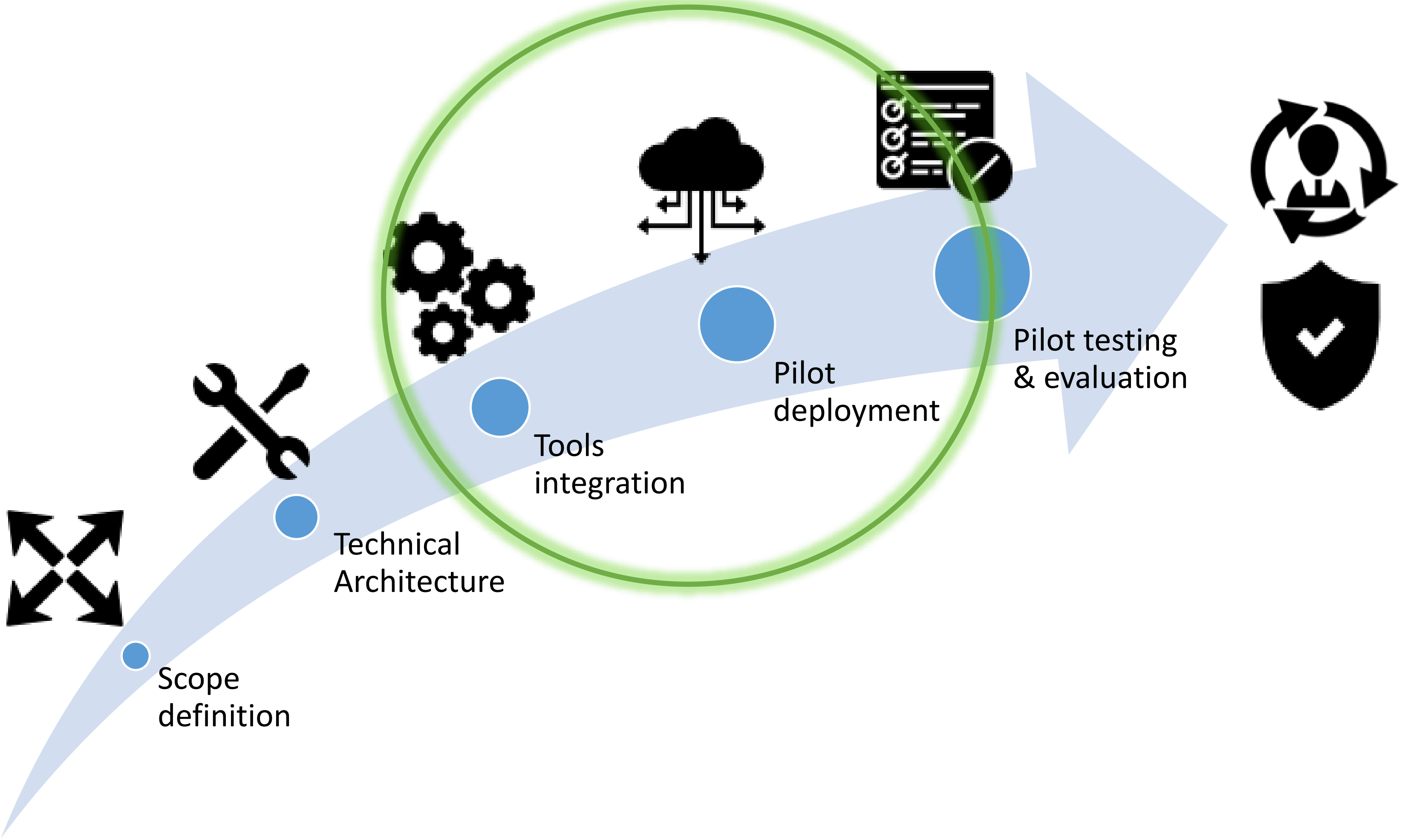
EUSEC
EU SECURITY CERTIFICATION

Pilot 2 - TECHNICAL REPORT ON PILOT INTEGRATION FOR PROVIDER SELECTION AND CONTINUOUS CERTIFICATION

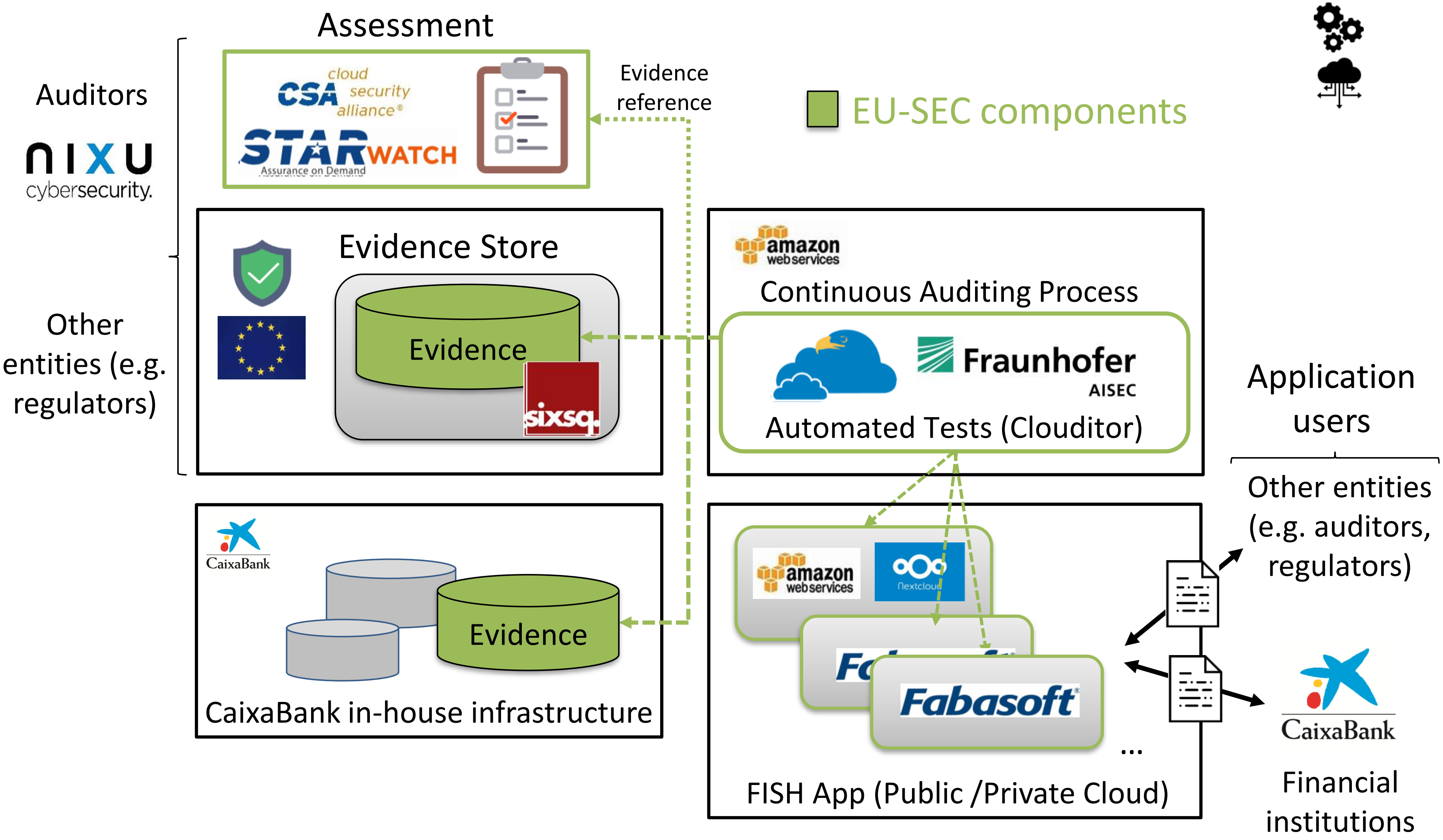
PILOT IMPLEMENTATION AND TESTING

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.

Pilot - Technical Reference Architecture



Assessment

Evidence reference

🟩 EU-SEC components

Auditors

Other entities (e.g. regulators)

Evidence Store

Evidence

Continuous Auditing Process

Automated Tests (Clouditor)

Application users

Other entities (e.g. auditors, regulators)

Evidence

CaixaBank in-house infrastructure

FISH App (Public /Private Cloud)

...

