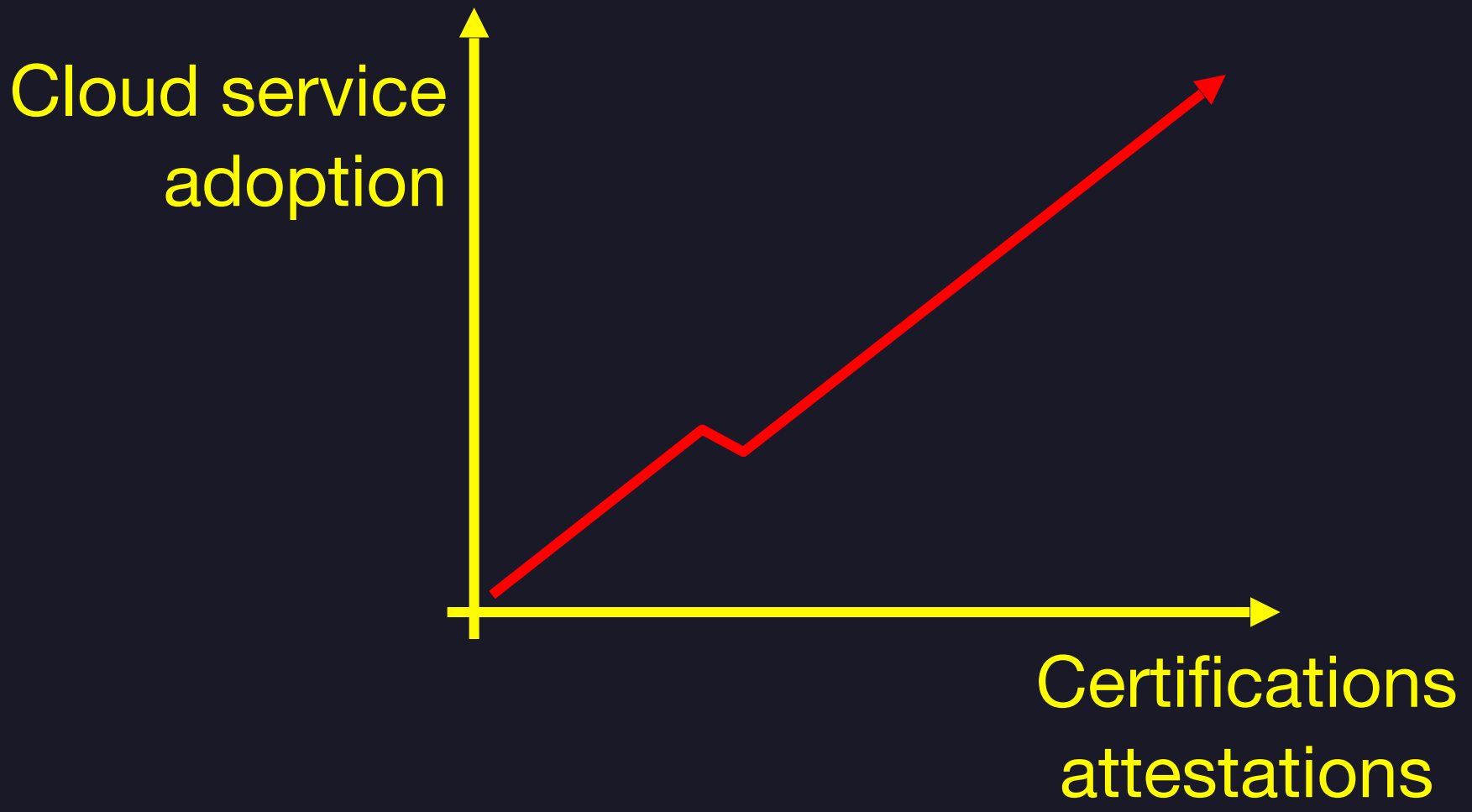
CSA | EU Summit 2020

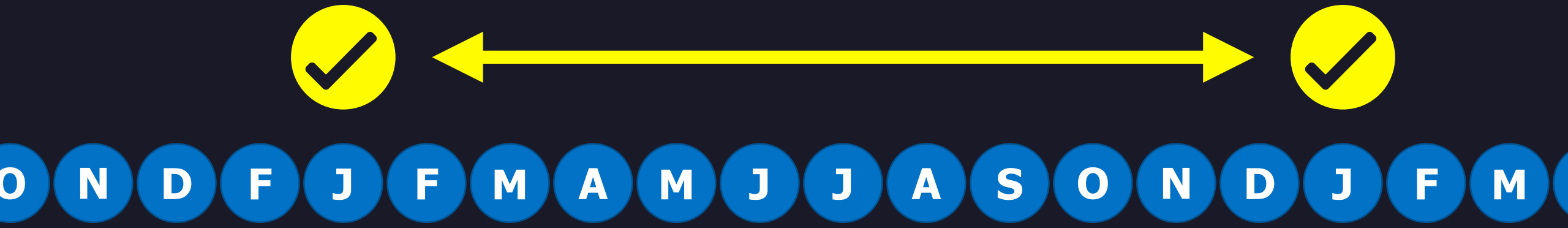
Continuous Audit-Based Certification

Alain Pannetrat, Senior Researcher, CSA

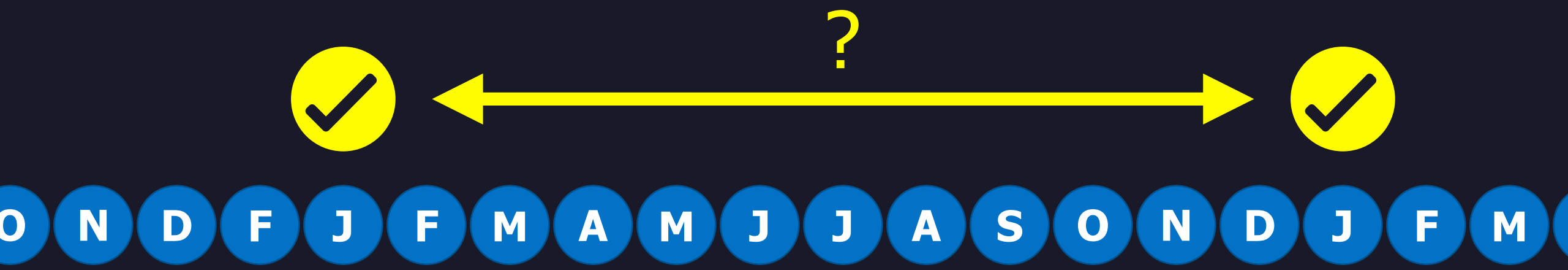
CERTIFICATION IS A SUCCESS STORY



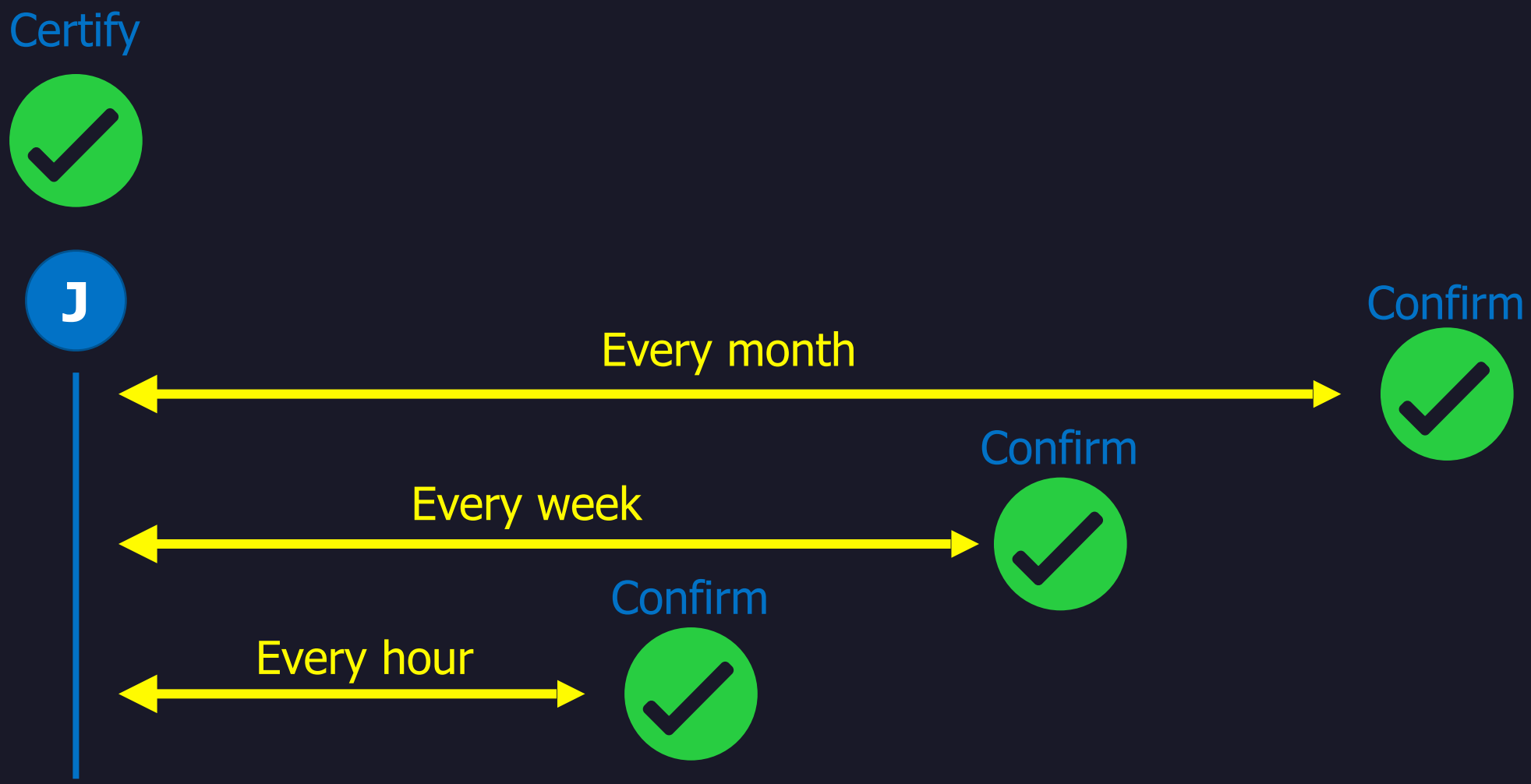
TRADITIONAL CERTIFICATION



TRADITIONAL CERTIFICATION



CONTINUOUS CERTIFICATION



APPLICATIONS: NOT JUST CERTIFICATION

Continuous (audit-based) certification

Continuous self-assessments

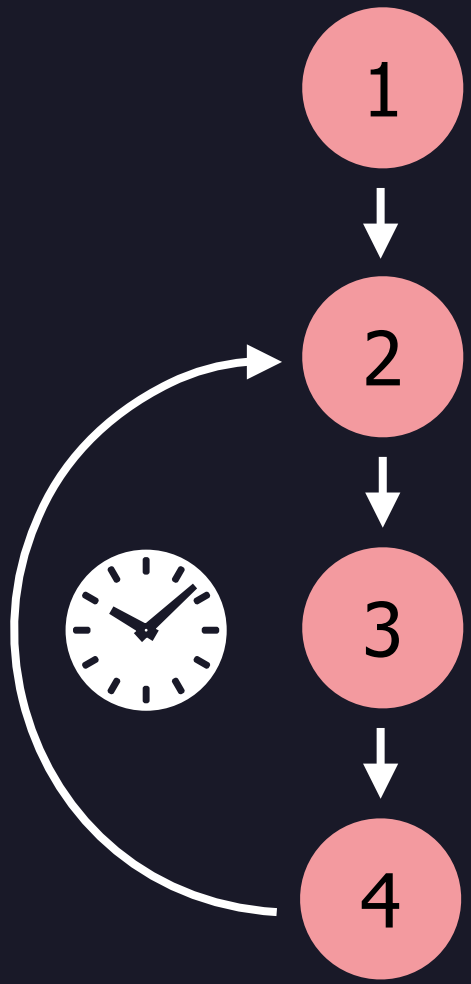
External information technology services

Internal information technology services

CSA | EU Summit 2020

How?

CONTINUOUS AUDITING



1. Start with a compliant system
