A Gentle Introduction to CSA Audit-based Continuous Certification

Hing-Yan LEE (Dr.), Executive Vice President, APAC
Cloud Security Alliance

31 Jul 2020

GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA
Singapore Chapter

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT
- GLOBAL, NOT-FOR-PROFIT ORGANIZATION
- RESEARCH AND EDUCATIONAL PROGRAMS
- CLOUD PROVIDER CERTIFICATION – CSA STAR
- USER CERTIFICATION – CCSK
- THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD

Open Certification Framework

CSA OCF is an industry initiative to allow global, accredited, trusted certification of CSPs.


CERTIFICATION IS A SUCCESS STORY
Cloud service adoption
Certifications attestations

Traditional Certification

Traditional Certification

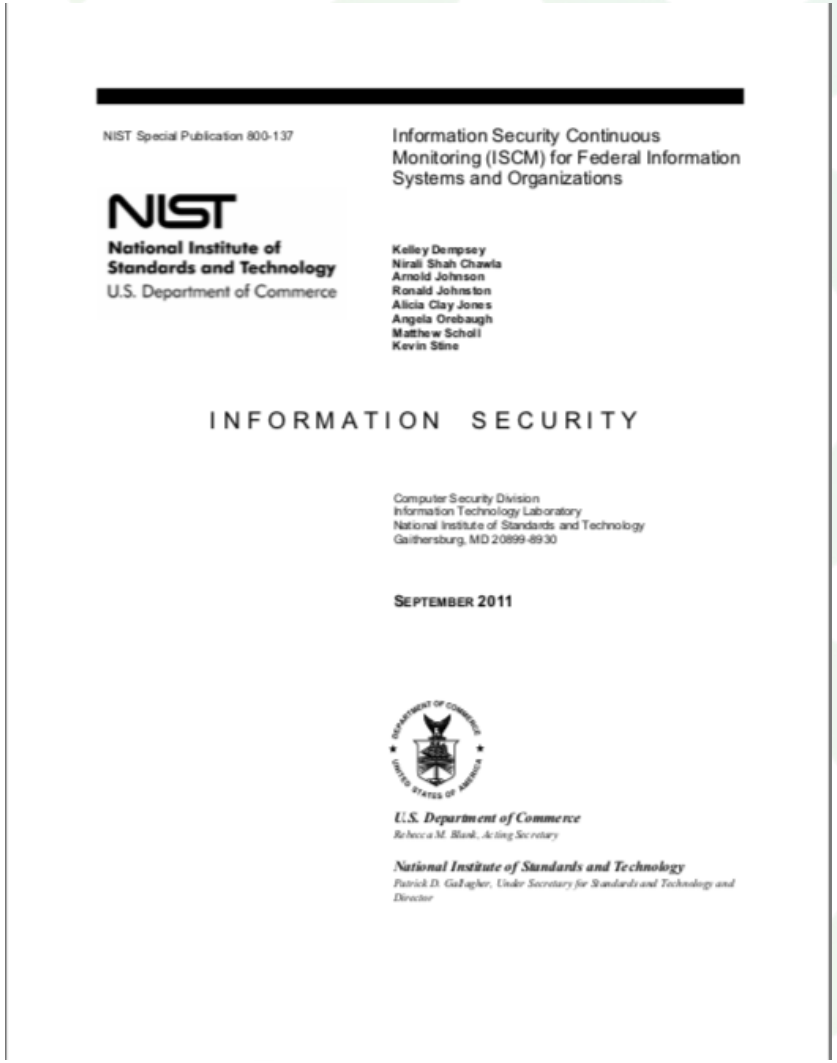
For come cloud customers in heavily regulated industries or with very sensitive data (e.g. banking, healthcare), (bi-)annual certifications are not enough.

They need CONTINUOUS assurance.

Continuous Certification

NIST

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, & threats to support organizational risk management decisions.



NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

SEPTEMBER 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Applications: Not Just Certification

