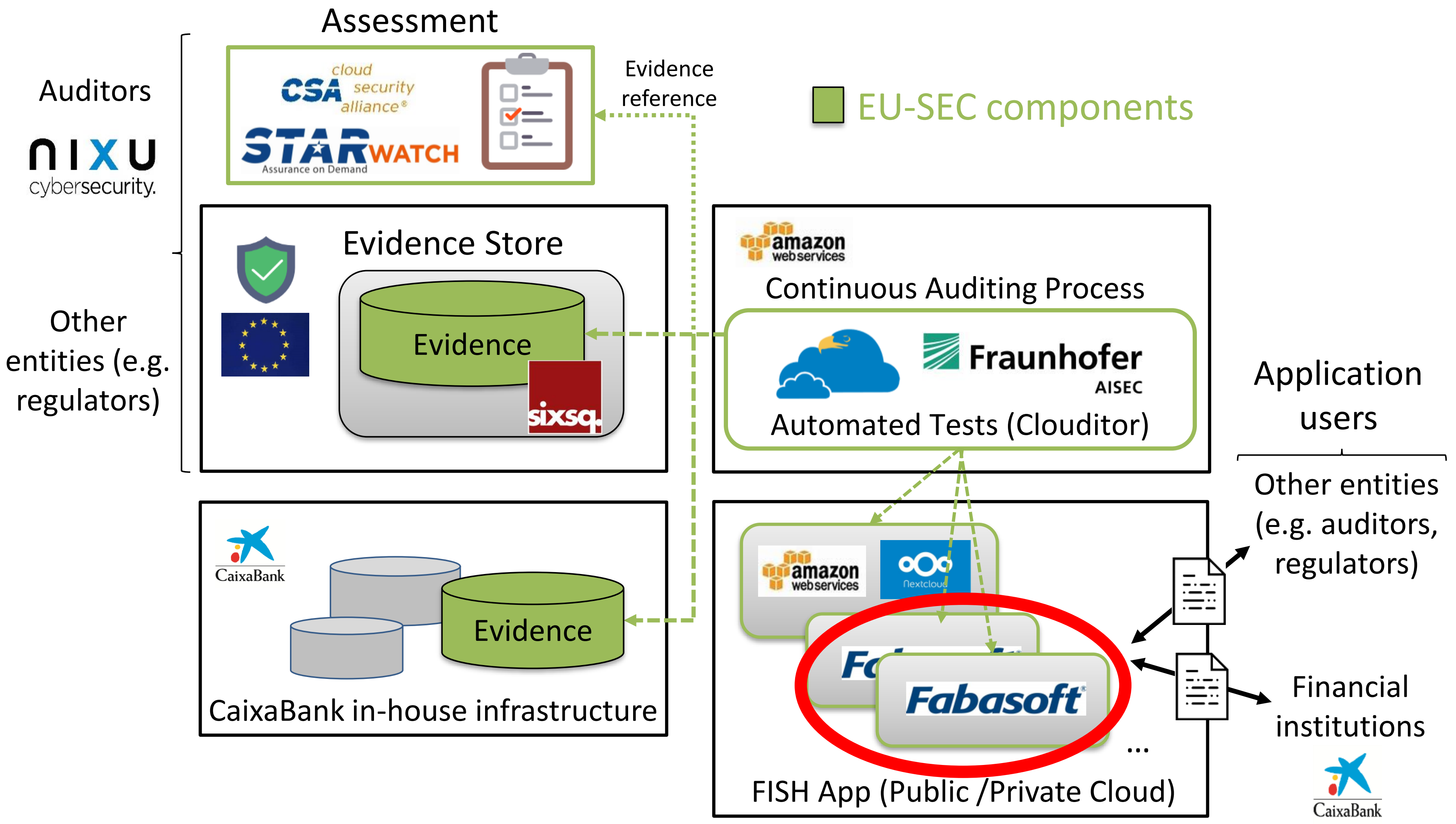
Agree which documents to exchange

Send file



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

Continuous Auditing Technical Architecture
FISH Application (SaaS approach)

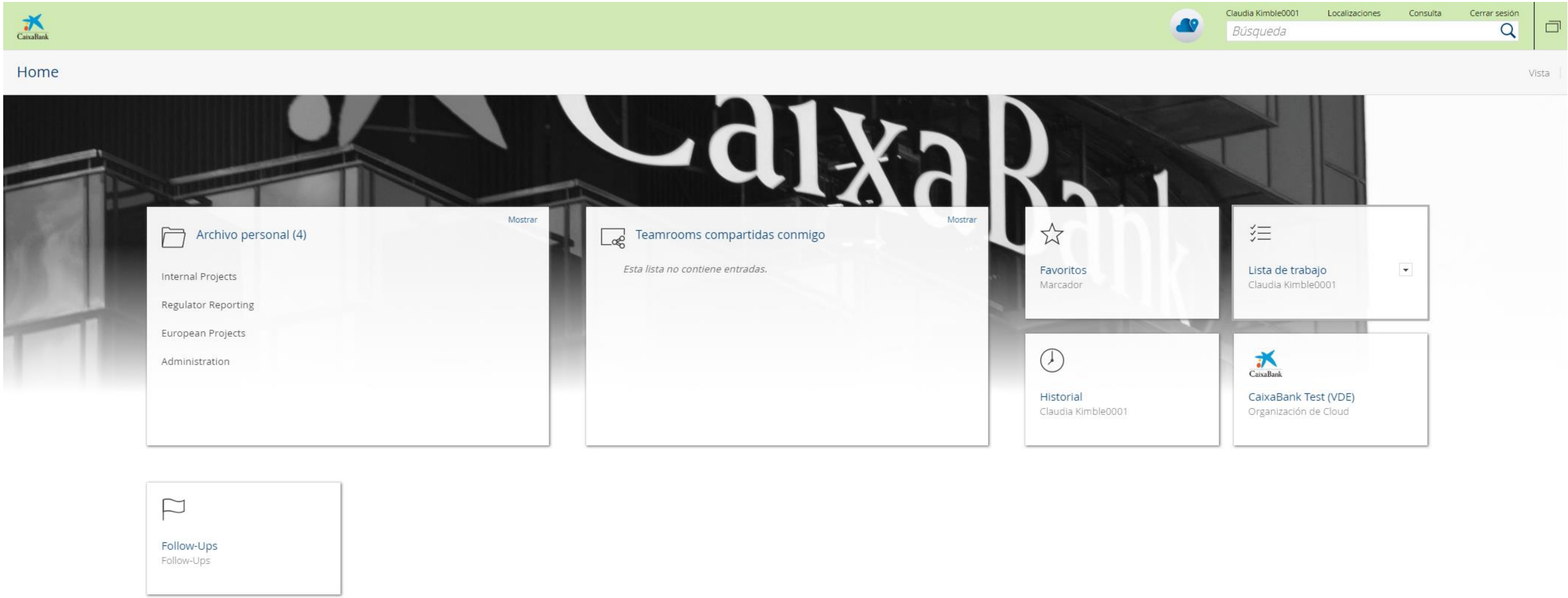


9th April 2019

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

Continuous Auditing Technical Architecture

FISH Application (SaaS approach)



CaixaBank

Claudia Kimble0001 Localizaciones Consulta Cerrar sesión

Búsqueda

Home

Vista

Archivo personal (4) Mostrar

- Internal Projects
- Regulator Reporting
- European Projects
- Administration

Teamrooms compartidas conmigo Mostrar

Esta lista no contiene entradas.

Favoritos
Marcador

Lista de trabajo
Claudia Kimble0001

Historial
Claudia Kimble0001

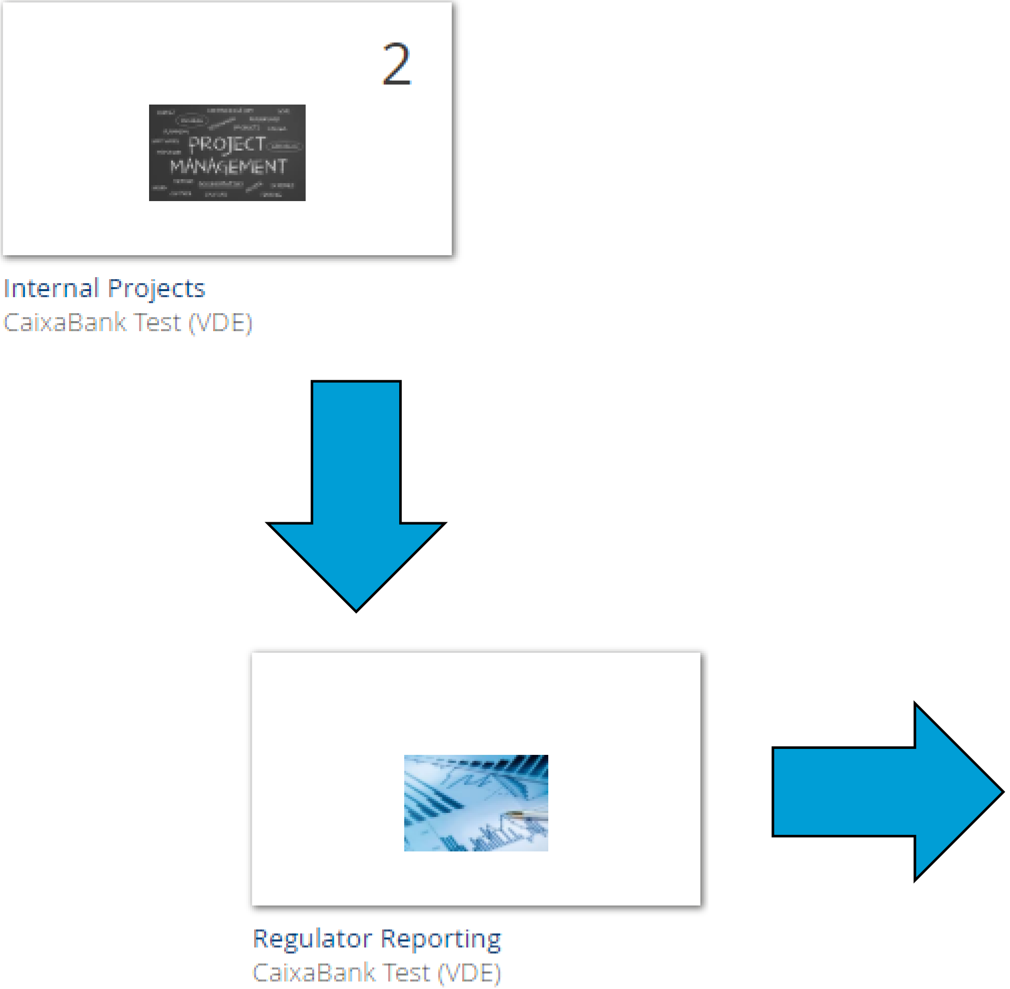
CaixaBank Test (VDE)
Organización de Cloud

