Fraunhofer FOKUS
Institut für Offene Kommunikationssysteme

Continuous Auditing Certification

Dorian Knoblauch

21.6.2019

Fraunhofer FOKUS

Cloud Certification

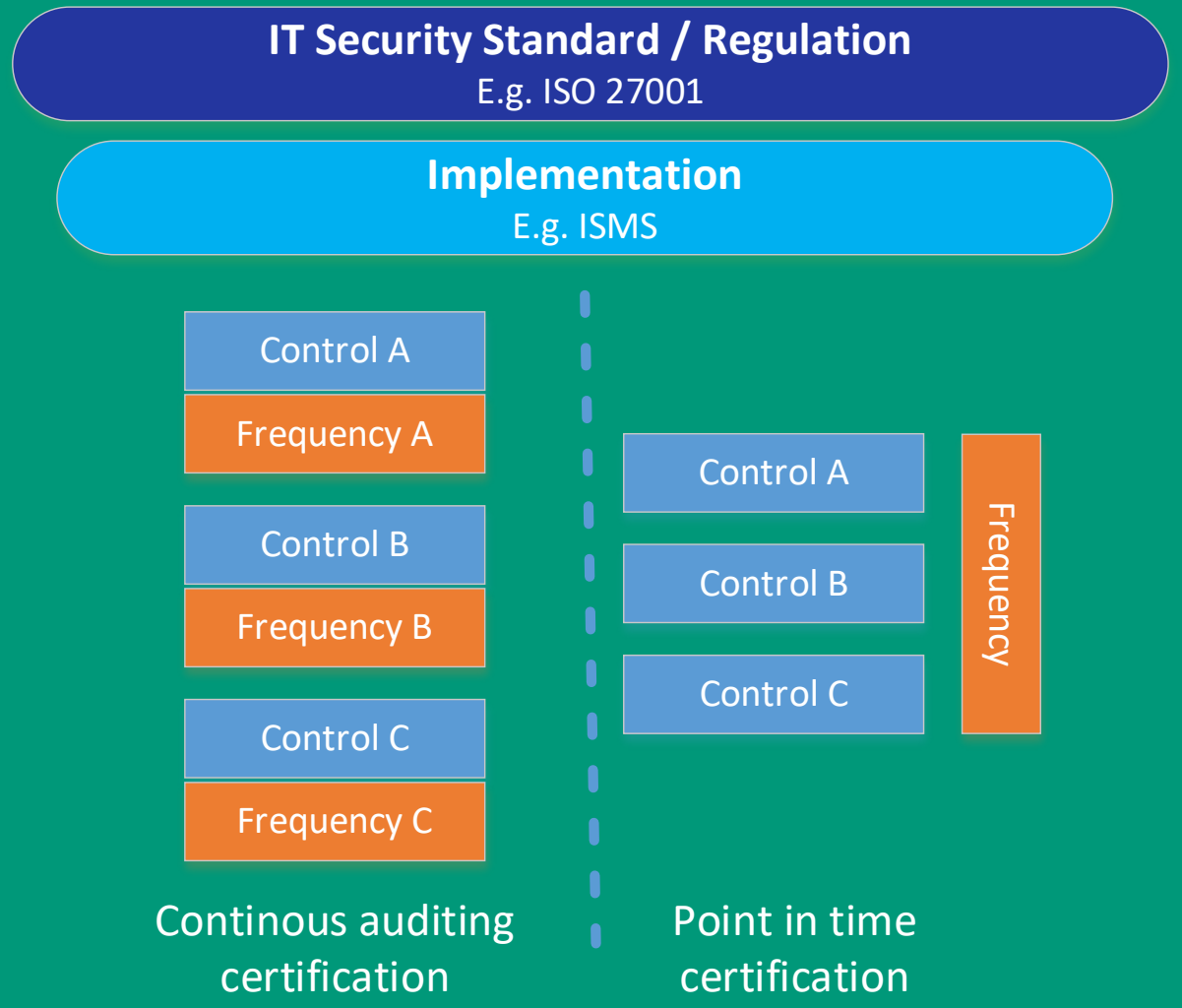
1

Certification in Cloud Computing NOW

- **Cloud computing also means shift in and governance over security and privacy**
- from direct control
- to an indirect form of control
- **CSC have to rely on statements and confirmations of CSP**
- Code of conducts
- Attestations
- Certifications
- **Third party audits and certifications have become the most effective solution to increase the level of trust**
- performed annually or bi-annually
- **Interim changes are made to security and privacy practices go unaudited**
- While this may be an acceptable risk for some cloud customers, for others, these assurance gaps remain a strong barrier to cloud adoption.

