EUSEC
EU SECURITY CERTIFICATION

EU-SEC The European Security Certification Framework

CONTINUOUS AUDITING CERTIFICATION

Fraunhofer FOKUS

Content

EUSEC
EU SECURITY CERTIFICATION

- Problem Statement
- Objectives / Principles and challenges
- Approach
- Continuous auditing certification architectures and procedures
- Measurements
- Continuous auditing certification scheme
- Governance structure
- Conclusions

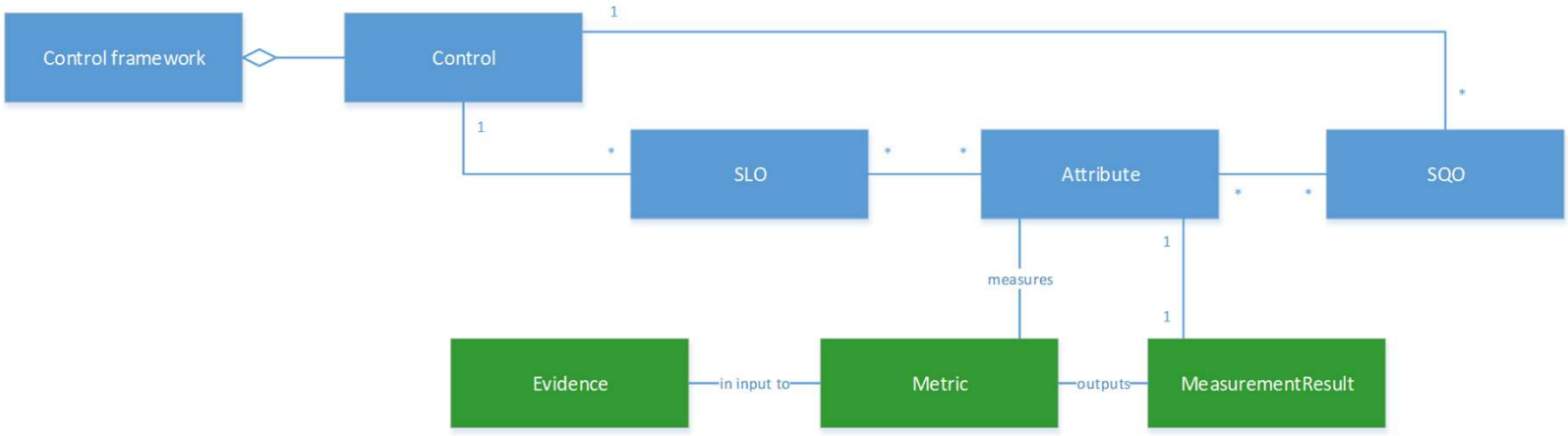
Problem Statement

EUSEC
EU SECURITY CERTIFICATION

- Currently Security audits are usually performed in a two year cycle according to the requirements of the granted certificate.
- This creates a time window of uncertainty where no audit is performed.
- The cloud service customers do not have an up-to-date status on the fulfilment of the requirements, established by the certification goals.
- The continuous audit approach in this document addresses this issue by providing a way of continuously asses the compliance status
- CA allows to continuously asses the conformance status with regard to:
  - Regulations
  - Requirements
  - Controls

Approach – Control breakdown

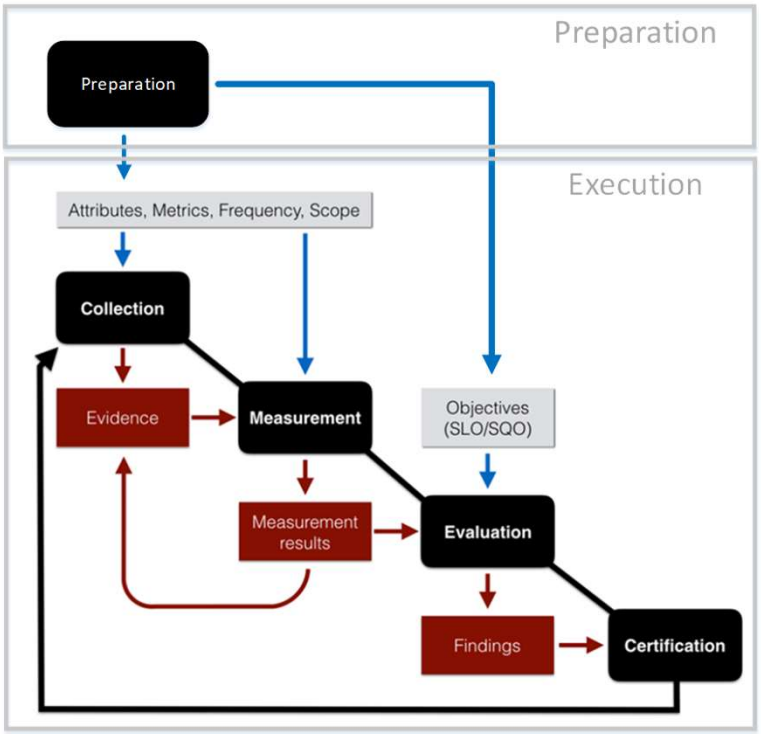
- Rather than once every two years CA gives an assessment at each point in time
- Achieve a high grade of automation
- Develop fallbacks for human assessments when needed.
- Provide a model for disassembling controls into function able metrics



Continuous auditing certification architectures and procedures

EUSEC
EU SECURITY CERTIFICATION

- Continuous auditing is enabled in 4 phases
- The operationalisation of the controls takes place in the preparation phase
  - This initial setup is performed once
  - SLO's and SQO's are defined to describe controls
  - Resolves in a set of:
    - Attributes for certain parameters
    - Metrics for assessing the attributes
    - Frequency's in which the assessment has to take place
    - Scope of the assessment
- The collection of evidences takes place in the collection and Measurement phase.
- In the Evaluation phase the check if a certain objective is fulfilled is performed.
- According to the result of the evaluation a certificate is granted or not.