Financial institutions

Pilot - Continuous Audit-based Certification API (CAC API)

API ENDPOINT	DESCRIPTION
/scopes/	Cloud services are realised by different technologies often arranged in architectural layers and scopes. This call return all scopes used by the service.
/{scope}/objects/	Returns Object ids of all objects that are in the scope of the audit.
/{scope}/persistence/{objectId}/storage/	Returns persistence information for a particular data object by its Id.
/{scope}/persistence/{objectId}/location/	Returns location the ISO 3166-1 alpha-2 country code of the location of the data of the object.
/{scope}/persistence/{objectId}/encryption	Retrieves the encryption info of an object.
/{scope}/identityfederation/admins/	Returns a list of administrators.
/{scope}/identityfederation/{userId}/groups	Returns the groups of a user.
/{scope}/identityfederation/{userId}/auth	Returns the authentication type of a user. E.g password, two-factor.
/{scope}/identityfederation/{userId}/logins	Returns a list of the last logins of a user.
/{scope}/identityfederation/data/access	Checks whether a user has a certain access to an object.
/{scope}/identityfederation/{userId}/ passwordRequirements	Returns the password requirements for a specific user.
/{scope}/meta/submitted	Gives information on when certain documents have been pushed to dedicated endpoints of the customer.

Pilot – Mapping pilot requirements to SLOs/SQOs

DATA LOCATION

- Persistent data storage
- Location of VM data

ENCRYPTION

- Data at rest
- Data in transit
- Key Management
- Security Cyphers

IDENTITY FEDERATION

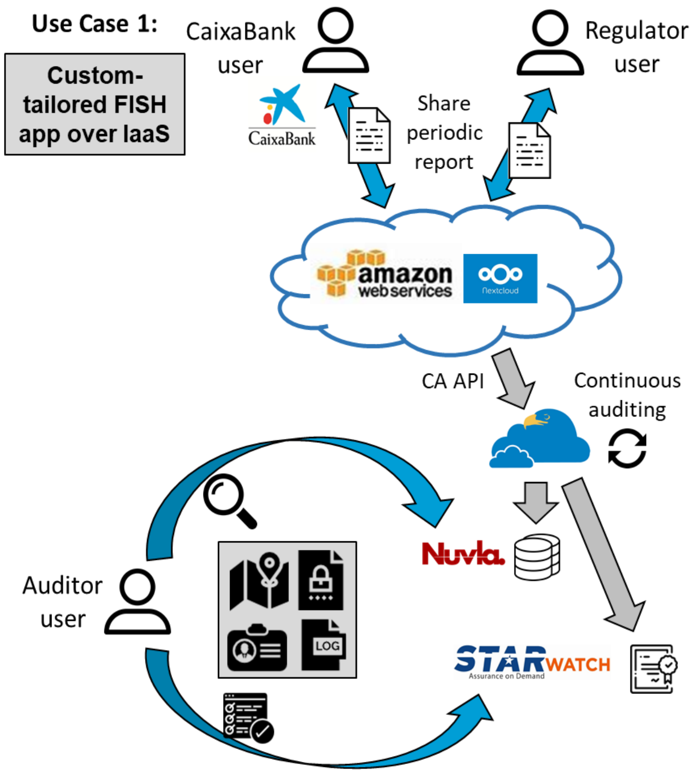
- Application level
- Platform level

EVIDENCE SECURITY

- Critical logs storage
- Critical logs accessibility
- Critical logs location

Pilot – Use Cases

- **Custom-tailored FISH (Financial Information Sharing) application over IaaS:** Proof-of-concept built over a AWS (Amazon Web Services). The application was designed to be simple while still offering the main functionalities needed in the sensitive information exchange between the user and the regulator.
- **SaaS FISH application:** test the certification of a FISH application in SaaS with more advanced actions between users (e.g. multiparty interactions and document management).