2. Collect evidence: logs, API calls, security events, …
3. Measure: evaluate a security attribute based on collected evidence.
4. Assess: Compare measurement result with predefined objective

DESCRIBING A CERTIFICATION TARGET

Security attributes: WHAT we measure.

Metrics: HOW we measure.

Frequency: WHEN we measure.

Service Level Objectives/Service Qualitative Objectives: Condition for compliance.

EXAMPLE

Security attributes: **Password strength**

Metrics: Password length in characters **L** and number of different character types **N**

Frequency: Test **every 60 minutes** with a script

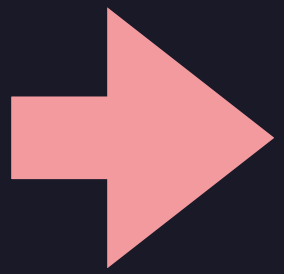
Service Level Objectives: **L>=8** and **N>=2**

TRADITIONAL VS. CONTINUOUS

"Traditional" certification

Control objectives

Manual evaluation



"continuous" audit-based certification

Security Attributes

Metrics

Service Level Objective & Service Qualitative Objective

Automated evaluation

ISO/IEC 19086-1

EXAMPLE: CONTROL VS SLO

A requirement: automate as much as possible

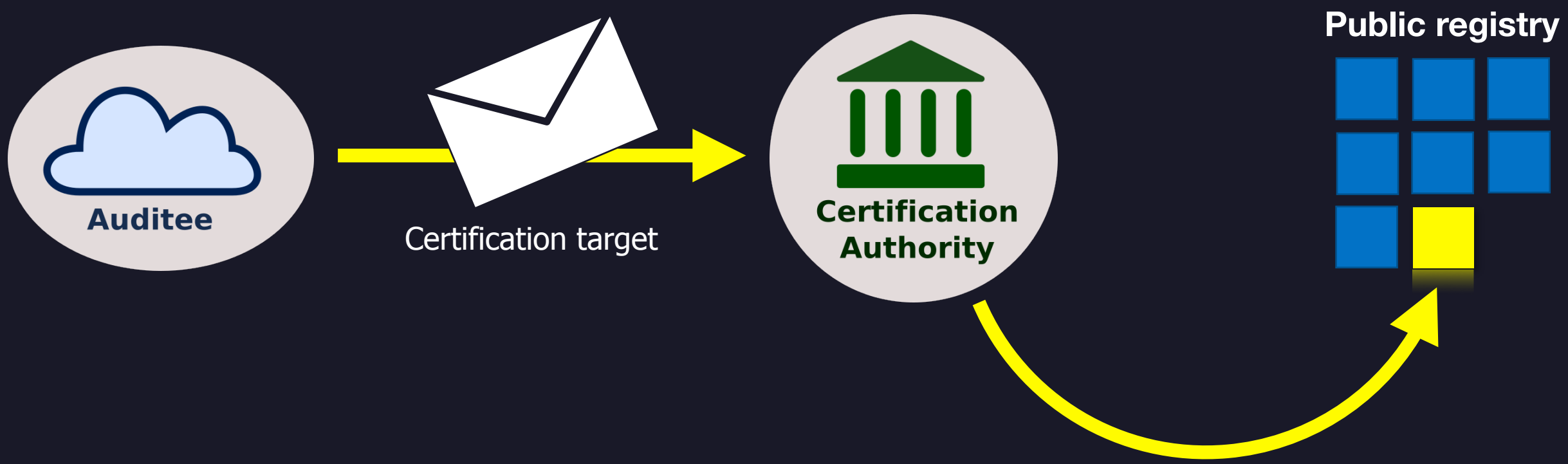
CONTROL OBJECTIVES	SERVICE LEVEL OBJECTIVES
"Business continuity plans shall be documented and tested regularly"	• Percentage of backup restoration tests per month • Percentage of backup restoration failures per month • Maximum recovery time • Recovery point actual (RPA) Check: Monthly, daily, hourly…