Follow-Ups
Follow-Ups

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

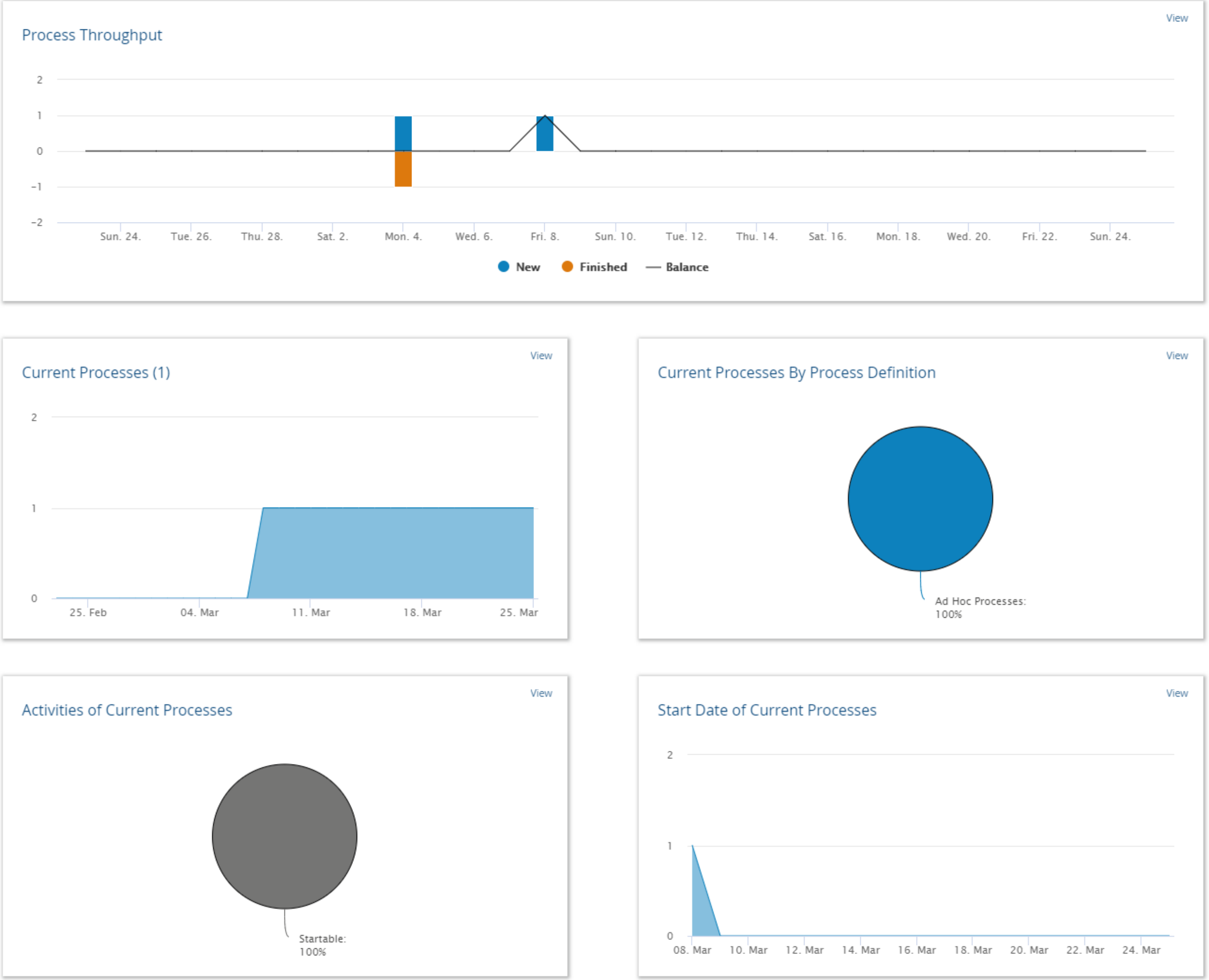
Continuous Auditing Technical Architecture

FISH Application (SaaS approach)



Internal Projects
CaixaBank Test (VDE)

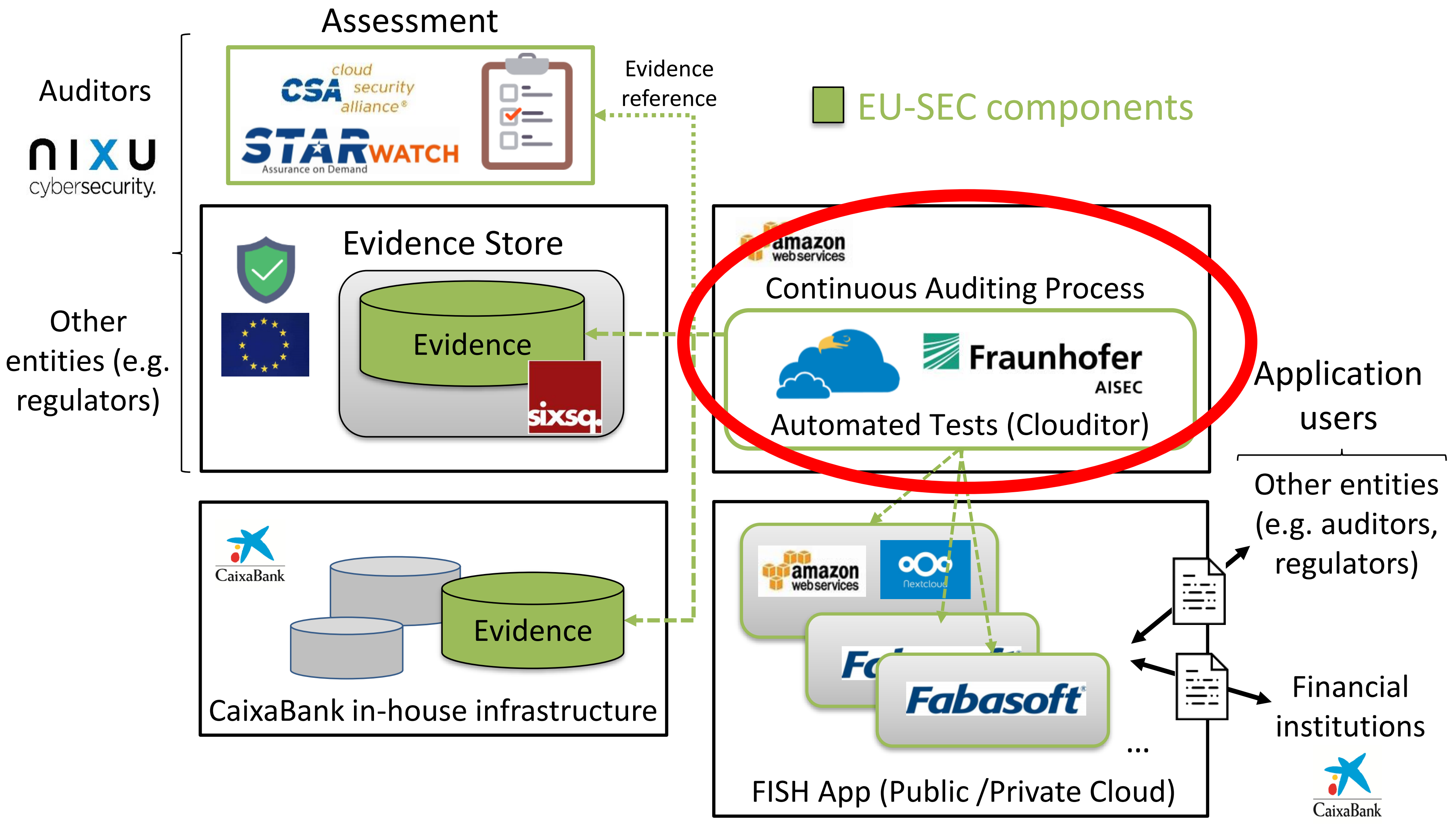
Regulator Reporting
CaixaBank Test (VDE)



