EUSEC
EU SECURITY CERTIFICATION

Pilot 2 - Continuous Monitoring/Auditing Based Certification

PILOT PREPARATION

Baseline

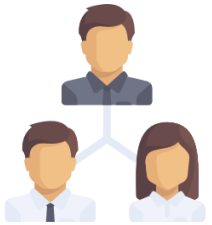
EUSEC
EU SECURITY CERTIFICATION

Trusted information sharing

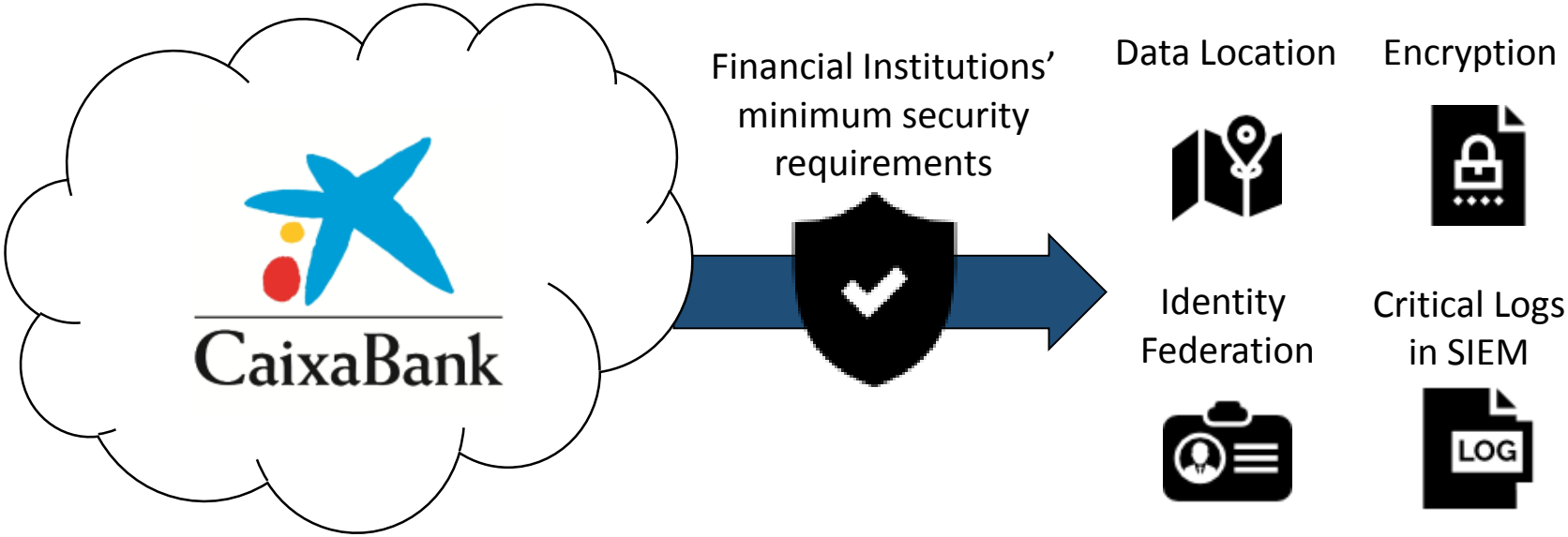
Financial institutions need to report sensible information to the regulators in a reliable and trusted way.

Collaboration

In some cases, this exchange of information can involve multiple entities and organisms.