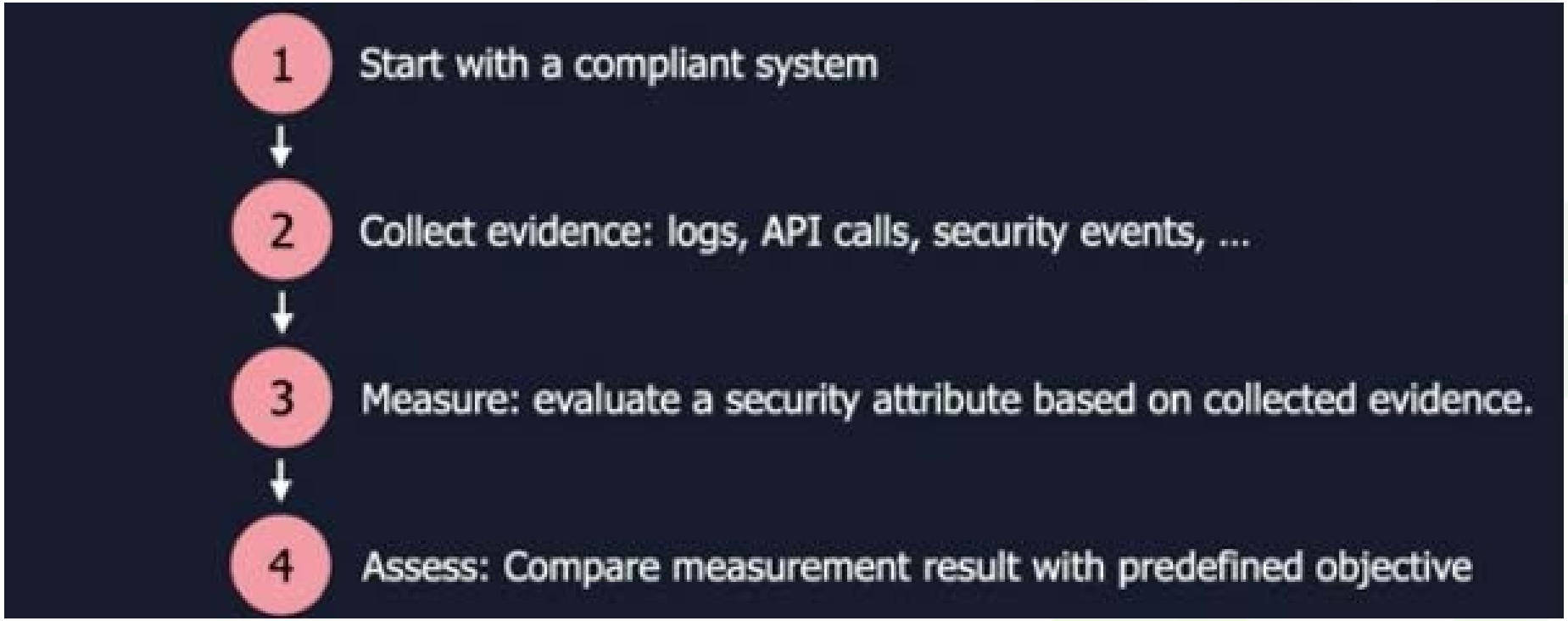
Continuous (audit-based) certification

Continuous self-assessments

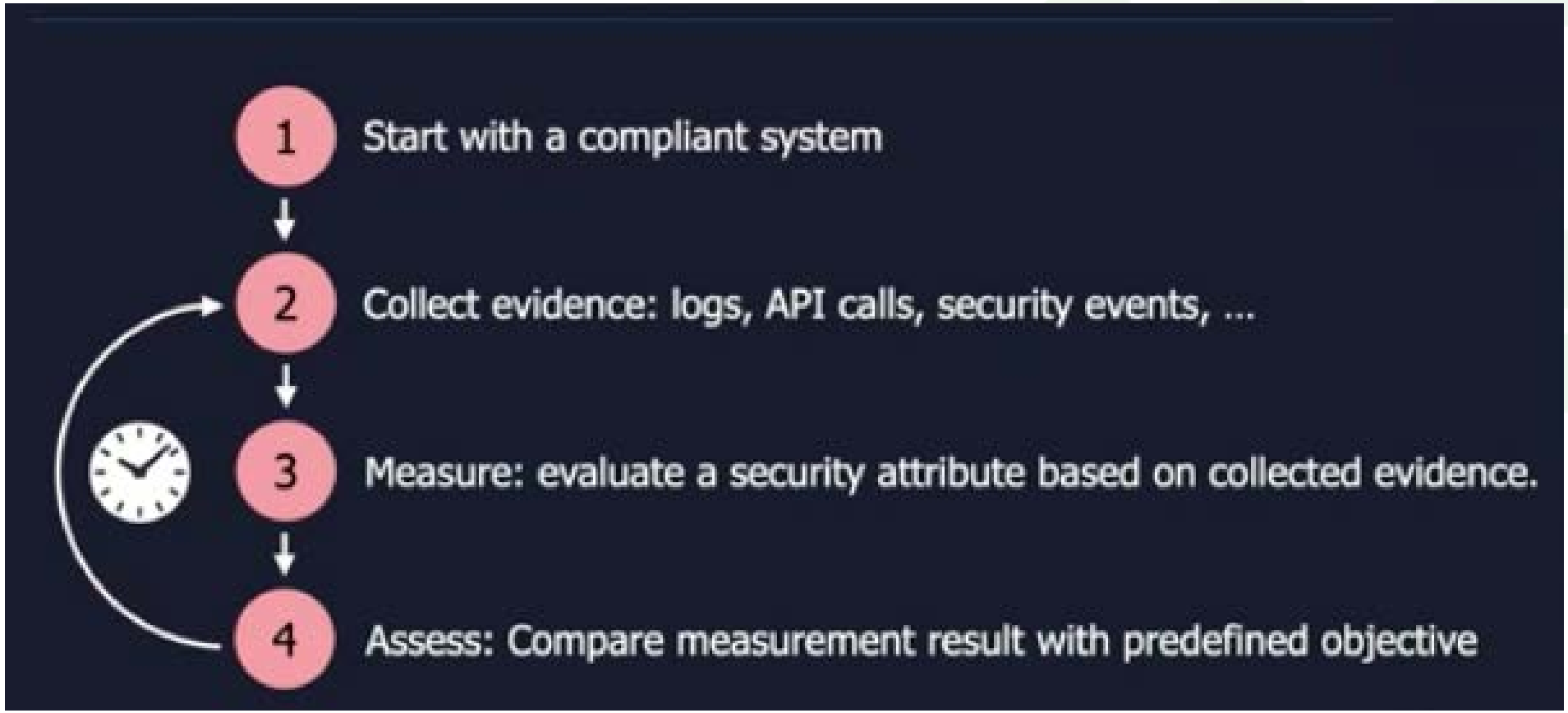
External information technology services

Internal information technology services

Continuous Auditing



Continuous Auditing



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.