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

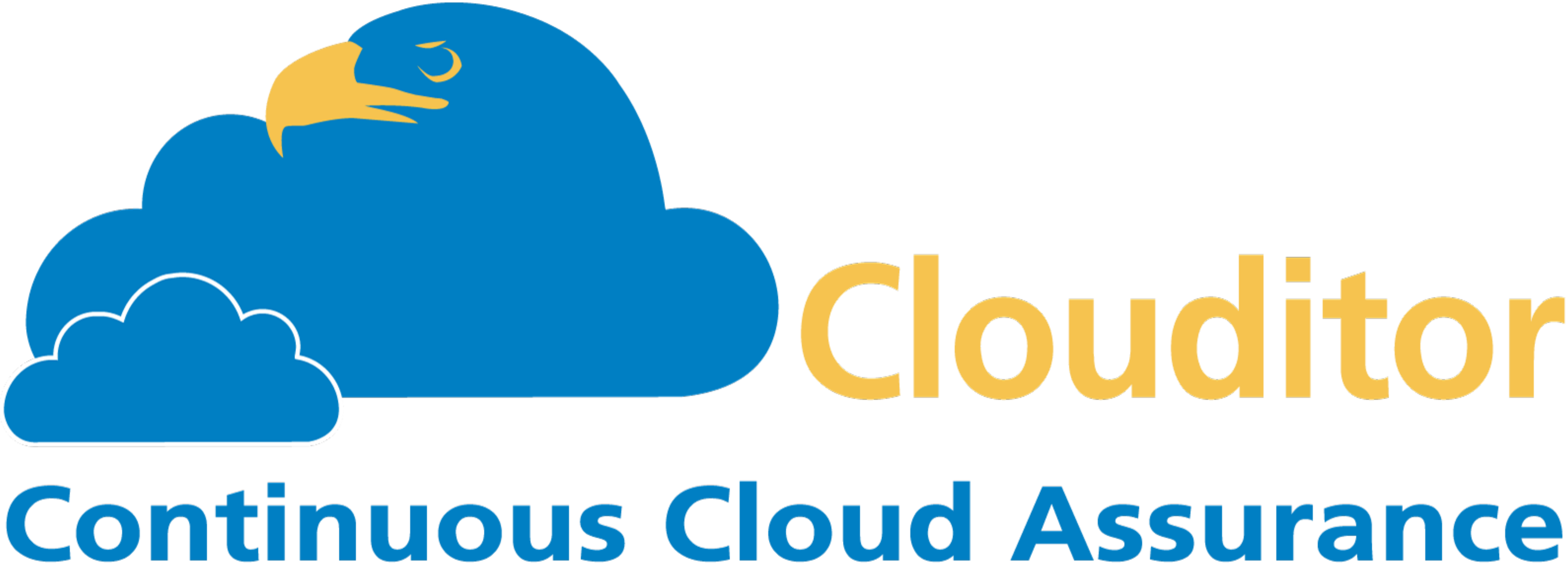
Continuous Auditing Technical Architecture

Clouditor



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

Continuous Auditing Technical Architecture
Clouditor



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

Continuous Auditing Technical Architecture
Clouditor

What is Clouditor?

- Cloud Compliance Tool to automatically check the compliance status of a cloud service
- Originated out of a German public funded project, NGCert, developed by Fraunhofer AISEC
- One of the goals of EU-SEC is to increase the TRL (Technology Readiness Level) of tools such as Clouditor
- Fraunhofer AISEC is currently aiming towards an available evaluation version of Clouditor after the EU-SEC pilot
- Currently supports Azure, AWS and EU-SEC Audit API Backends with over 100 compliance rules.

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

Continuous Auditing Technical Architecture
Clouditor

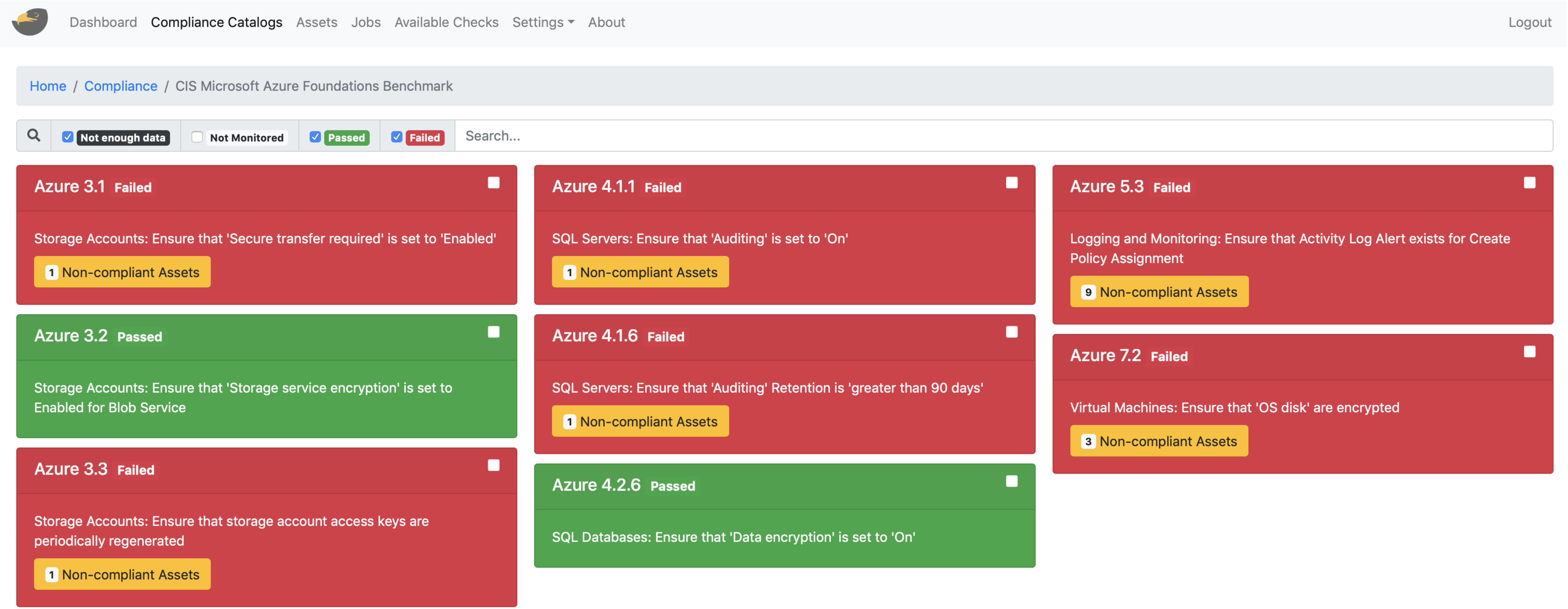
What is the role of Clouditor in EU-SEC?

- Clouditor gathers evidences from the FISH application(s) using the defined EU-SEC Audit API
- It evaluated the evidence against a set of compliance rules, i.e. “encryption must be AES-256”
- Finally,
  - forwards evidence for cold storage to the Nuvla evidence stores and
  - updates the certification status in StarWatch.

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

Continuous Auditing Technical Architecture

Clouditor – Controls Overview



Home / Compliance / CIS Microsoft Azure Foundations Benchmark

☑ Not enough data ☐ Not Monitored ☑ Passed ☑ Failed Search...

Azure 3.1 Failed ☐

Storage Accounts: Ensure that 'Secure transfer required' is set to 'Enabled'

1 Non-compliant Assets

Azure 3.2 Passed ☐

Storage Accounts: Ensure that 'Storage service encryption' is set to Enabled for Blob Service

Azure 3.3 Failed ☐

Storage Accounts: Ensure that storage account access keys are periodically regenerated

1 Non-compliant Assets

Azure 4.1.1 Failed ☐

SQL Servers: Ensure that 'Auditing' is set to 'On'

1 Non-compliant Assets

Azure 4.1.6 Failed ☐

SQL Servers: Ensure that 'Auditing' Retention is 'greater than 90 days'

1 Non-compliant Assets

Azure 4.2.6 Passed ☐

SQL Databases: Ensure that 'Data encryption' is set to 'On'

Azure 5.3 Failed ☐

Logging and Monitoring: Ensure that Activity Log Alert exists for Create Policy Assignment