Use Case 1:

Custom-tailored FISH app over IaaS

CaixaBank user

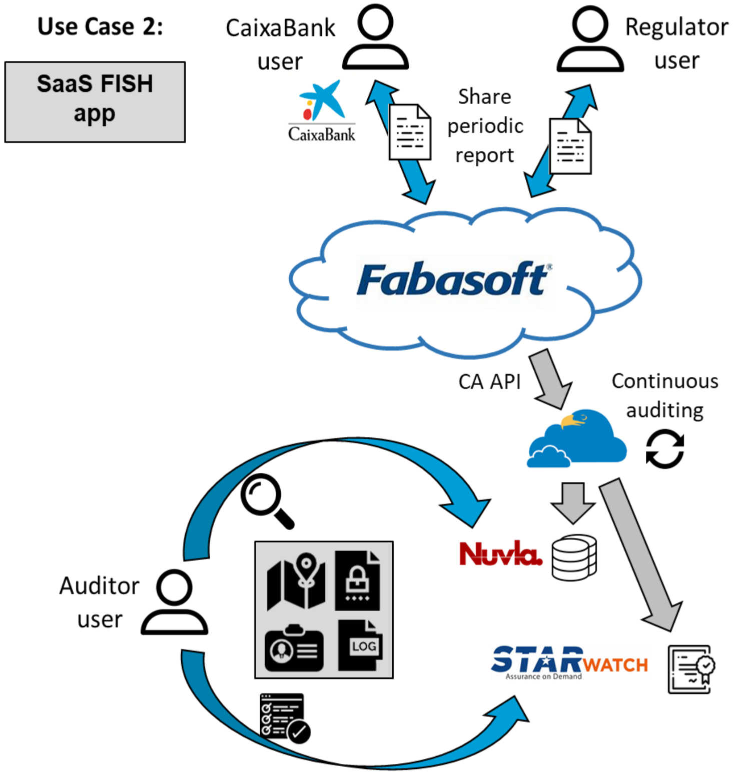
Regulator user

Share periodic report

CA API

Continuous auditing

Auditor user



Use Case 2:

SaaS FISH app

CaixaBank user

Regulator user

Share periodic report

CA API

Continuous auditing

Auditor user

Pilot – Use Cases definition

Use case definition: actors, scenario, steps.

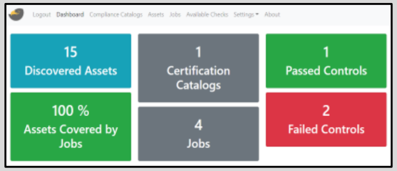
EU-SEC.FISH.IAAS.v1		
Financial Information reporting to regulator - FISH app approach over IAAS.	Version No:	1.1
…		

EU-SEC.FISH.SAAS.v1		
Financial Information reporting to multiple users of the regulator entity - FISH app approach over SAAS.	Version No:	1.1
…		

- **Financial Institution (FI):** An employee of a financial institution dedicated to the financial sector.
- **Regulator User (R):** An employee of the entity that regulates the financial sector.
- **Additional Regulator User (R2):** Another employee of a regulator entity.
- **Cloud Service Provider (CSP):** Cloud provider and FISH application provider.
- **Auditor (AU):** Auditor or an external entity employee that is in charge of validating the performance and trustworthiness of the FISH application in the cloud.

Pilot – Testing

USE CASES



Logout Dashboard Compliance Catalogs Assets Jobs Available Checks Settings About

15 Discovered Assets

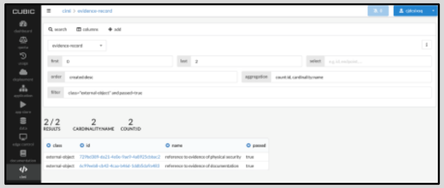
1 Certification Catalogs

1 Passed Controls

100 % Assets Covered by Jobs

4 Jobs

2 Failed Controls



CUBIC

ciml > evidence-record

search columns add

evidence-record

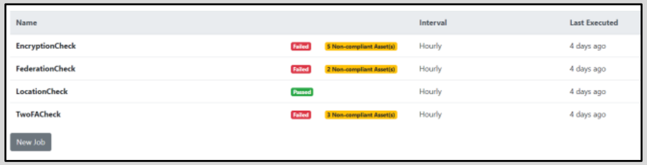
first 0 last 2 select e.g. id, endpoint,...