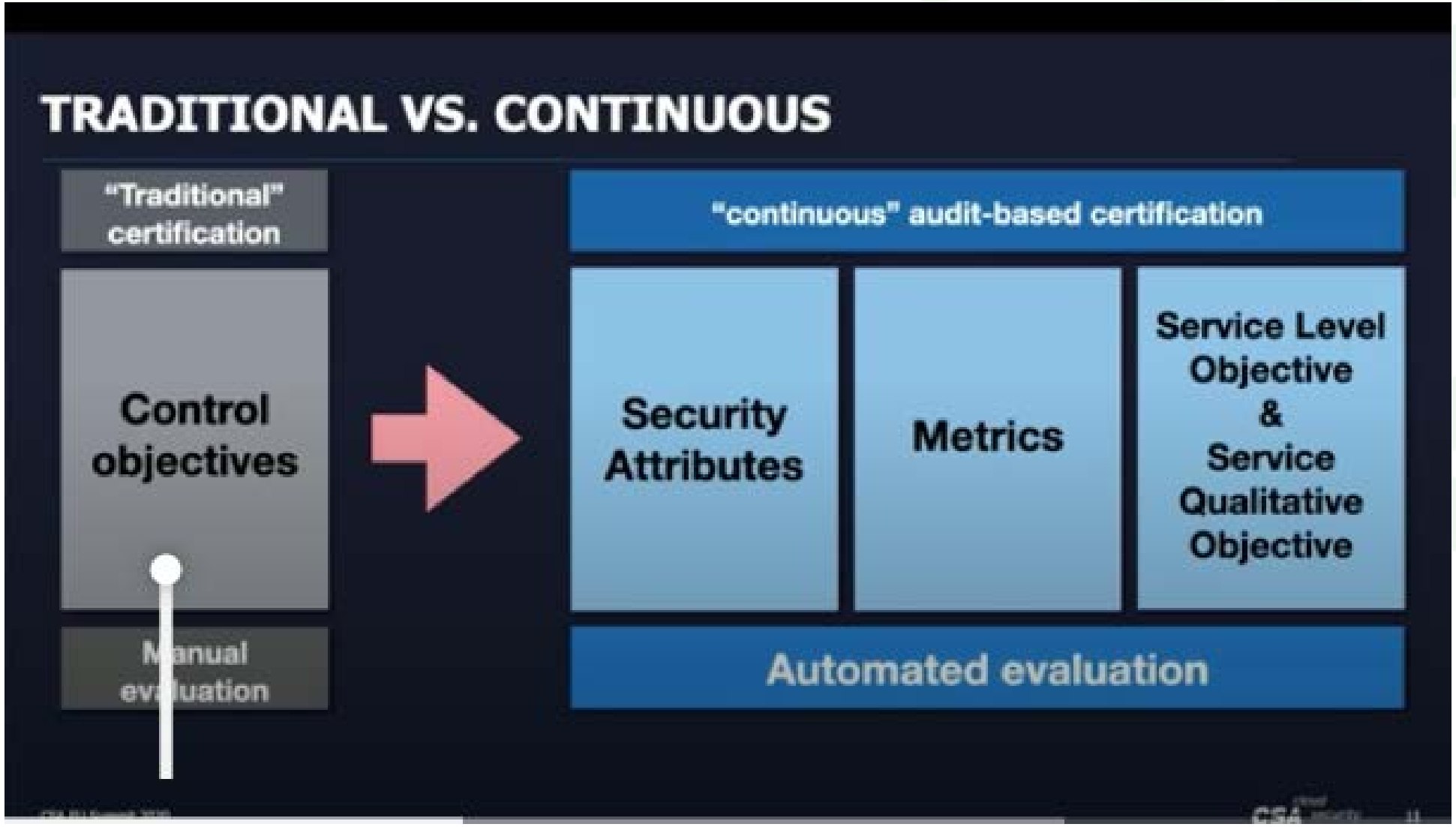
Example

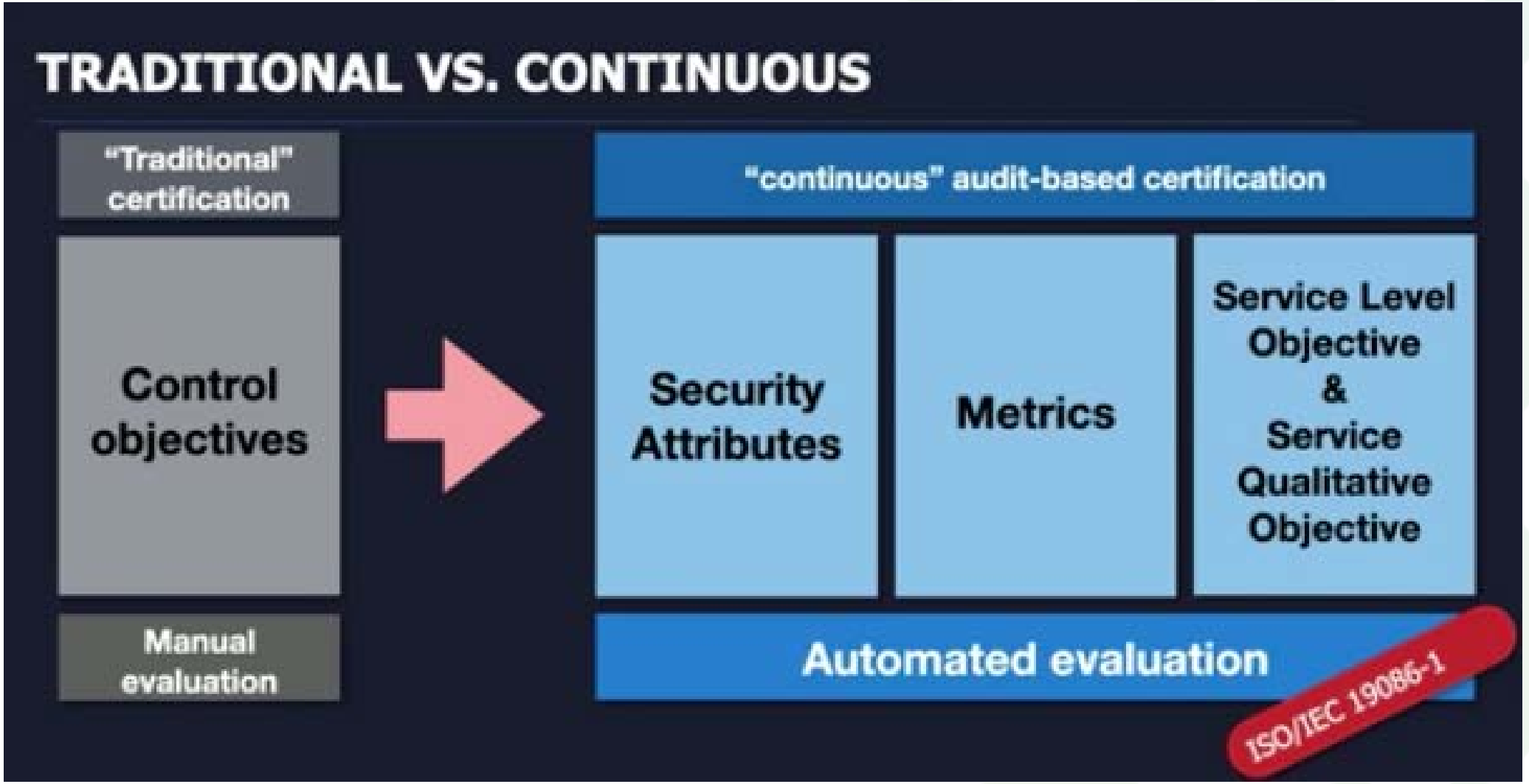
Security attributes: Password strength

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
"continuous" audit-based certification
Control objectives
Security Attributes
Metrics
Service Level Objective & Service Qualitative Objective
Manual evaluation
Automated evaluation