9 Non-compliant Assets

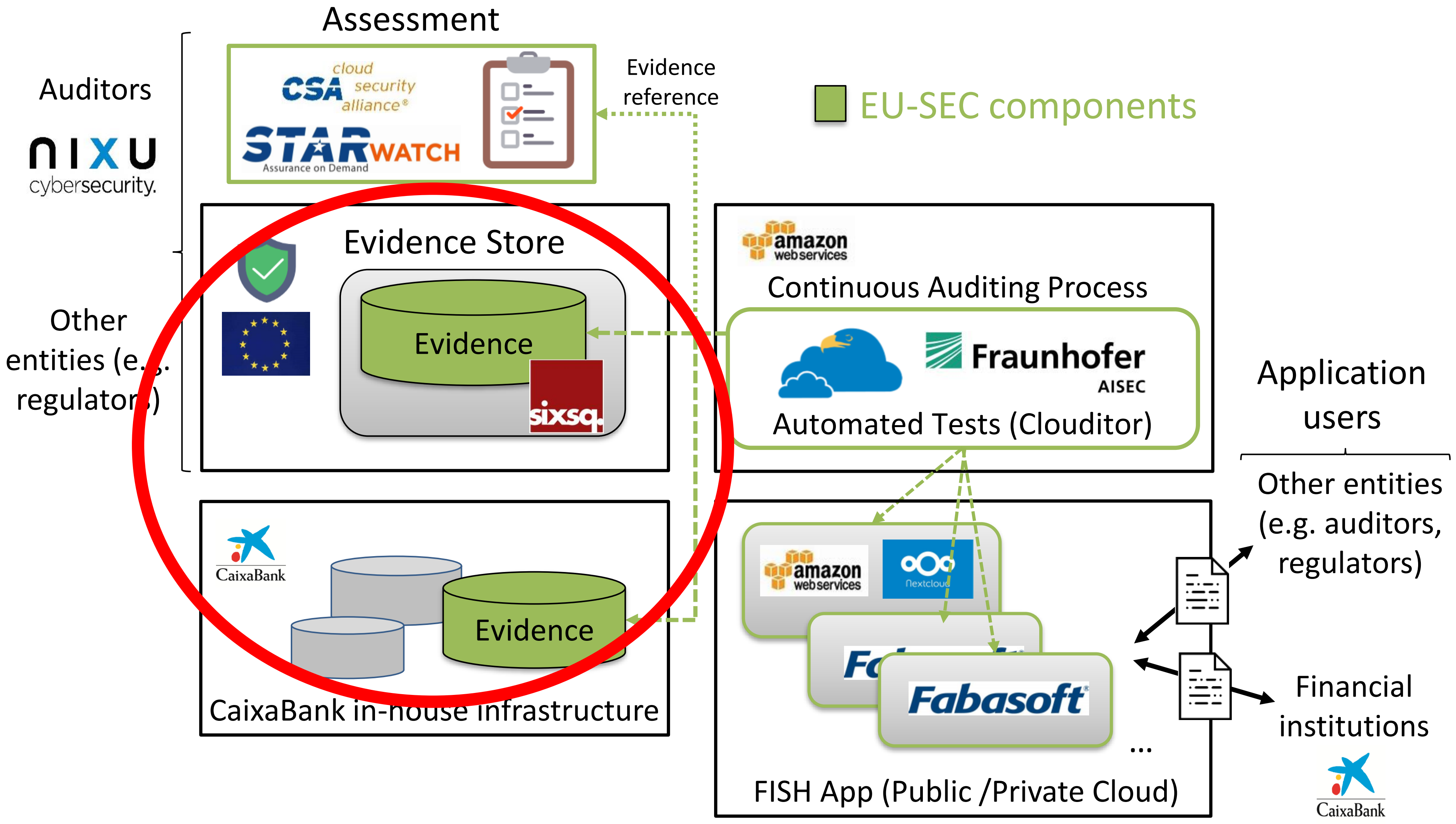
Azure 7.2 Failed ☐

Virtual Machines: Ensure that 'OS disk' are encrypted

3 Non-compliant Assets

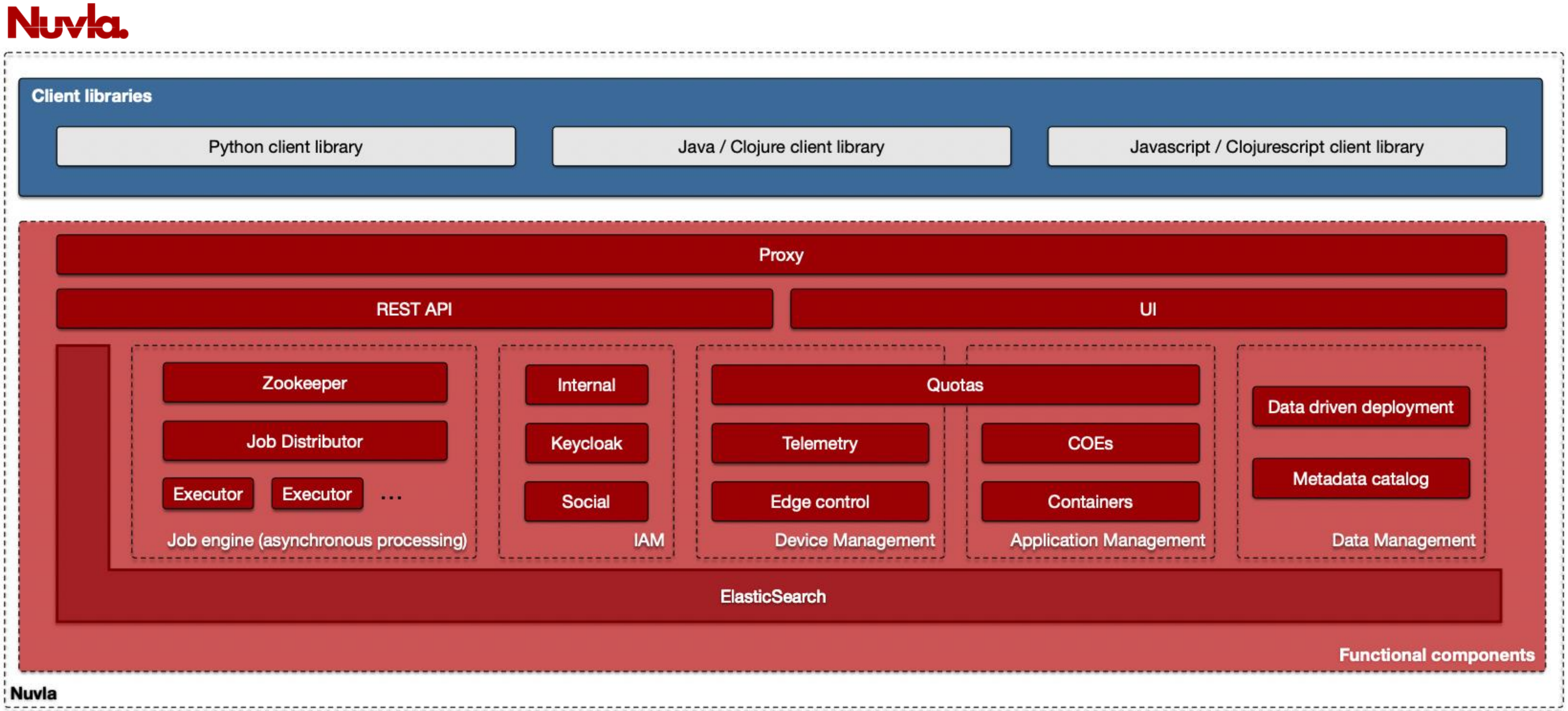
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing Technical Architecture
Evidence Store



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

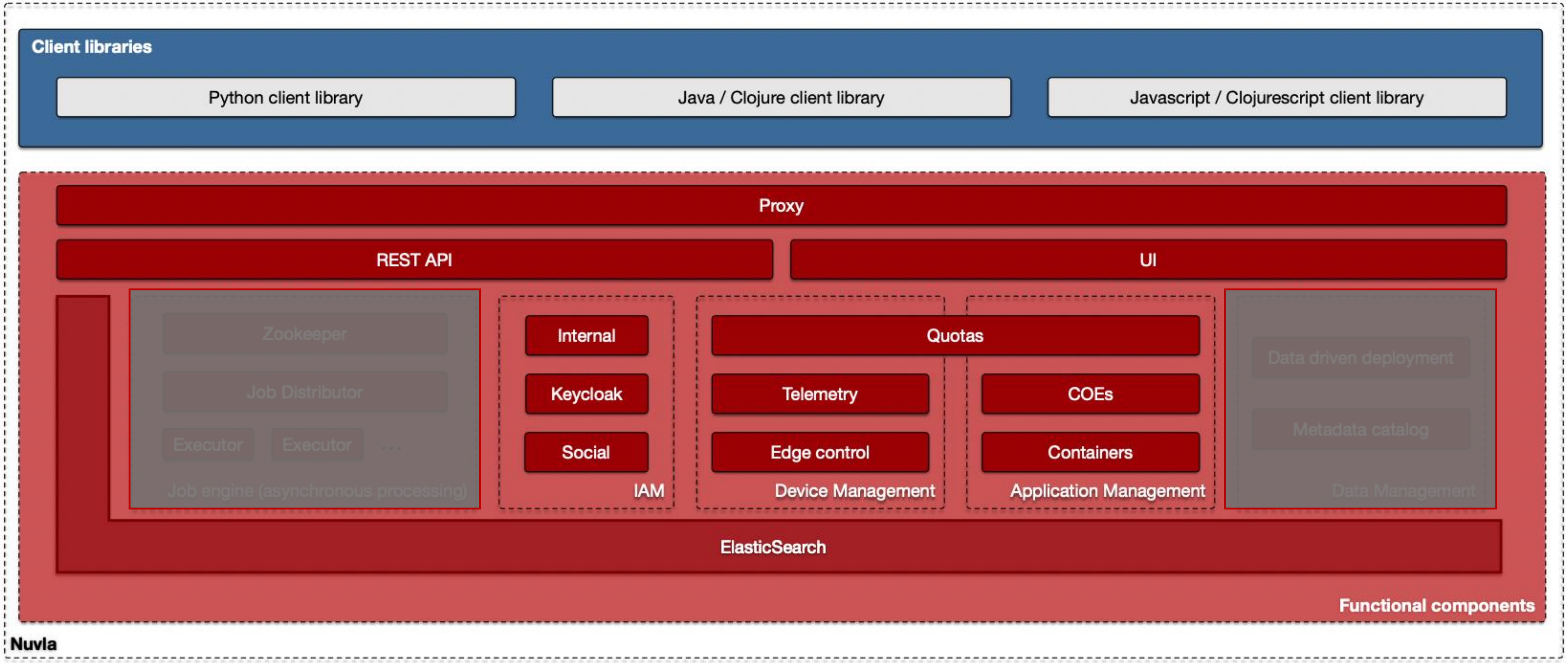
Continuous Auditing Technical Architecture
Evidence Store