CSA | EU Summit 2020

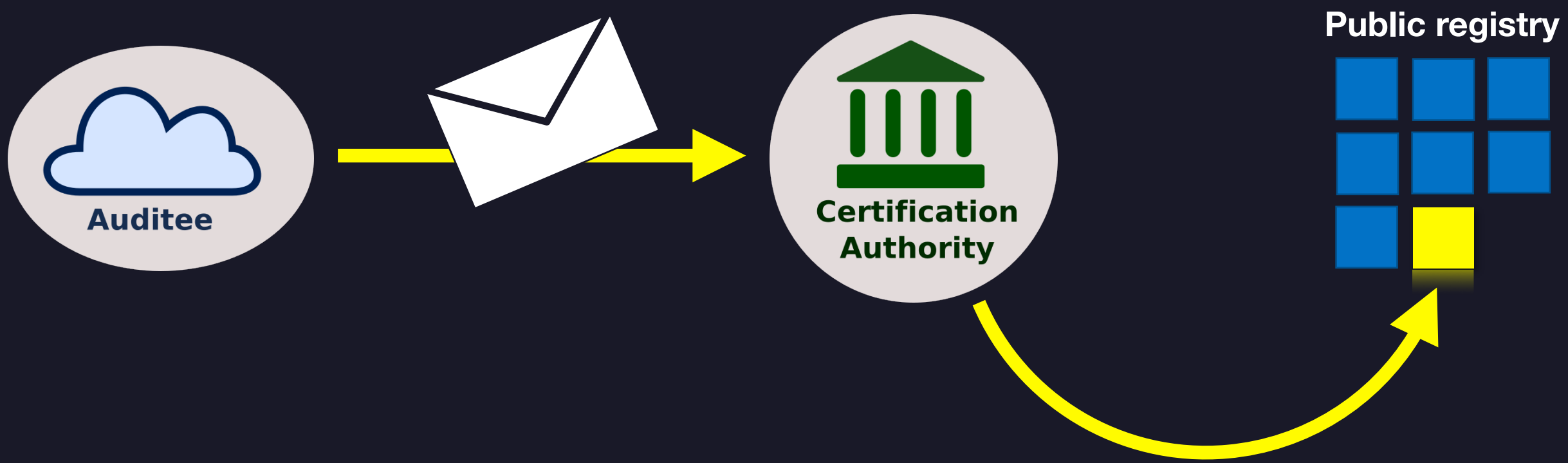
Self-assessments and Certifications

Let’s run a continuous assurance framework!