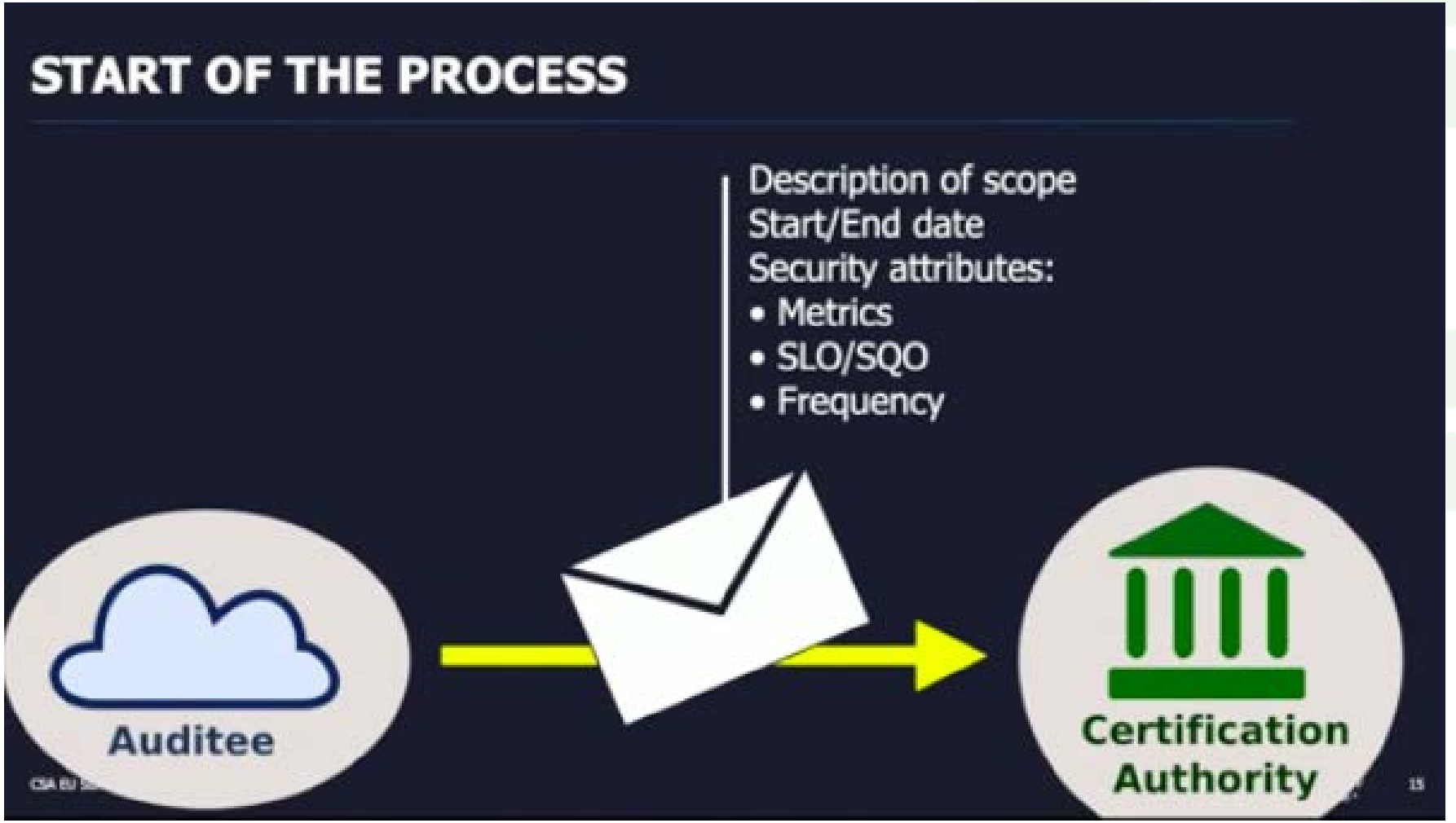

TRADITIONAL VS. CONTINUOUS
"Traditional" certification
Control objectives
Manual evaluation
"continuous" audit-based certification
Security Attributes
Metrics
Service Level Objective & Service Qualitative Objective
Automated evaluation
ISO/IEC 19086-1

EXAMPLE: CONTROL VS SLO

A requirement: automate as much as possible