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

Continuous Auditing Technical Architecture
Evidence Store

Nuvla ...for Continuous Auditing



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

Continuous Auditing Technical Architecture

Evidence Store

- Internal, social and federated authentication
- ACL-based resource management
- CIMI compliant API (DMTF standard)
- Containerized architecture
- Audit portal via graphical user interface
- Full evidence management capabilities via RESTful interface
- API server supports both self-signed certificates and LE auto-generated certificates
- Open source

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

Continuous Auditing Technical Architecture

Evidence Store

Deployment

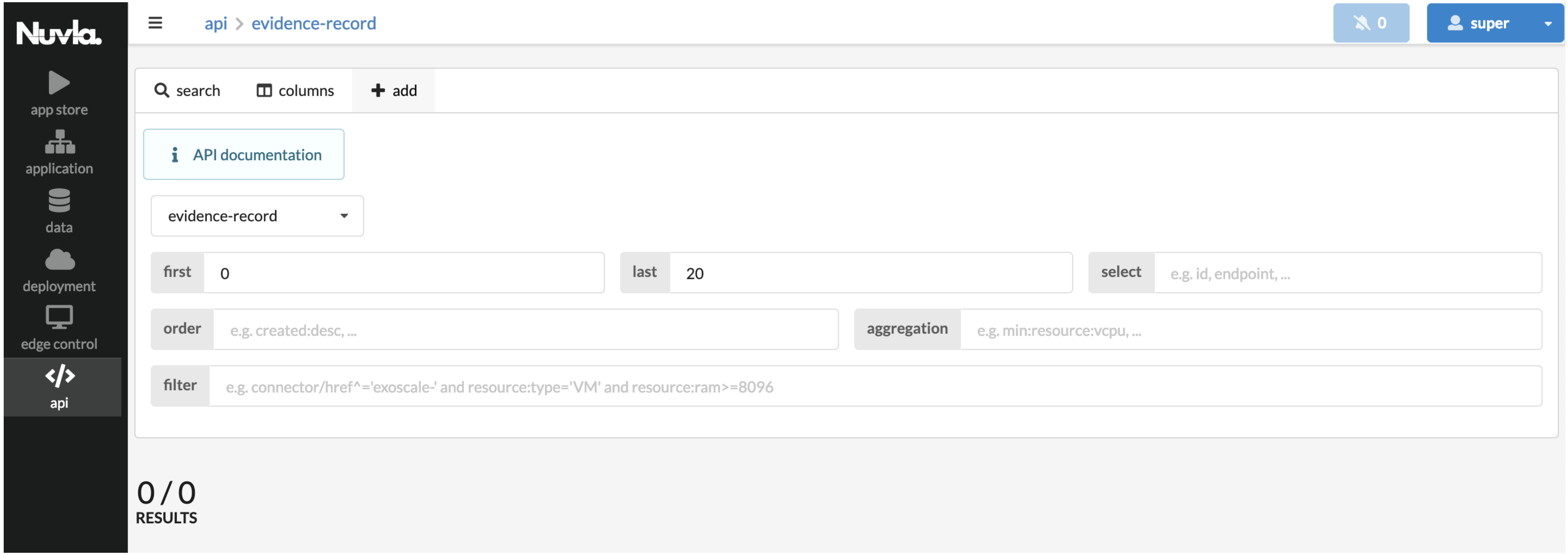
- Highly portable Docker based deployment (via Docker Compose or Docker Swarm)
- Compatible with Windows, MacOS or Linux
- Minimum requirements: 2 cores and 4GB RAM
- One line deployment:

```
docker stack deploy --compose-file nuvla-evidence-store.yml evidence-store
```

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

Continuous Auditing Technical Architecture
Evidence Store

- The Evidence Store owner is automatically given administration privileges
- Management of new users and evidence records via both the API and the UI



evidence-record

first 0

last 20

select e.g. id, endpoint, ...

order e.g. created:desc, ...

aggregation e.g. min:resource:vcpu, ...

filter e.g. connector/href^='exoscale-' and resource:type='VM' and resource:ram>=8096

0 / 0
RESULTS

9th April 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.

Continuous Auditing Technical Architecture

Evidence Store

- **Management of evidence records**

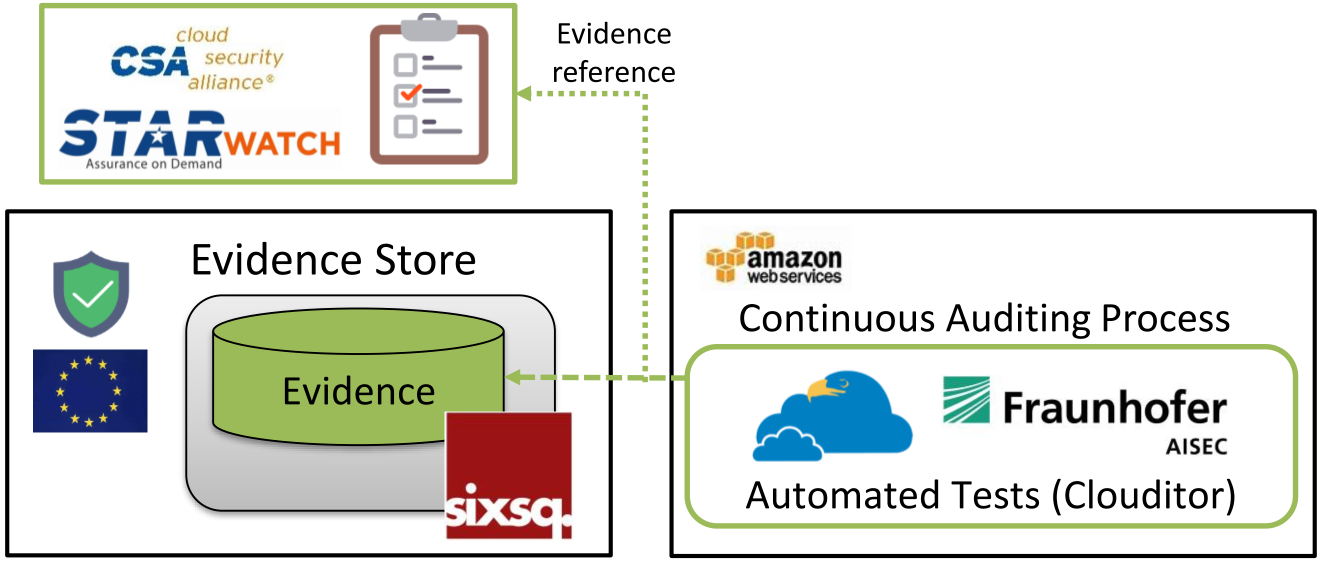
- Evidence records follow an open schema, allowing users to define a namespace and record as much evidence metadata as necessary
- Non-text evidence (like images or documents) can also be referenced from an evidence record, via an “external-object” resource which allows the management of S3 objects through Nuvla
- Evidence records are owned by their publisher, who can also grant READ and/or WRITE access to other users (like auditors or auditees)