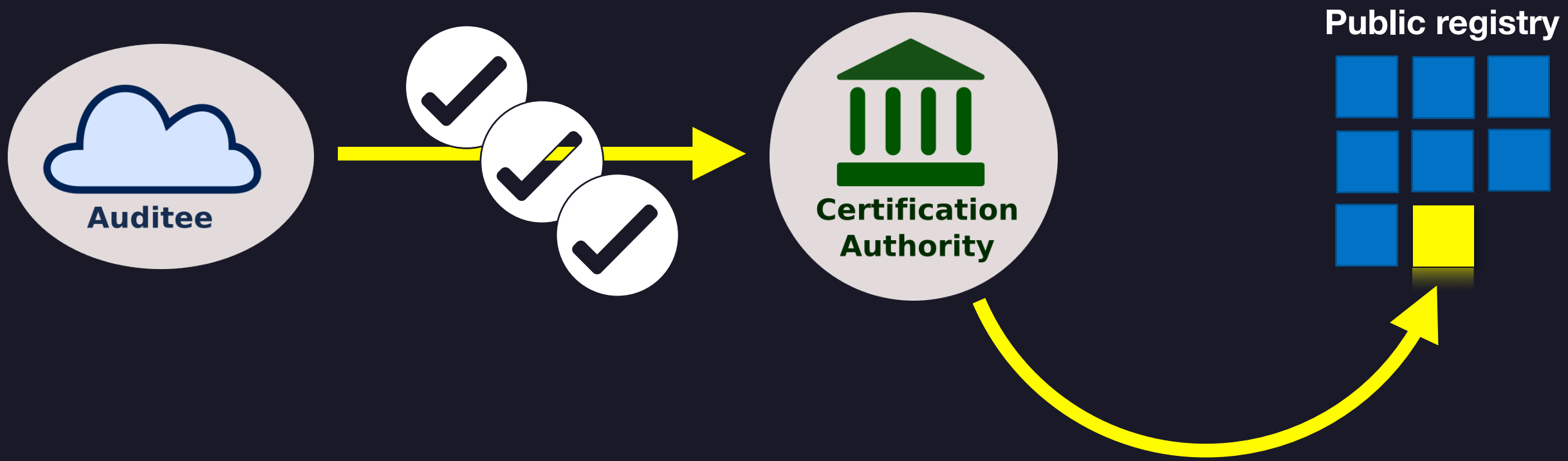
START OF THE PROCESS



START OF THE PROCESS

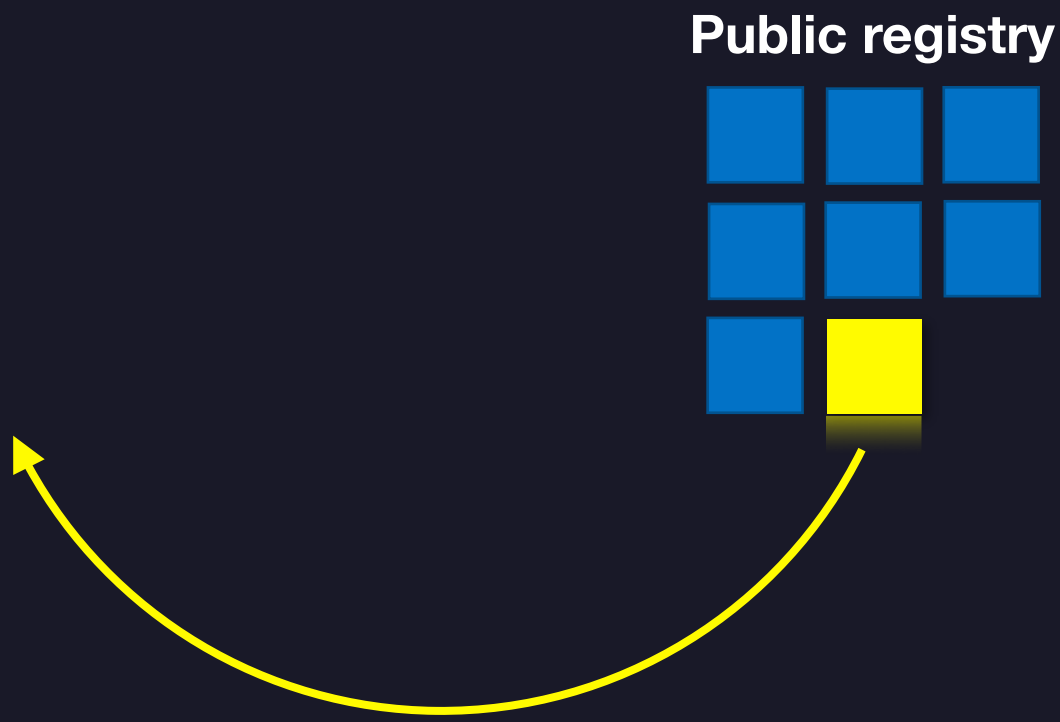


RUNNING THE PROCESS



PUBLIC REGISTRY

Scope of information system
Start / End date
Last compliance date
Status: OK, Pending, Ended



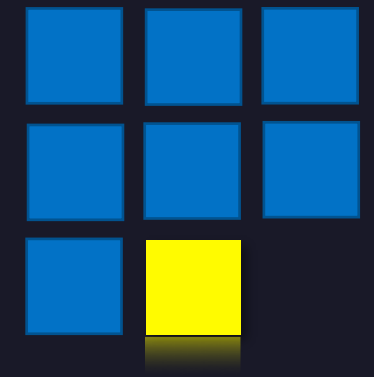
DEALING WITH NON-COMPLIANCES

What is a non-compliance?

1) If an SLO or SQO is not met
2) If a result is not submitted within agreed frequency.

Dealing with non-compliances

1) Last compliance date is not updated in the registry anymore
2) If non-compliance(s) persist for more than X days (“grace period”), the service is removed from the registry.



3 ASSURANCE MODELS

Continuous self-assessment:

- User defines the certification target, submits it to the CA, reports on compliance.

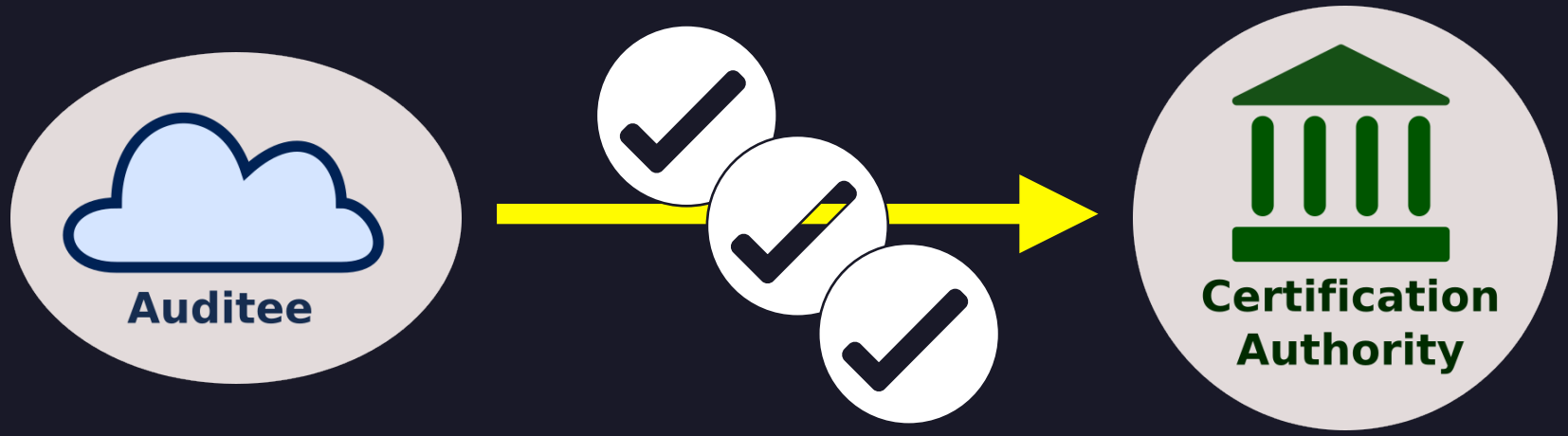
Extended certification with continuous self-assessment:

- User undergoes "classic" certification with third party auditor.
- Third party auditor also checks certification target + tools are fit for purpose & trustworthy
- User does self-assessment and reporting alone