Continuous Auditing based Certification

- **Basic Idea:**
- Assess the effectiveness of each control in a suitable frequency
- In this sense the effectiveness of a security mean gets checked and published according to its update frequency
- Goal:
  - Increase the assessment frequency of all applied security controls
  - Provide the real time status of the conformance to the standards.
- Methods:
  - Automation
  - Switch from a process diven audit to a data driven one.



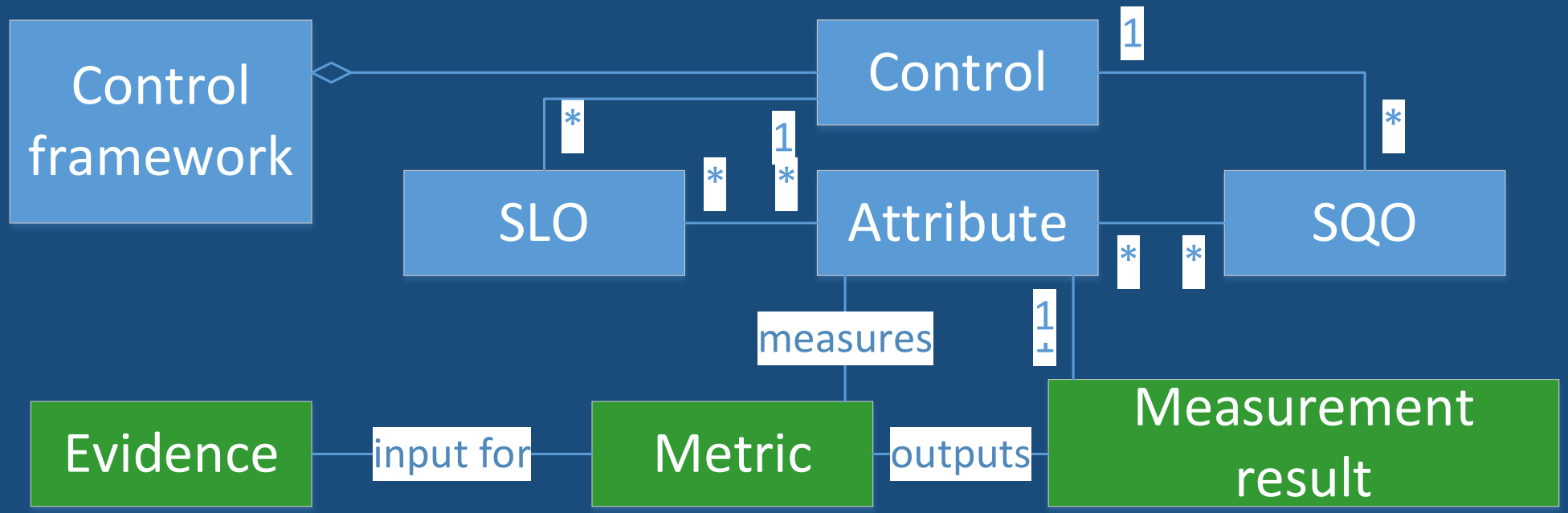
Fraunhofer FOKUS

Architecture

2

Fraunhofer FOKUS

Breakdown of a Control



1. **Each security sontrol framework consist of multiple controls.**
2. **Each Control is described via ist characterizing objectives.**
3. **Objectives are decribed via attributes.**
4. **The attributes are getting evaluated and assessed**

Fraunhofer FOKUS

Example for a breakdown

Control: …“Monitoring of network traffic“…

IaaS-Provider

Objectives: … „incoming and outgoning traffic on packet level“ …

Attributes: Number of analyzed packages, Number of unanalyzed packages, types of packages.