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

Continuous Auditing Technical Architecture
Evidence Store

Workflow

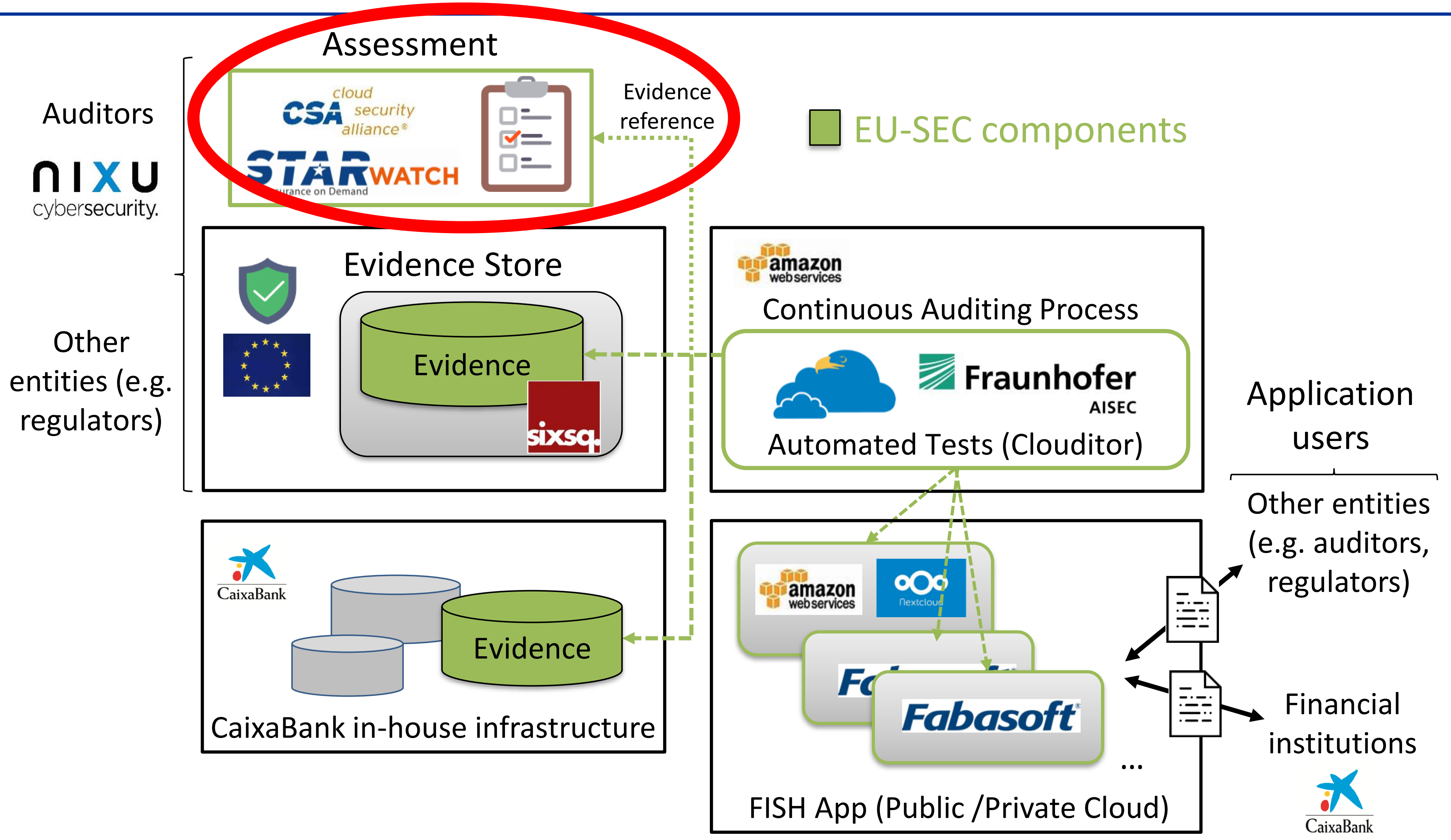
1. Deploy each component separately
2. Create a Clouditor user (for programmatic access) in the Evidence Store (Nuvla)
3. Clouditor posts evidence records into the Evidence Store
4. On every POST, the Evidence Store generate an unique and random ID for the evidence record
5. Clouditor takes this reference and publishes it into Starwatch for tracking purposes
6. Clouditor can (at generation time or later) edit the evidence record to grant READ access to auditors and auditees



Multiple evidence stores can be set, and Clouditor can be configured to post evidence records to multiple instances

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

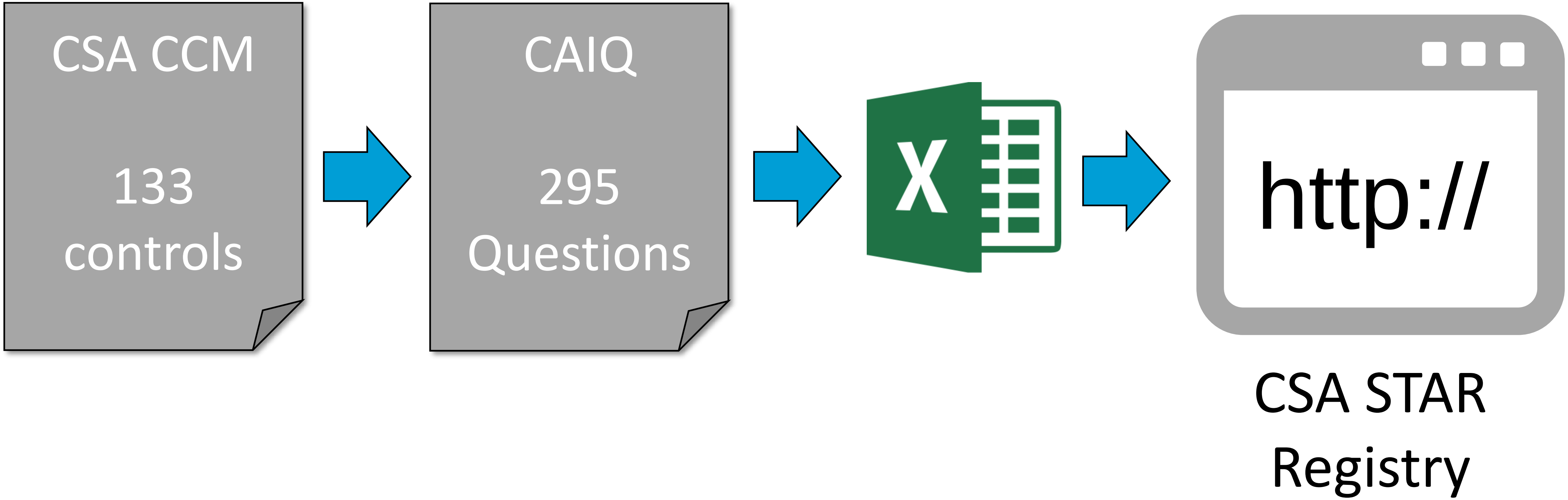
Continuous Auditing Technical Architecture
StarWatch



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

Continuous Auditing Technical Architecture

Before StarWatch was the CAIQ/CCM



CSA CCM

133 controls

CAIQ

295 Questions

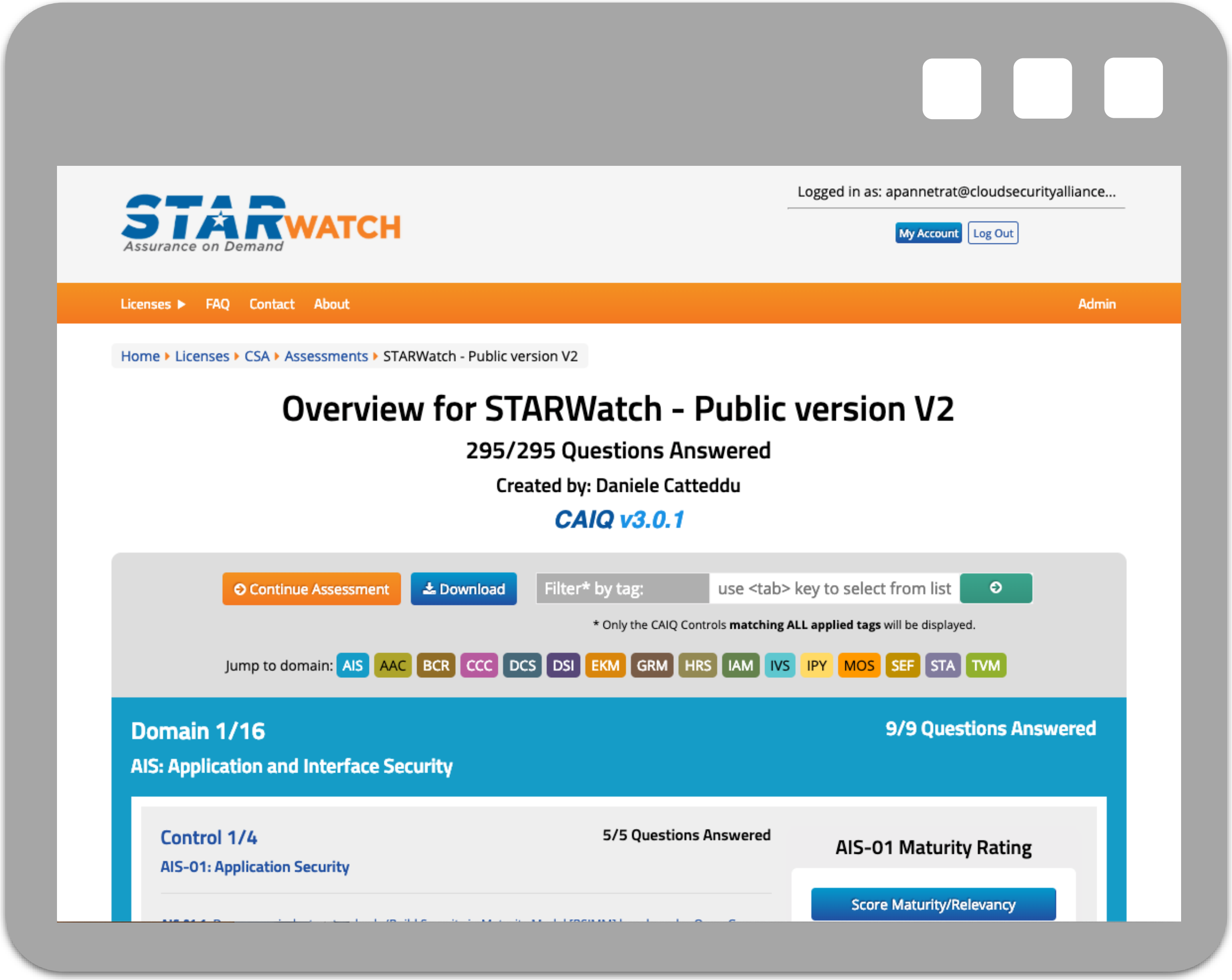
http://

CSA STAR Registry

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

Continuous Auditing Technical Architecture

StarWatch was born



Logged in as: apannetrat@cloudsecurityalliance...