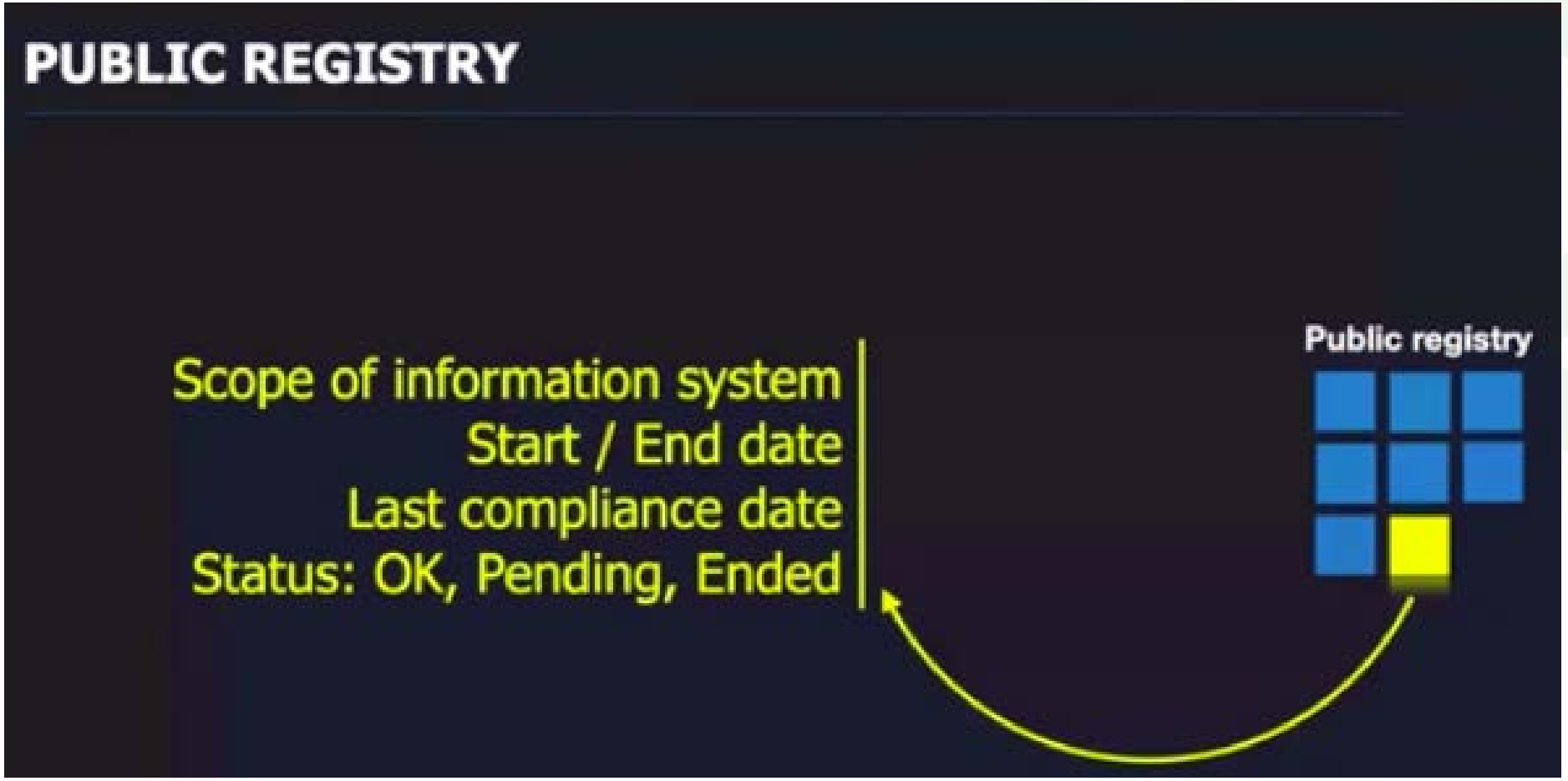
CONTROL OBJECTIVES	SERVICE LEVEL OBJECTIVES
"Business continuity plans shall be documented and tested regularly"	• Percentage of backup restoration tests per month • Percentage of backup restoration failures per month • Maximum recovery time • Recovery point actual (RPA) Check: Monthly, daily, hourly…