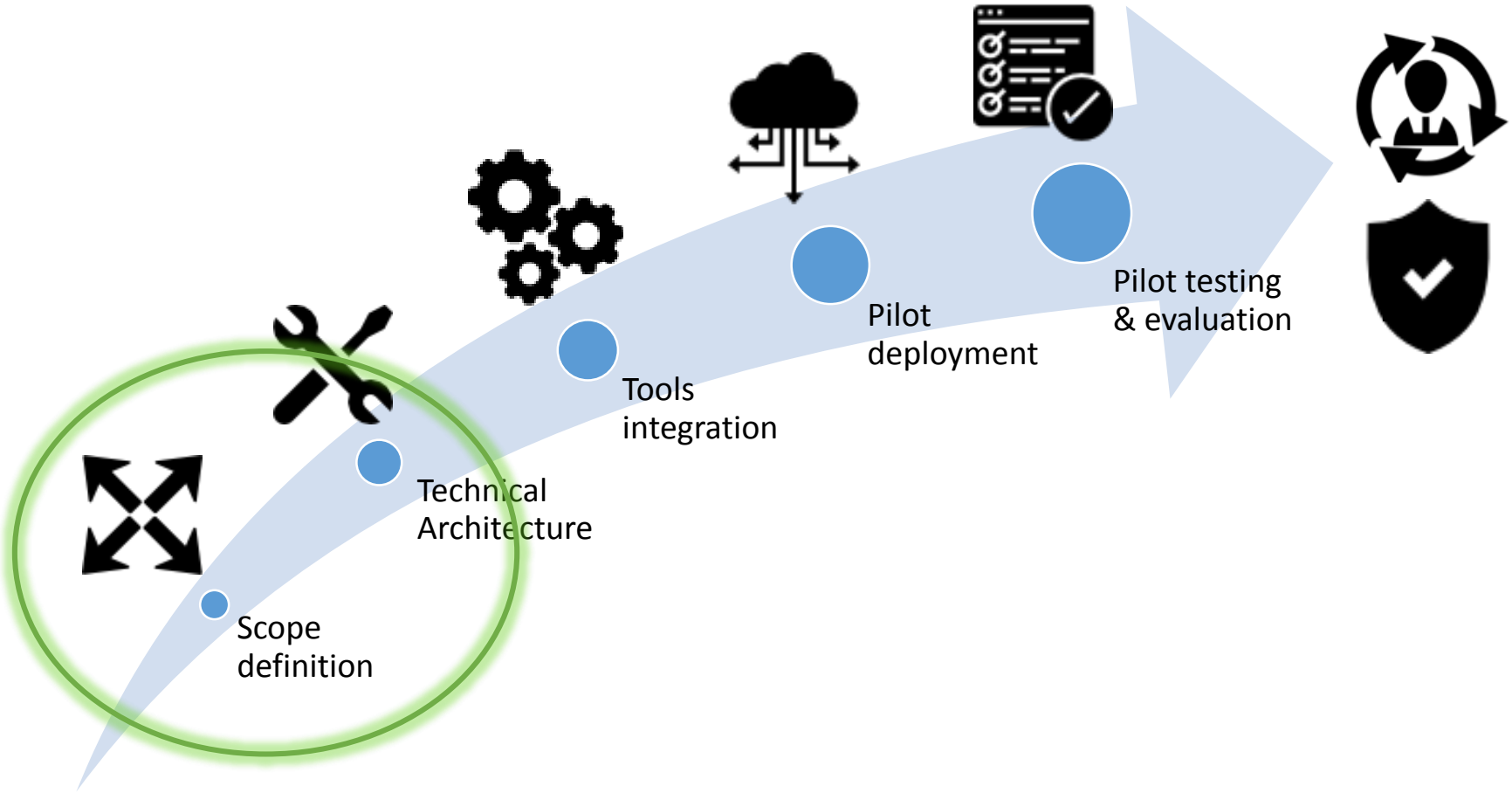


Industrial gap motivation: Lack of a continuous auditing service that verifies that the Cloud provider running the information sharing service actually complies with Financial Institutions' requirements.



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

Pilot phases

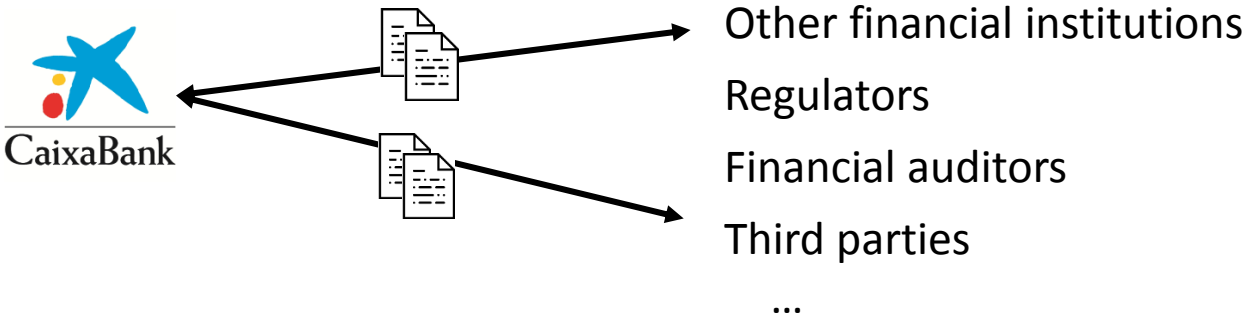


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Scope Definition - Problem statement

Current scenario and problem statement:

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

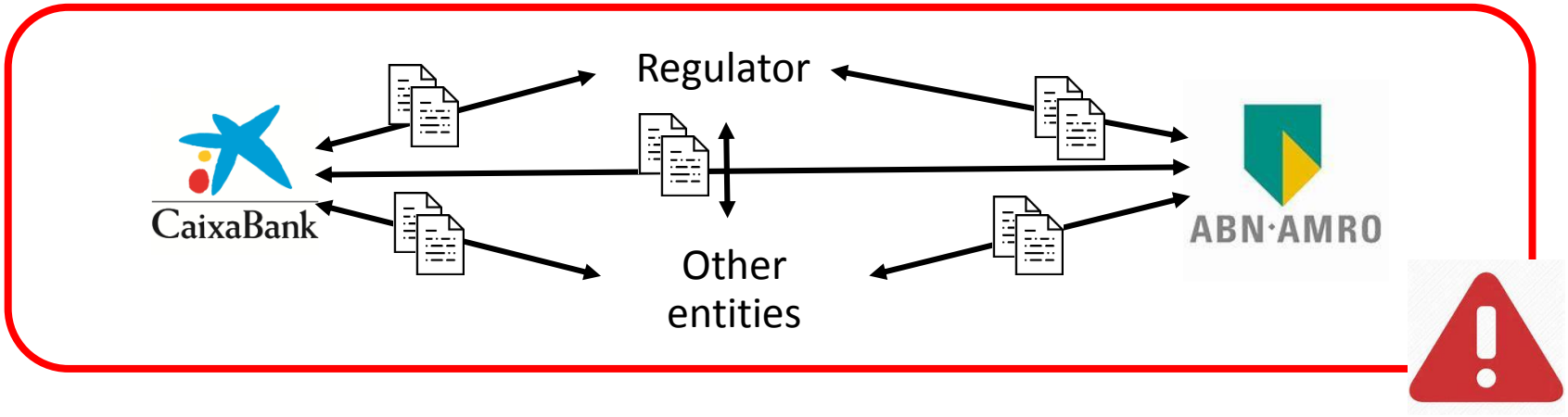


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Scope Definition - Problem statement

Current scenario and problem statement:

- 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 tedious document management**:
  - Report sensitive information via mail, physical sharing of information,…



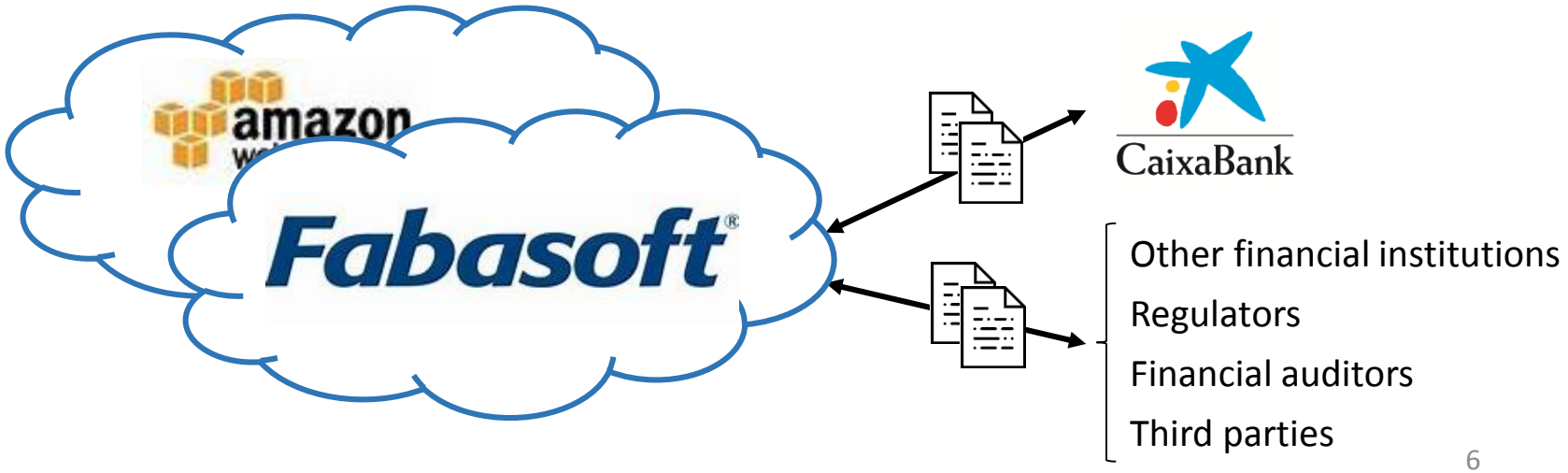
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Approach – Technical Architecture Definition