Home ▸ Licenses ▸ CSA ▸ Assessments ▸ STARWatch - Public version V2

Overview for STARWatch - Public version V2

295/295 Questions Answered

Created by: Daniele Catteddu

CAIQ v3.0.1

* Only the CAIQ Controls **matching ALL applied tags** will be displayed.

Jump to domain: AIS AAC BCR CCC DCS DSI EKM GRM HRS IAM IVS IPY MOS SEF STA TVM

Domain 1/16 **9/9 Questions Answered**

AIS: Application and Interface Security

Control 1/4 5/5 Questions Answered

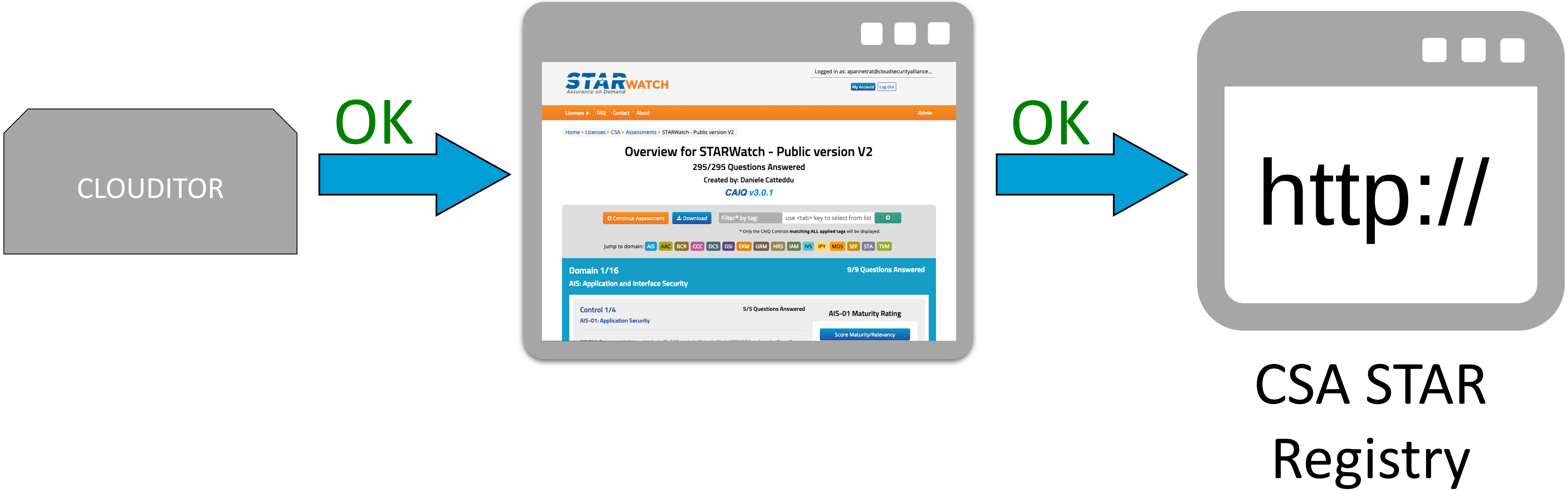
AIS-01: Application Security

AIS-01 Maturity Rating

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

Continuous Auditing Technical Architecture

StarWatch in EU-SEC



CLOUDITOR

OK

Logged in as: apannetrat@cloudsecurityalliance...

Home ▸ Licenses ▸ CSA ▸ Assessments ▸ STARWatch - Public version V2

Overview for STARWatch - Public version V2

295/295 Questions Answered

Created by: Daniele Catteddu

CAIQ v3.0.1

Filter* by tag: use <tab> key to select from list

* Only the CAIQ Controls **matching ALL applied tags** will be displayed.

Domain 1/16 — 9/9 Questions Answered

AIS: Application and Interface Security

Control 1/4 — 5/5 Questions Answered

AIS-01: Application Security

AIS-01 Maturity Rating

OK

http://

CSA STAR Registry

9th April 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.

Continuous Auditing Technical Architecture

Star Registry for continuous certification

- Case 1 🟢
  - The objectives (SLO/SQO) have been confirmed in due time.
  - The “continuous” certificate is considered as valid in the STAR Registry.

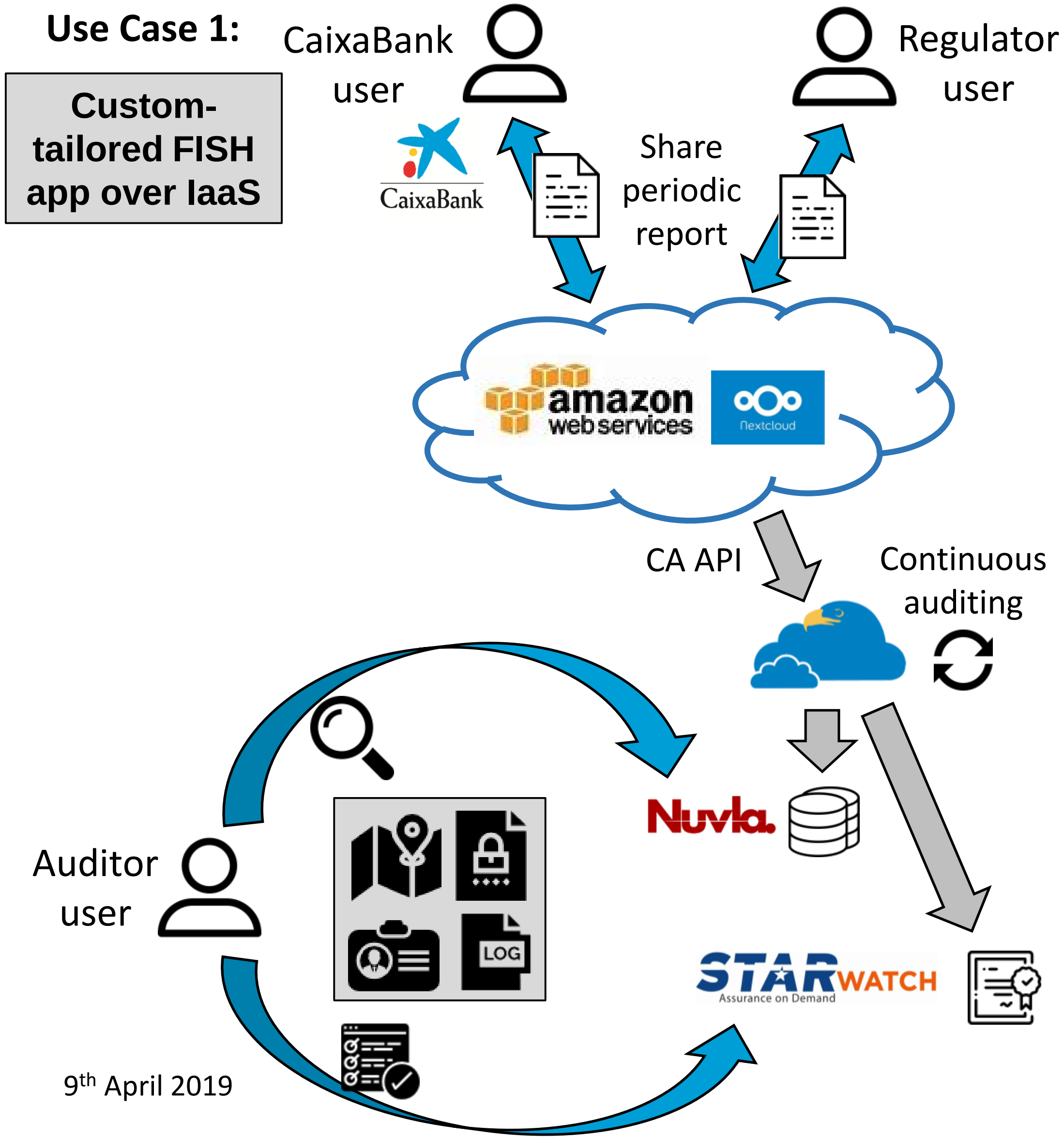
- Case 2: 🟠
  - At least one objective (SLO/SQO) has NOT been confirmed in due time.
  - The “continuous” certificate is considered as “suspended” in the STAR Registry.

- Case 3: 🔴
  - At least one objective (SLO/SQO) has NOT been confirmed in due time, and has stayed so for more than two weeks.
  - The “continuous” certificate removed from the STAR Registry (revoked).