Running a Continuous Assurance Framework


START OF THE PROCESS
Description of scope
Start/End date
Security attributes:
• Metrics
• SLO/SQO
• Frequency
Auditee
Certification Authority


RUNNING THE PROCESS
Auditee
Certification Authority
Public registry

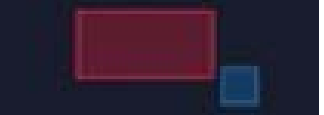
PUBLIC REGISTRY

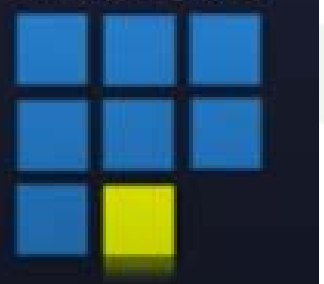


DEALING WITH NON-COMPLIANCES

What is a non-compliance?

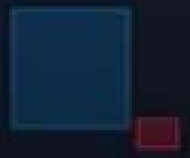
1) If an SLO or SQO is not met
2) If a result is not submitted within agreed frequency.





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

3 ASSURANCE MODELS

Continuous self-assessment:

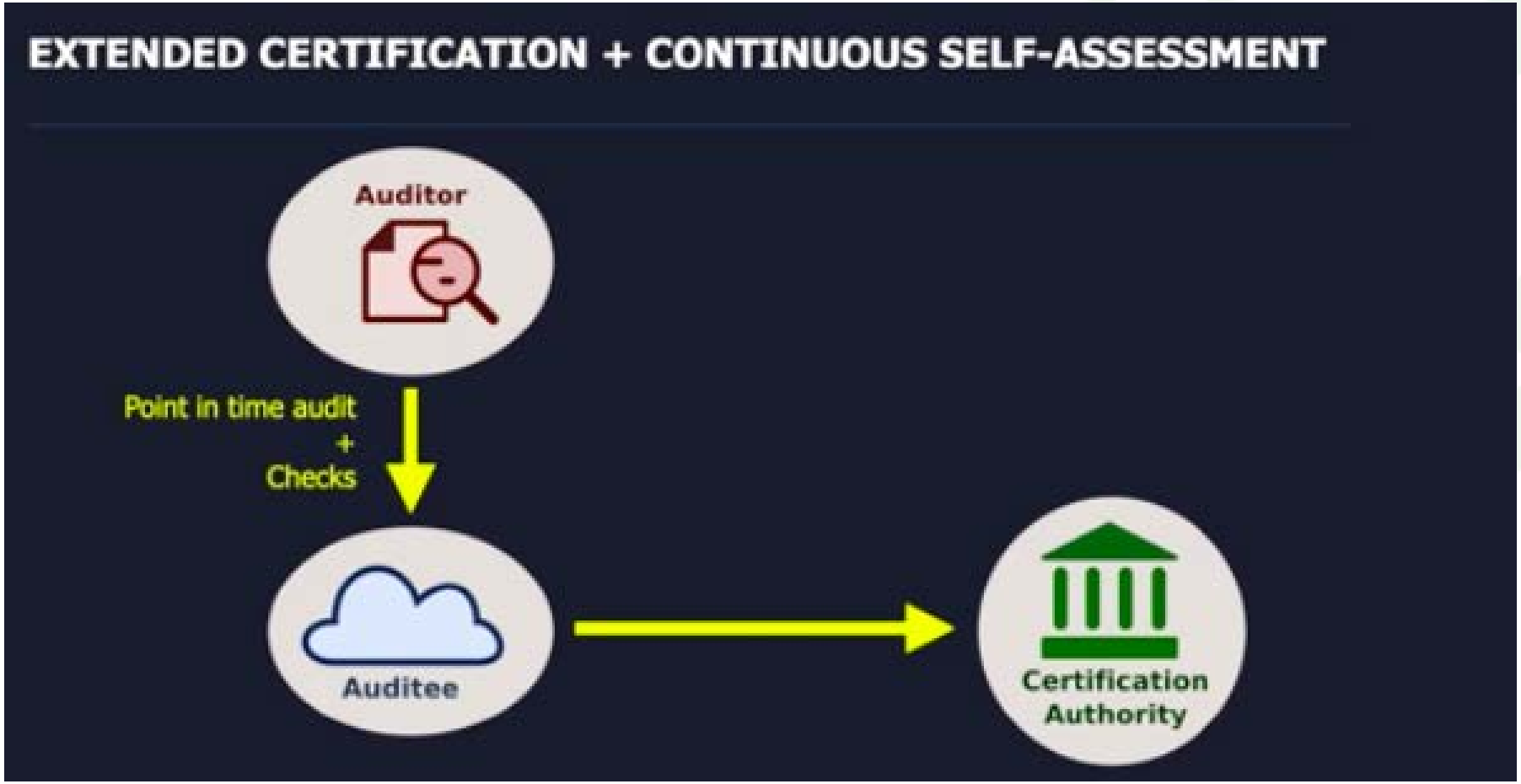
- User defines the certification target, submits it to the CA, reports on compliance.