- Do we experience differences in auditing different **service models**, i.e. IaaS and SaaS?
- Can FISH and the auditing service **run in the same Cloud?**

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

- Variation 1) Use **Fabasoft as a Cloud platform for information sharing (SaaS):**
- Variation 2) **Build custom-tailored FISH** application using existing components, i.e. open source on top of a **commercial Cloud provider (IaaS)**



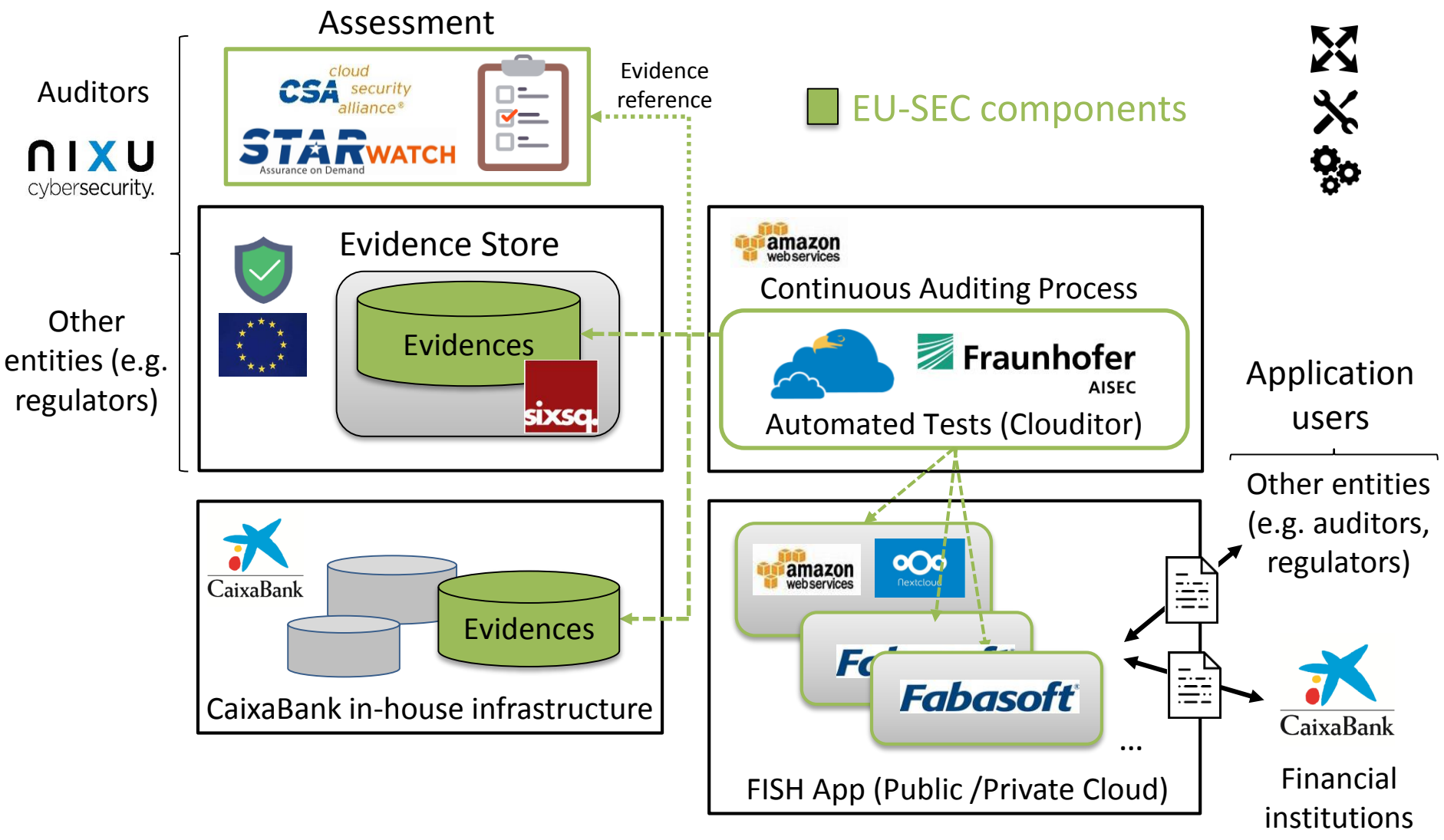
Approach - Requirements definition

- CAIXABANK requirements identification

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

- Which tools and tests can we use to audit continuously these controls?

Results - Technical Architecture Overview



Continuous Audit API (CA API)

- **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/