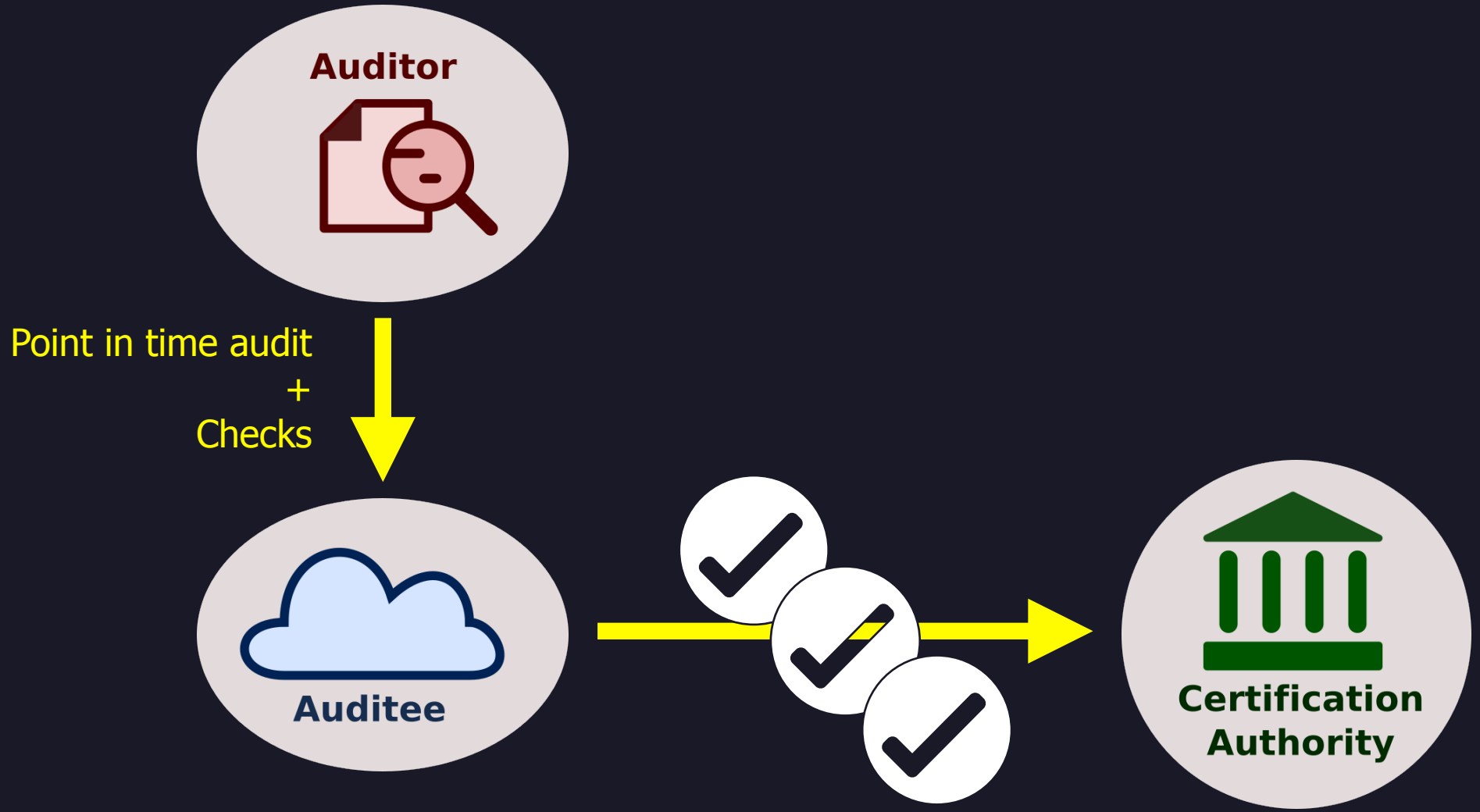
Continuous certification:

- User undergoes "classic" certification with third party auditor.
- Third party auditor also checks certification target + tools are fit for purpose & trustworthy
- User does assessment and reporting under the supervision of the third party auditor