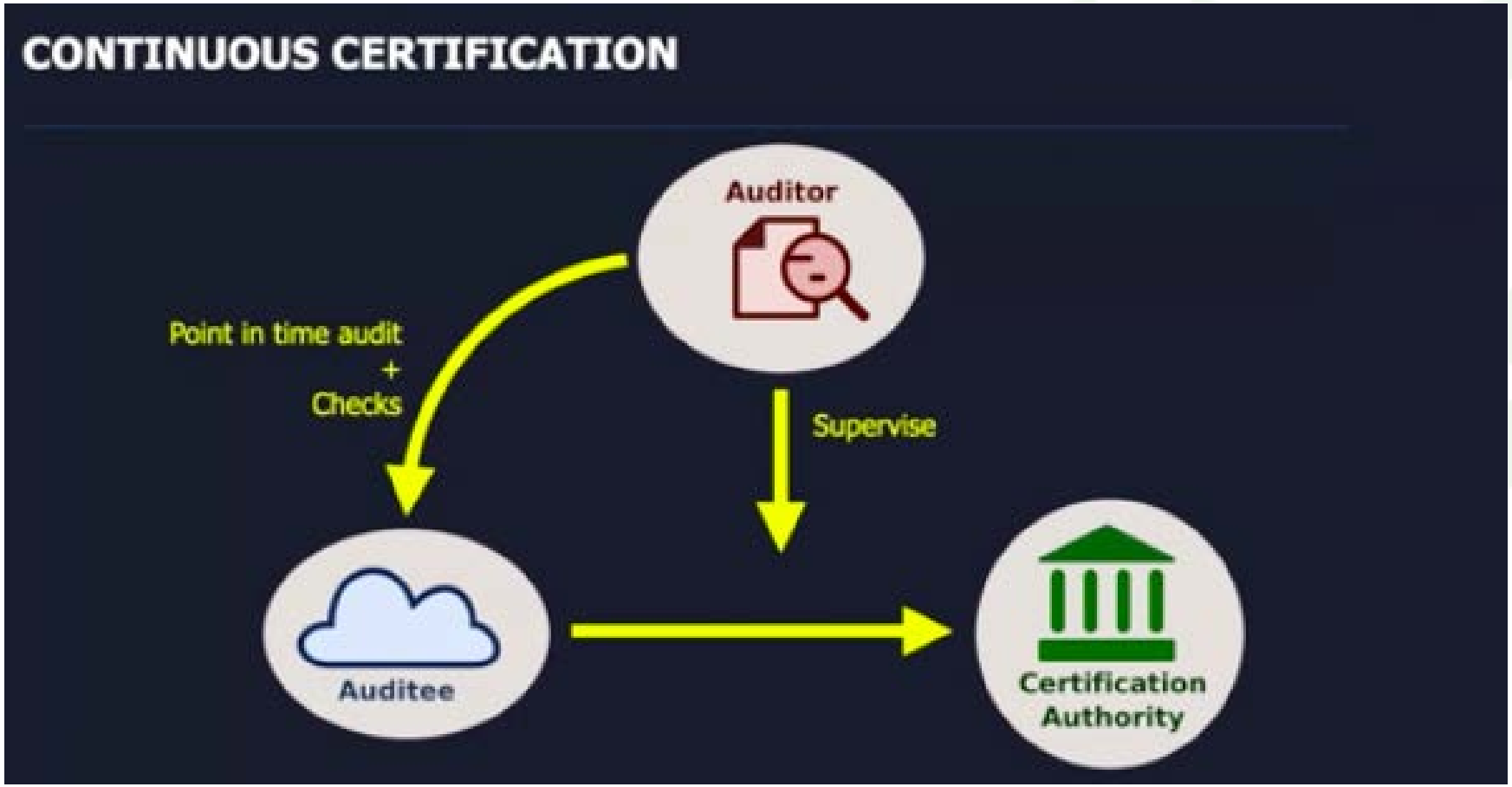
Extended certification with continuous self-assessment:

- 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:

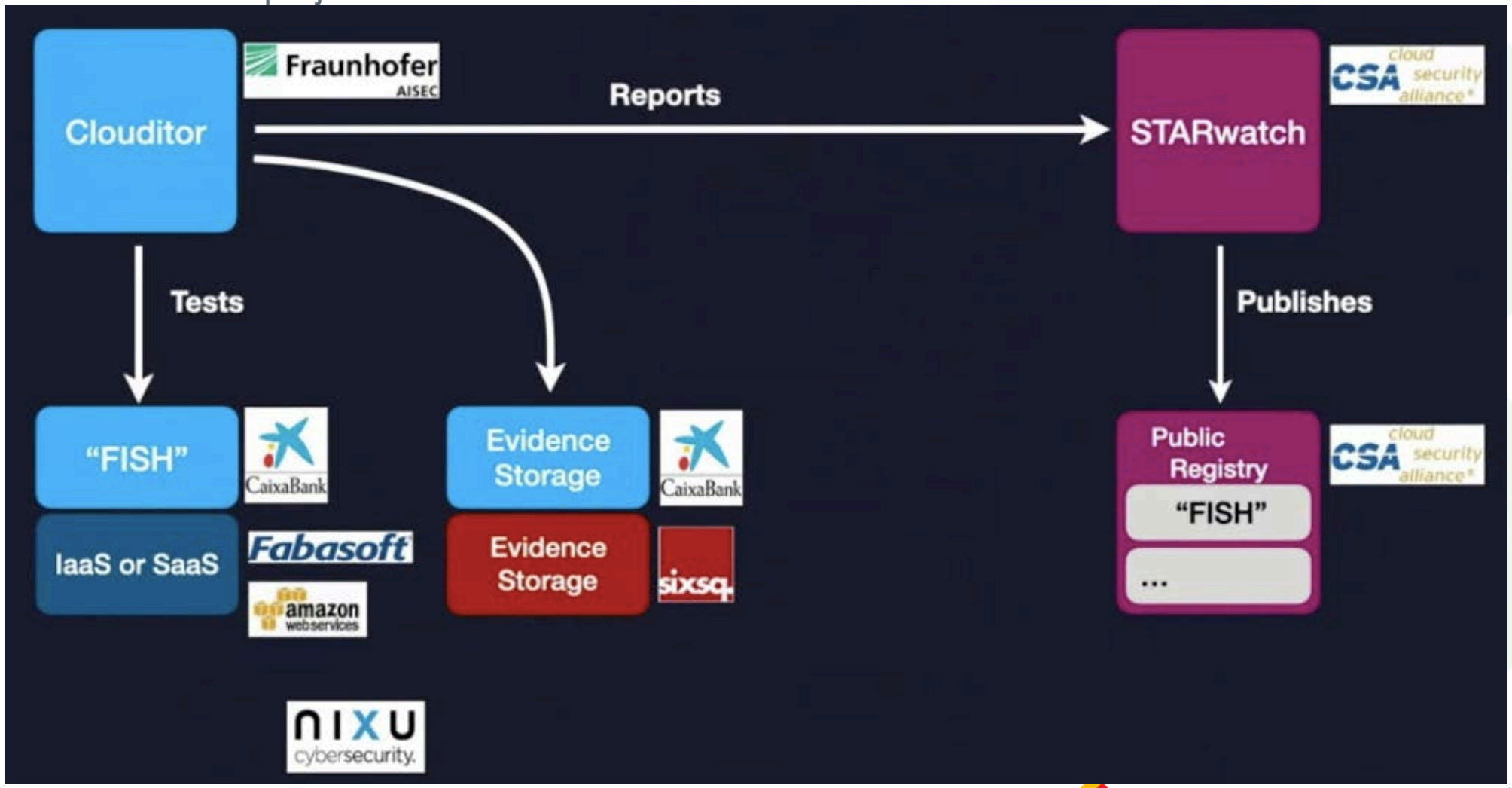
- User undergoes "classic" certification with third party auditor.
- Third party auditor also checks certification target + tools are fit for purpose & trustworthy
- User does assessment and reporting under the supervision of the third party auditor


EXTENDED CERTIFICATION + CONTINUOUS SELF-ASSESSMENT
Auditor
Point in time audit
+
Checks
Auditee
Certification
Authority


CONTINUOUS CERTIFICATION
Auditor
Point in time audit
+
Checks
Supervise
Auditee
Certification
Authority

Pilot Deployment

EU funded EU-SEC project



Challenge

Metrices (or their lack of)

What's Next?

CSA is running a Continuous Audit Metrics WG

- Do join us!

CSA is already experimenting with "continuous" assurance

- Submit a CAIQ self-assessment on a monthly basis

Our aim: First Continuous Certification n 2021.

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®

Singapore Chapter