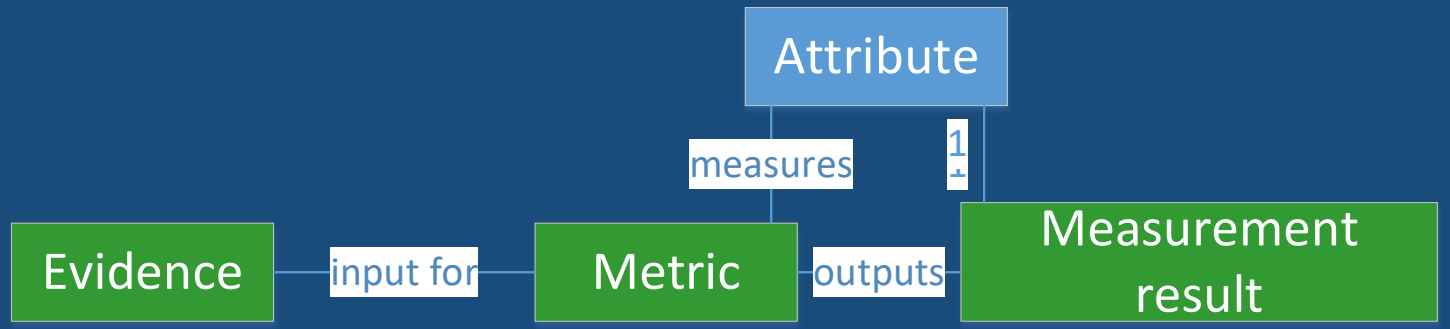
SaaS-Provider (Email)

Objectives: … „incoming and outgoing emails have to be checked“ …

In case of a in-house IT-infrastructure: „ also inspect on packet layer“

Attributes: Mails scanned for malware, unscanned packages

Measurement of an attribute



- **Qualitative or quantitative assessment on an attribute**
- **Evidence (raw data)**
- Log files, data bases, documents, etc.
- The type of the evidence detemines if its assesment can be automated
- **Metric**
- Metric is a standard for a measurement.
- transforms the evidence into the measurement result.
- **Measurement result**
- Out of a metric
- Provides the value and unit, which describes the attribute

Fraunhofer FOKUS

Data normalization

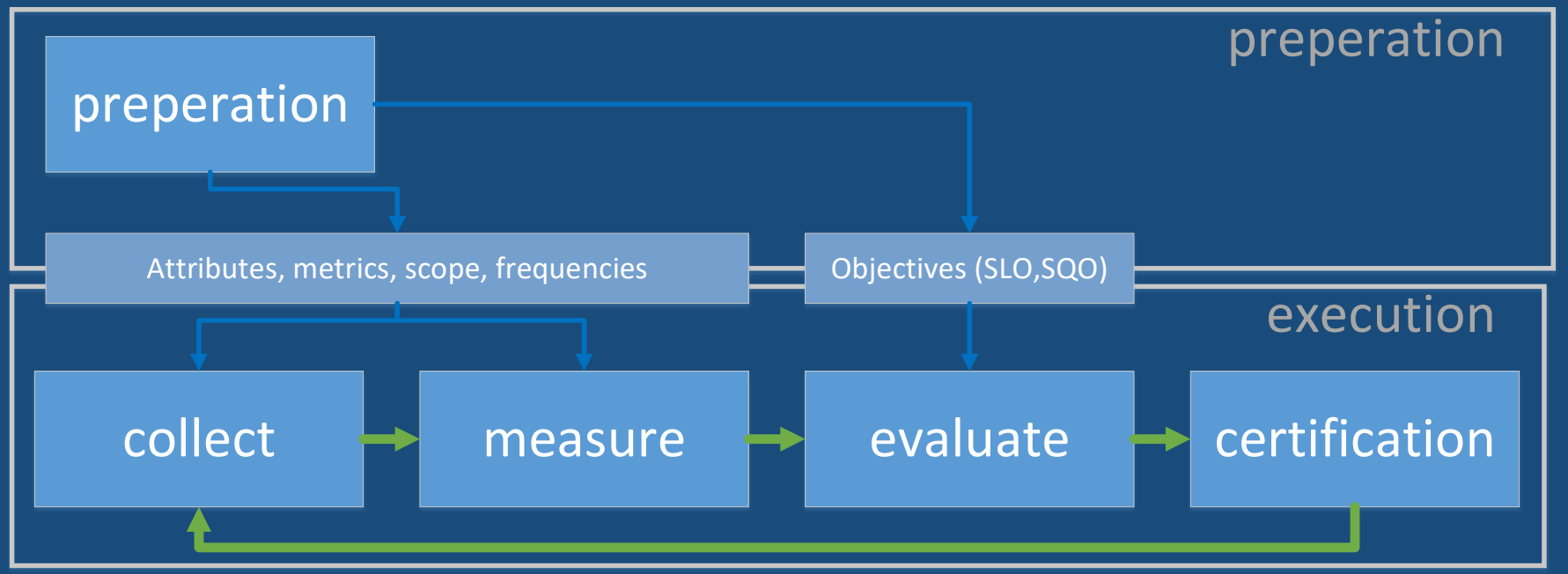
- **Problem: the data produced by IT-infrastructures is not in a representation that allows for a direct usage for the assessment of the fulfillment of conformity**
- Often gathered for security related reasons.
- Give information on the security status
- Security requirements are often not made for specific IT-infrastructure.
  - This leads to a diversity of implementations.