order created desc aggregation count id, cardinality name

filter class="external-object" and passed=true

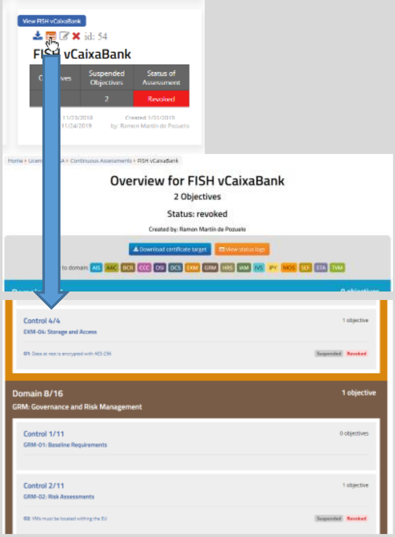
2 / 2 RESULTS 2 CARDINALITY:NAME 2 COUNT:ID

class	id	name	passed
external-object	729bd389-da21-4e0e-9ae9-4a8925cbbac2	reference to evidence of physical security	true
external-object	6c99eeb8-cb43-4caa-b46d-1dd65da9a483	reference to evidence of documentation	true



Name			Interval	Last Executed
EncryptionCheck	Failed	5 Non-compliant Asset(s)	Hourly	4 days ago
FederationCheck	Failed	2 Non-compliant Asset(s)	Hourly	4 days ago
LocationCheck	Passed		Hourly	4 days ago
TwoFACheck	Failed	3 Non-compliant Asset(s)	Hourly	4 days ago

New Job



View FISH vCaixaBank

id: 54

FISH vCaixaBank

Objectives	Suspended Objectives	Status of Assessment
	2	Revoked

11/23/2018 11/24/2019 Created 1/31/2019 by: Ramon Martin de Pozuelo

Home › Licen... › Continuous Assessments › FISH vCaixaBank

Overview for FISH vCaixaBank

2 Objectives

Status: revoked

Created by: Ramon Martin de Pozuelo

Download certificate target View status logs

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

Control 4/4 1 objective

EKM-04: Storage and Access

01: Data at rest is encrypted with AES-256 Suspended Revoked

Domain 8/16 1 objective

GRM: Governance and Risk Management

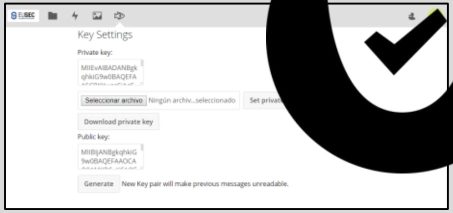
Control 1/11 0 objectives

GRM-01: Baseline Requirements

Control 2/11 1 objective

GRM-02: Risk Assessments

02: VMs must be located withing the EU Suspended Revoked



Key Settings

Private key:

MIIEvAIBADANBgk qhkiG9w0BAQEFA

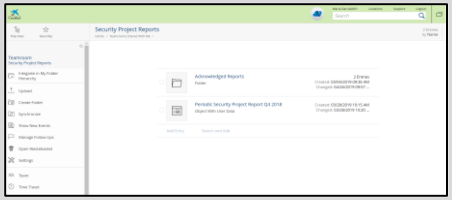
Seleccionar archivo Ningún archiv...seleccionado Set privat

Download private key

Public key:

MIIBIjANBgkqhkiG 9w0BAQEFAAOCA

Generate New Key pair will make previous messages unreadable.



Security Project Reports

Teamroom Security Project Reports

Integrate in My Folder Hierarchy

Upload

Create Folder

Synchronize

Show New Events

Manage Follow-Ups

Open Wastebasket

Settings

Team

Time Travel

Acknowledged Reports 2 Entries

Folder

Periodic Security Project Report Q4 2018

Object With User Data

Add Entry Search and Add

ARCHITECTURE

Architecture security recommendations

Information security management and architechture

Technical security requirements

HIGH-LEVEL

NON-FUNCTIONAL ASPECTS

Cloud customer perspective

First impressions from the pilot