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

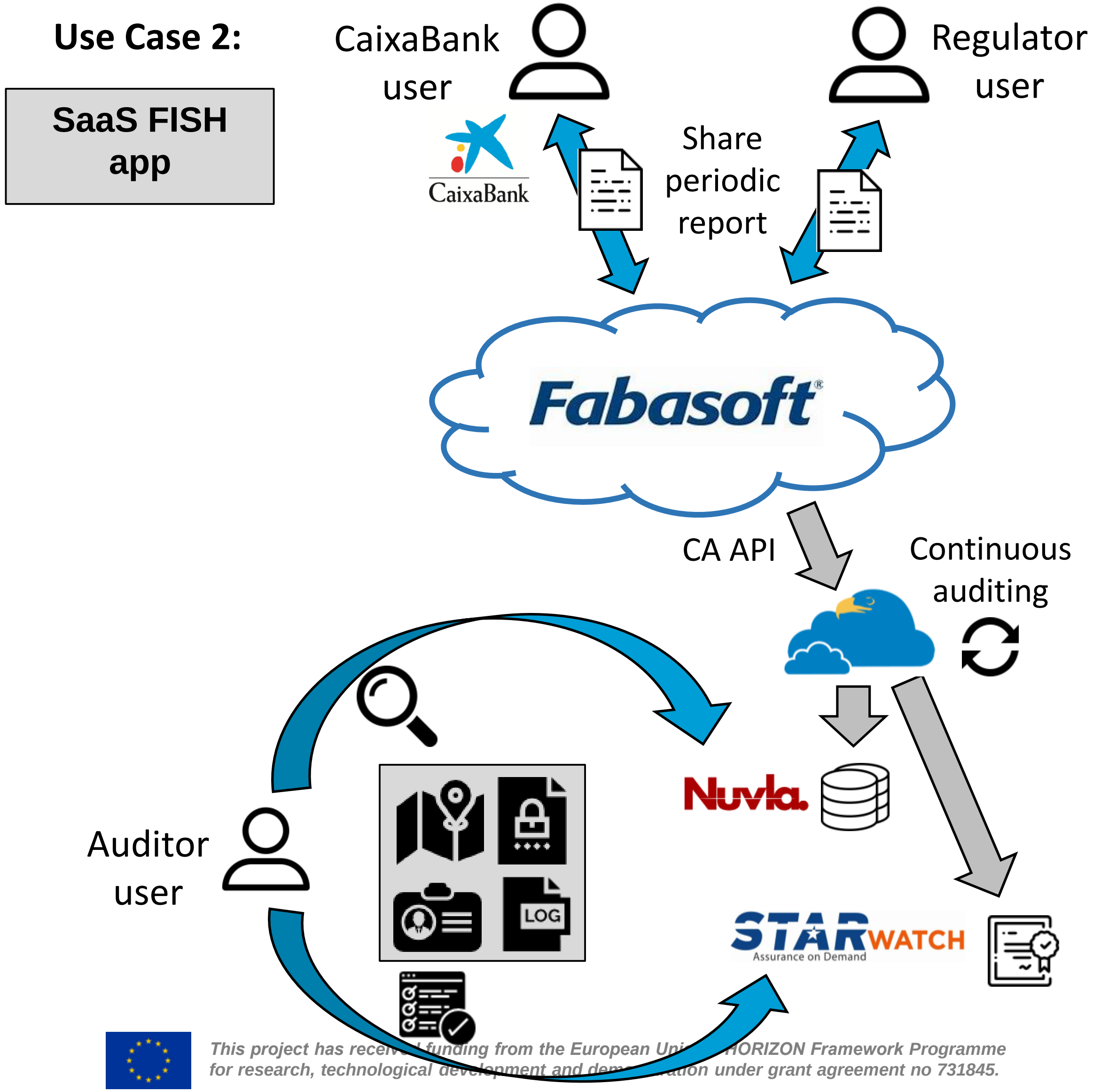
Continuous Auditing Technical Architecture

Use case specification



Use Case 1:

Custom-tailored FISH app over IaaS



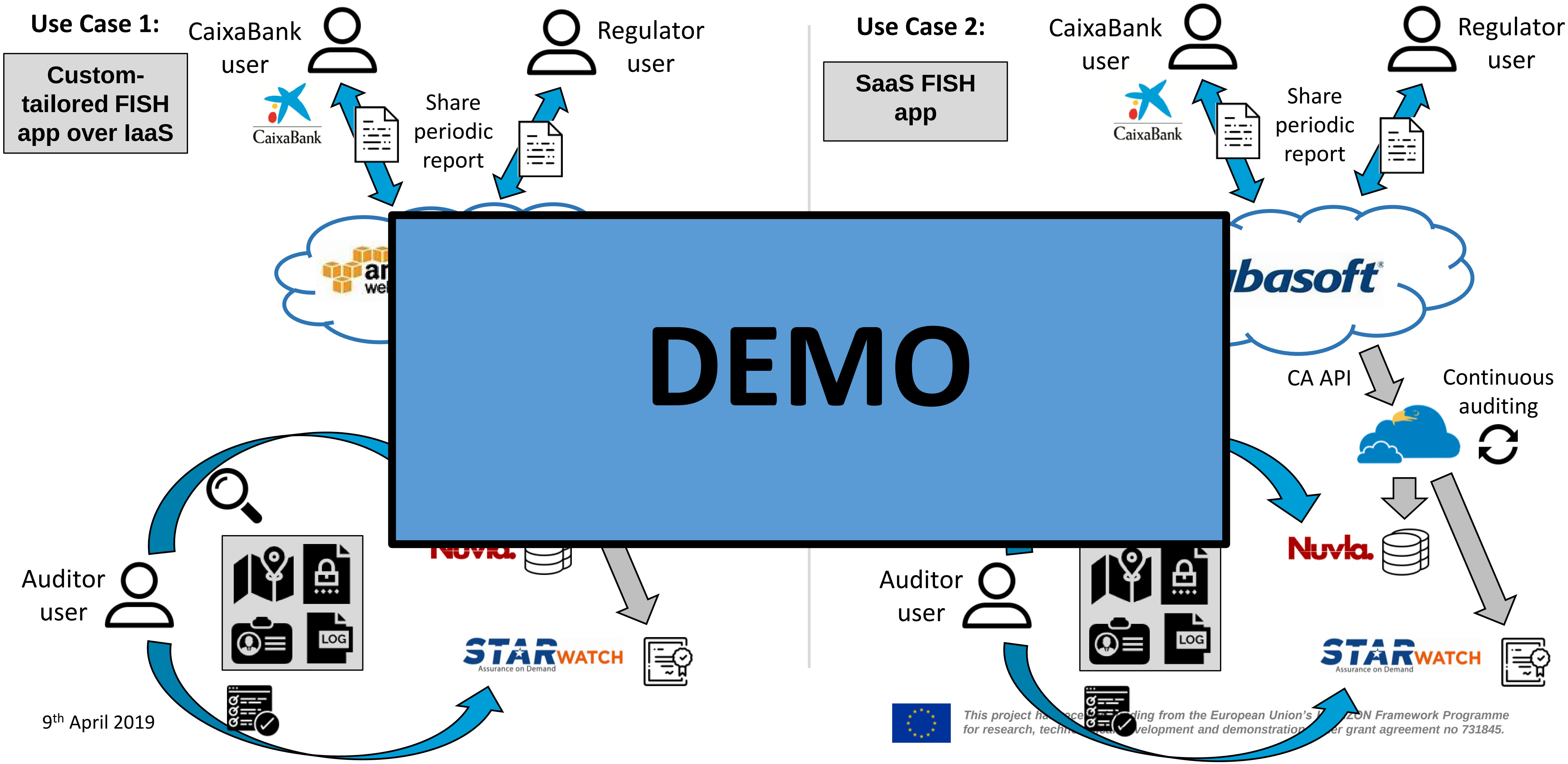
Use Case 2:

SaaS FISH app

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

Continuous Auditing Technical Architecture

Use case specification



This project ha ceiving from the European Union's ZON Framework Programme for research, techn velopment and demonstration er grant agreement no 731845.

Round Table Discussion – Questions & Answers

Ramon Martín de Pozuelo (CAIXABANK)

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

Continuous Auditing-based Certification

Round Table Discussion - Questions and Answers

EUSEC
EU SECURITY CERTIFICATION

- How is your entity dealing with sensitive information sharing (e.g FI reporting to regulator)? How are you performing it? Are you following and standardized way? Which platforms/tools are you using?

- What security requirements do you consider when moving services to the cloud? Which security controls would you define in the auditing process? Which certification scheme would you be interested to integrate?

- What would you demand of the EU-SEC Continuous Auditing architecture in order to completely trust and rely on it?

- As a customer, which Continuous Auditing client application approach would be more appealing for your entity? Would you rely on a SaaS app provided by a Cloud Service Provider or develop your own app over IaaS?

- What would you expect from EU-SEC pilot? What would you like to test?

- What do you consider the most critical points for wide adoption of the proposed solution? Are there any missing features, or ones you would change, in order to use this solution in your entities? Which drivers or obstacles do you foresee?

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

Continuous Auditing-based Certification

Round Table Discussion - Questions and Answers

Online Questionnaires:

Cloud Service Providers

https://www.surveymonkey.com/r/5K58TV8

Cloud Customers

https://www.surveymonkey.com/r/58B8T5X

Auditors

https://www.surveymonkey.com/r/5L7MG8T

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

Thank you for your attention!

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

Contact: *contact@sec-cert.eu*

Twitter: @EU_SEC

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