- **Solution: EU-SEC Audit API**
- Each type of Evidence has its own Rest-Endpoint
- For each Type of evidence its defined which values and in which ways those have to be transmitted.
- The EU-SEC Audit API is an open standard, wich has to be implemented by the cloud service provider.
- It provides the audit inctance with the values needed for an assessment
- The implementation of the Audit API gets it self audited (traditionally ;))

Phases of CAC

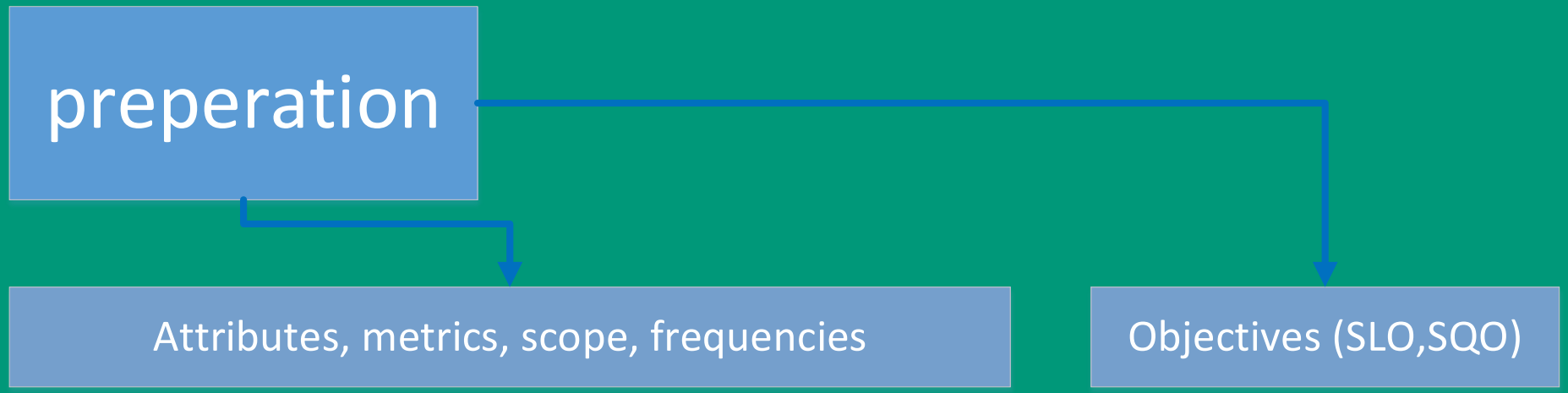
3

Phases of CAC



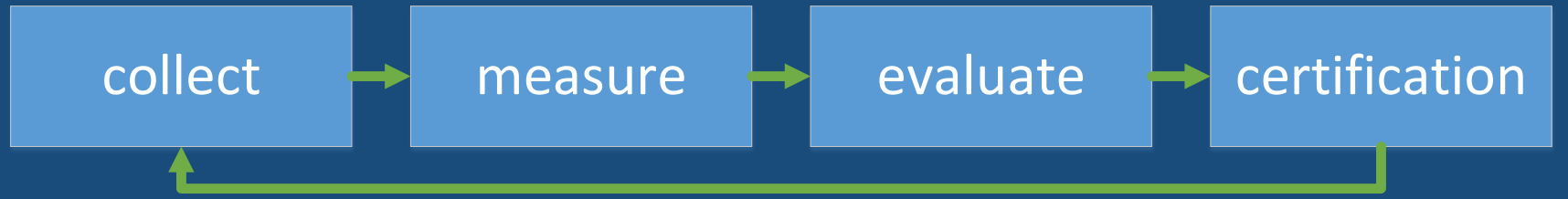
Fraunhofer FOKUS

Preparation Phase



- **Operationalization of the control in scope**
- Result:
  - Attributes, metrics, frequencies, scope and the objectives
- **Implementation of the EU-SEC Audit API**
- **This phase is audited ot even performed by a third party**