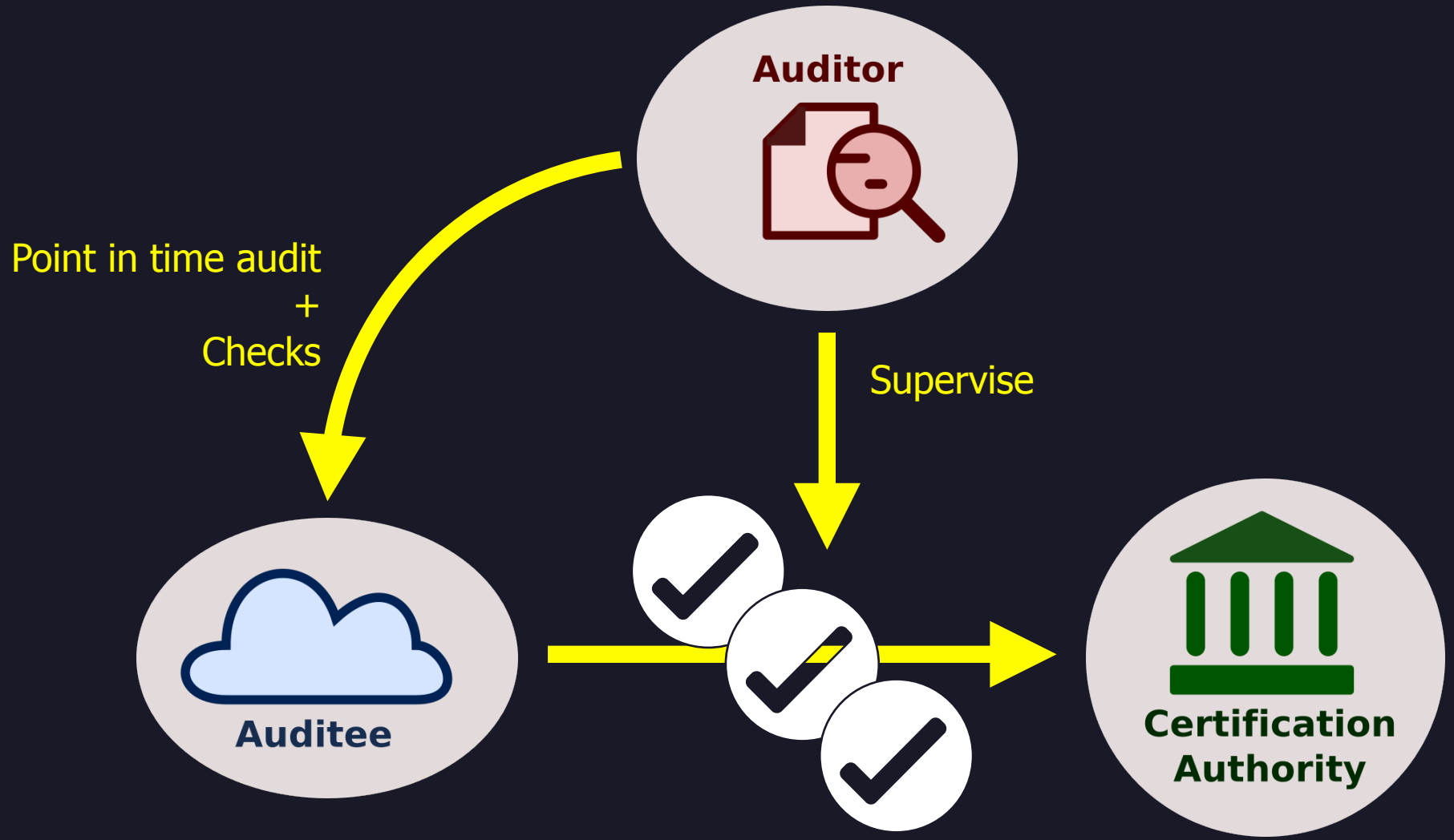
SELF ASSESSMENT



EXTENDED CERTIFICATION + CONTINUOUS SELF-ASSESSMENT



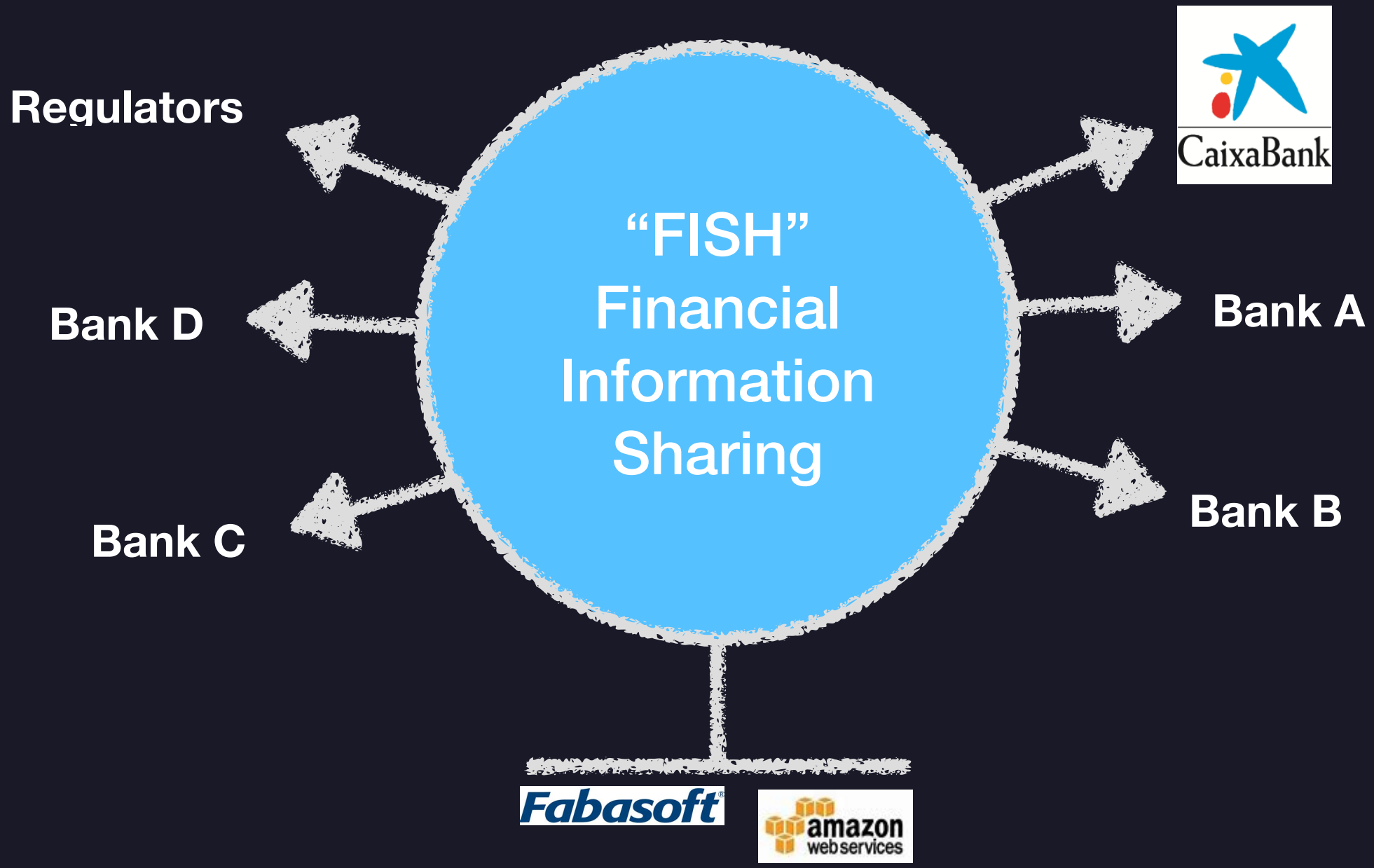
CONTINUOUS CERTIFICATION

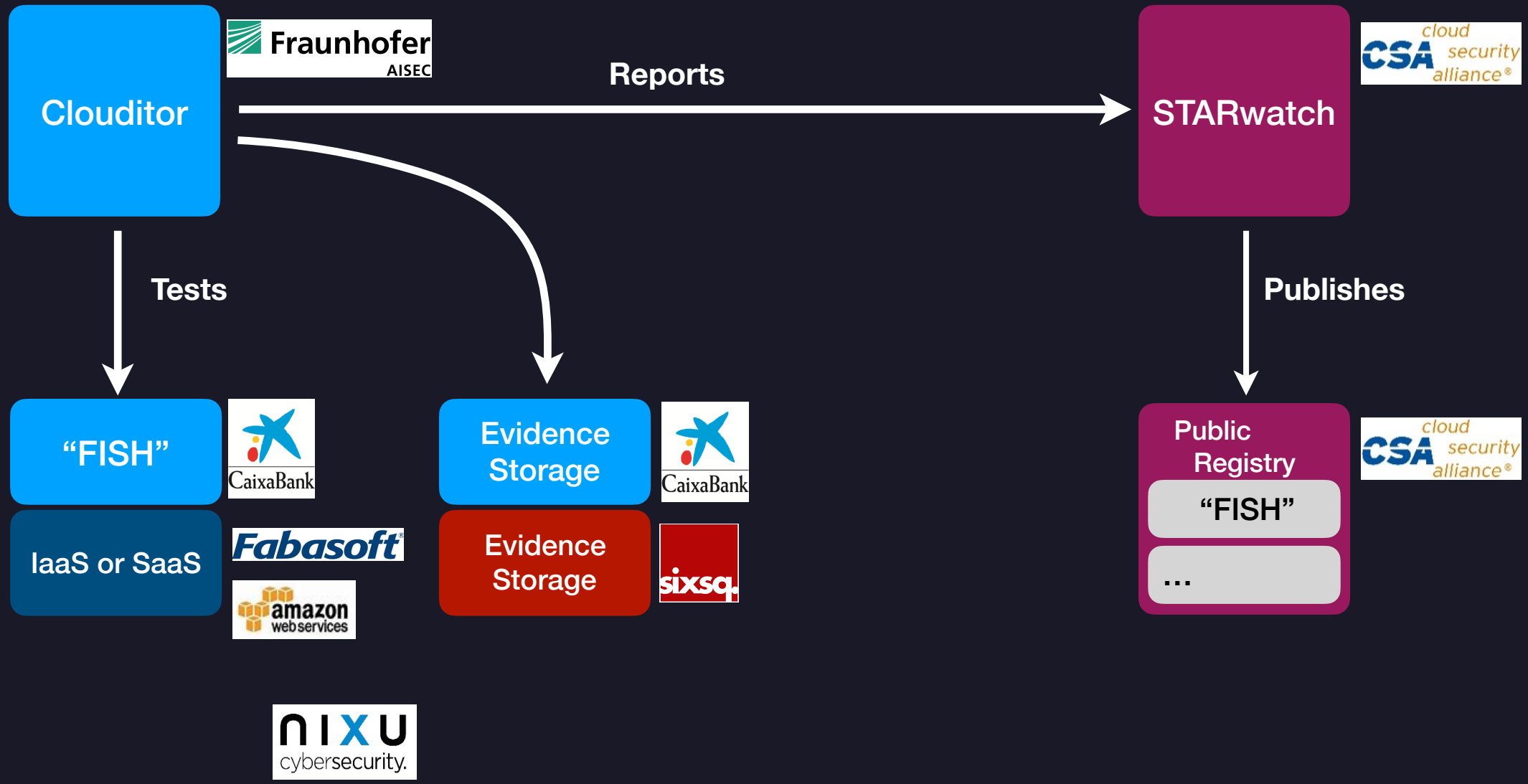


CSA | EU Summit 2020

EU-FUNDED PILOT

EU-SEC PROJECT


Regulators
Bank D
Bank C
"FISH"
Financial
Information
Sharing
CaixaBank
Bank A
Bank B
Fabasoft
amazon
web services


Clouditor
Fraunhofer AISEC
Reports
STARwatch
cloud security alliance
Tests
Publishes
"FISH"
CaixaBank
IaaS or SaaS
Fabasoft
amazon web services
Evidence Storage
CaixaBank
Evidence Storage
sixsq
Public Registry
"FISH"
...
cloud security alliance
nixu cybersecurity.

CSA | EU Summit 2020

Challenge

Metrics

WHAT NEXT?

CSA is running a Continuous Audit Metrics Working Group

- Join us!

CSA is already experimenting with “continuous” assurance

- Submit a CAIQ self-assessment on a monthly basis

Our aim: First Continuous Certification in 2021.

CSA Summit at RSA Conference 2020

apannetrat@cloudsecurityalliance.org