Execution Phase

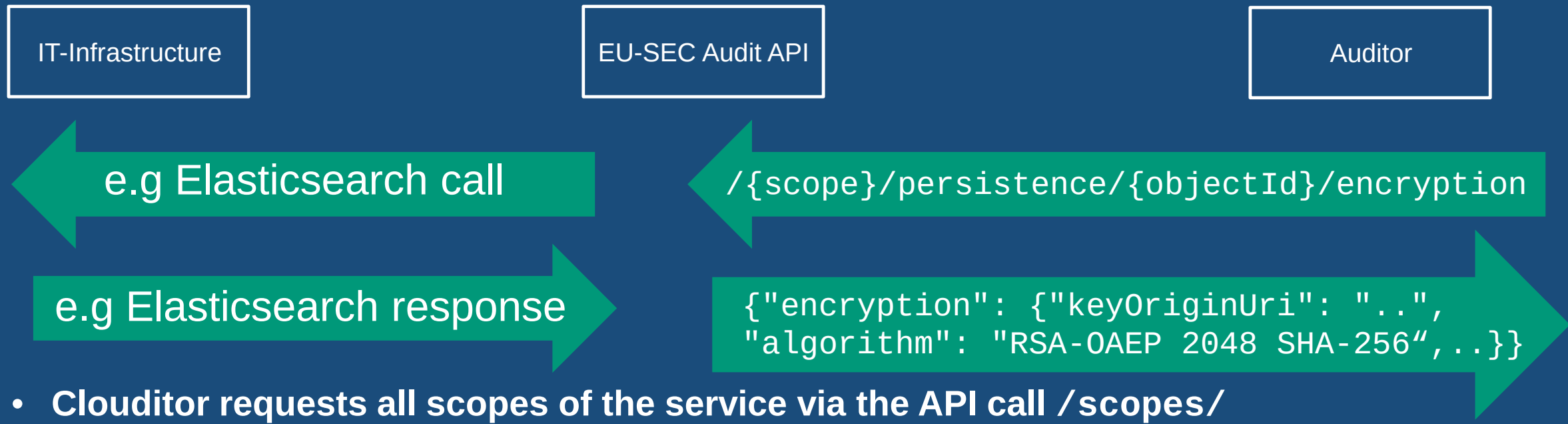


- **Continous assessment of the compliance status (according to the security and privacy requirements)**
- Continuous cyclic execution
- Idealy this process will be carried out with a high grade of automation.
  - As of today It requires still a lot of human intervention.

1. Collection phase: facilitates the collection of data for the automated assessment as well as for the non-automated assessment.
2. Measurement: transforms the collected raw data into a usable measurement result.
3. Evaluation phase: compliance status with the certification goal is determined
4. Certification Phase: an idependen third party authority evaluates and publishes the compliance status.

Fraunhofer FOKUS

Practical usage of the Audit API



- **Clouditor requests all scopes of the service via the API call `/scopes/`**
- **For each identified scope, the tool requests needed evidence for each object using the `/{scope}/objects/` end-point.**
- **For each objectId on each scope the encryption information is gathered by the API call `/{scope}/persistence/{objectId}/encryption`.**

Fraunhofer FOKUS

Certification schema

- **3 Models:**
- Continuous self-assessment auditing
  - Cost and time saving
  - No auditor involvement
- Extended Certification with Continuous Self-assessment
  - Combines self-assessment with traditional certification
  - Uses the same scope as the traditional certification
- Continuous certification
  - Each control has to be check continuously
  - Assessment is done by a third party

Fraunhofer FOKUS

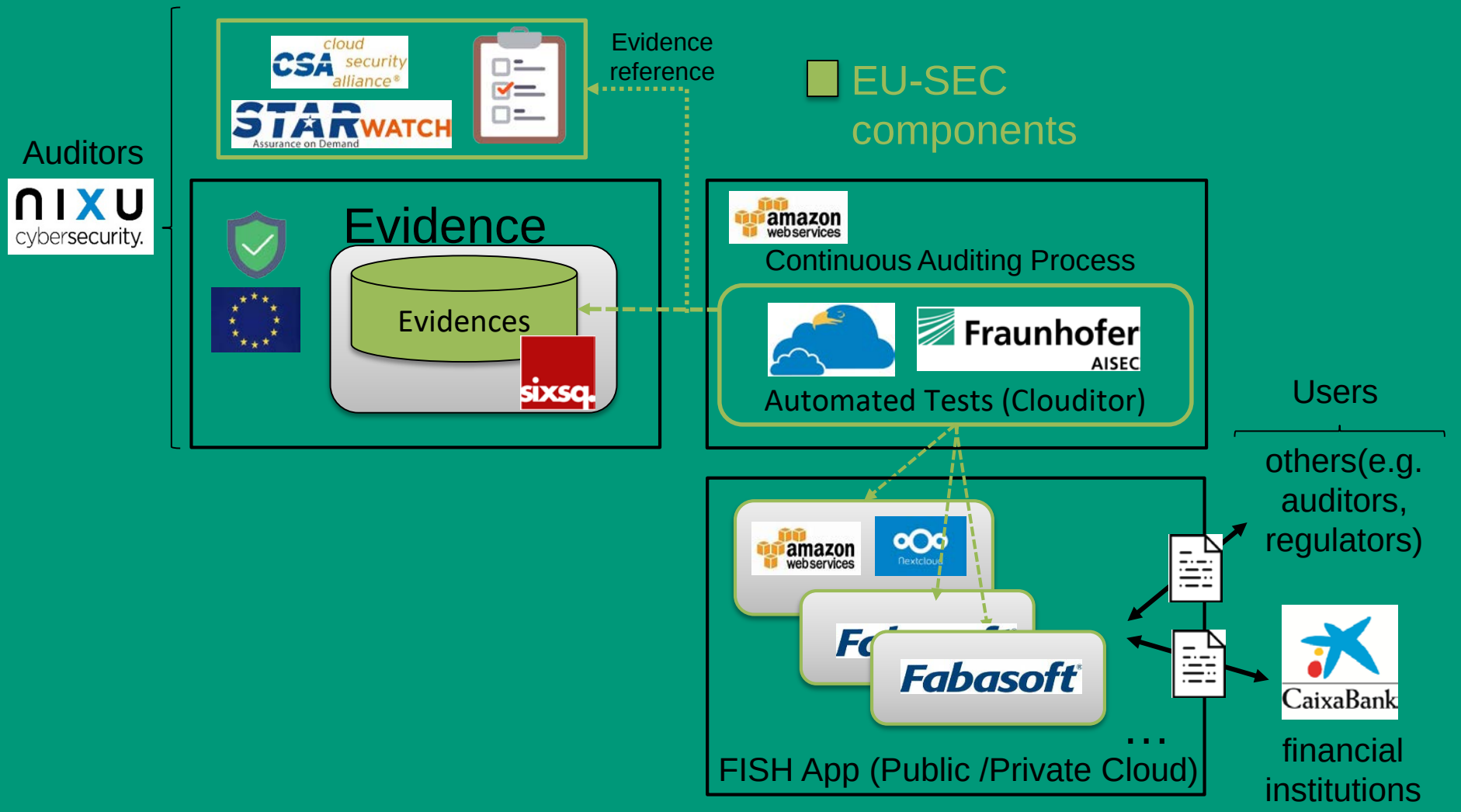
Pilot

4

Pilot

- **Inside the EU-Sec Project we’ve evaluated CAC in a Pilot.**
- **We wanted to show the applicability with different IT-Infrastructures.**
- **Use case from the banking sector (Project partner CaixaBank)**
- Excange of private personal data between banks and regulators
- The scope of the pilot was set by CaixaBank
- Subset of relevant controls.
- CAC serves the continuous assurance of the fulfillment of the requirements
- Controls are based on the CSA Cloud Control Matrix.

Pilot



Fraunhofer FOKUS

Conclusion and Future Work

- **Continuous Auditing introduces an enhancement to the classical “point in time”-certification**
- CAC is extremely relevant for specific sectors like banking or health
- Increased the audit frequency, with a method that keeps the overhead low.
- **We have provided a solution that helps to reduce the problem of high implementation efforts for continuous auditing by defining a clear and simple API**
- **CAC is not bound to a specific standard**

- **In its current state CAC is mote cost intensive that a traditional audit.**
- Just 25% of the Controls in current standards are fully automatable.
- To reduce cost the level of automation has to be increased.
- Need for further research and development
  - Natural Language Processing
  - DSL for Security controls and requirements

Thanks for your attention

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
info@fokus.fraunhofer.de
www.fokus.fraunhofer.de

Dorian Knoblauch
dorian.knoblauch@fokus.fraunhofer.de

Fraunhofer FOKUS