Measurement procedures

- A measurement provides assurance on the fulfilment of an attribute.
- In this context the measurement process consists of three elements which represent the three steps of data processing to obtain information on the attribute and ultimately on the objectives or SLO/SQO.

Continuous auditing certification scheme – 3 Certification models

- EU-SEC project proposes a framework that contains three models for continuous auditing.
- Each of three models provides a different level of assurance by covering requirements of continuous auditing with various levels of scrutiny.

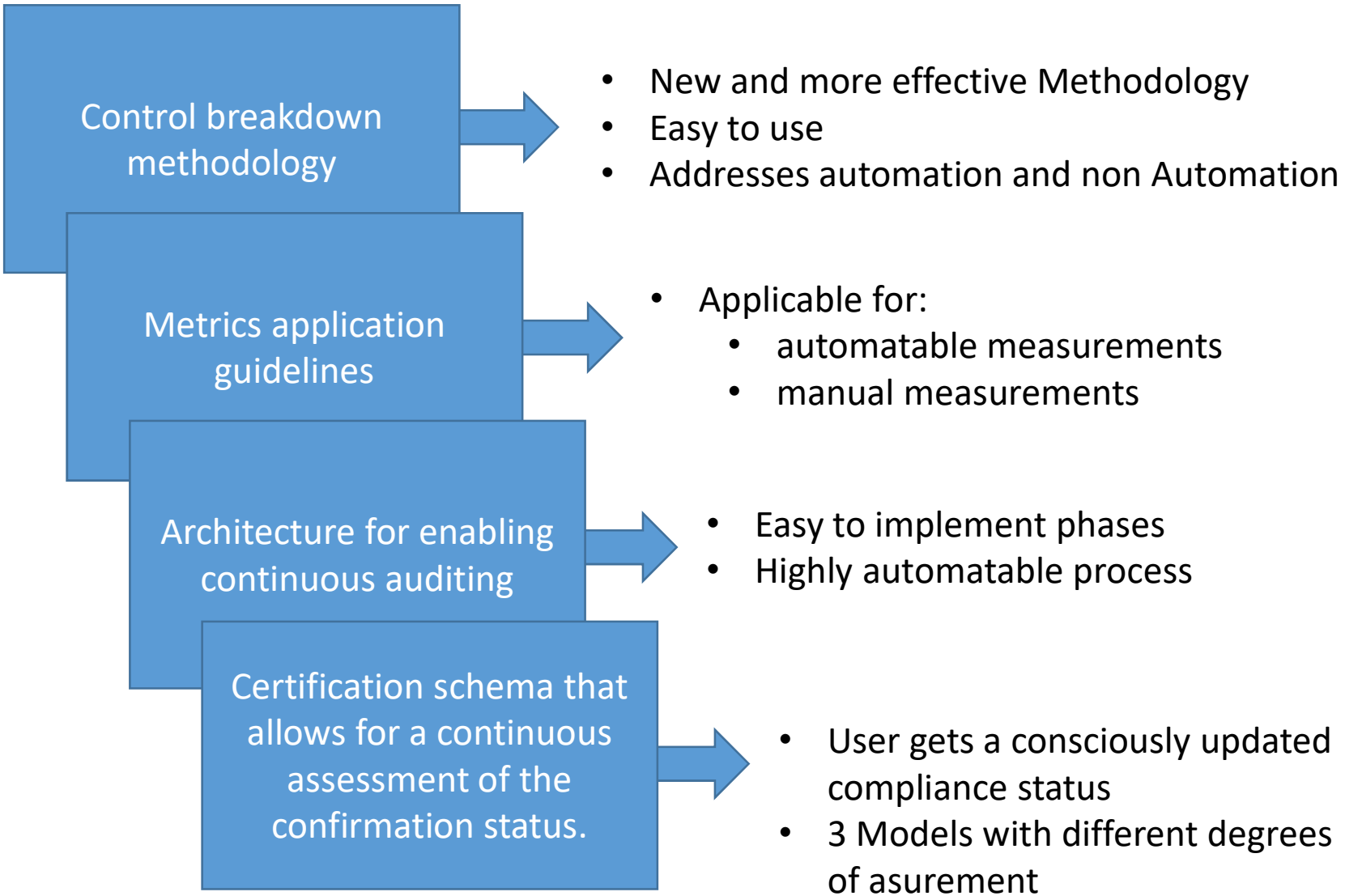
1. Continuous Self-assessment
2. Extended Certification with Continuous Self-assessment
3. Continuous Certification

Governance structure

EUSEC
EU SECURITY CERTIFICATION

- The governance structure guides the entire continuous auditing process from conceptual design through set up, implementation and parameterisation to operation and maintenance as well as further development.
- Roles and responsibilities are laid out.
- Governance processes are described.

Conclusion



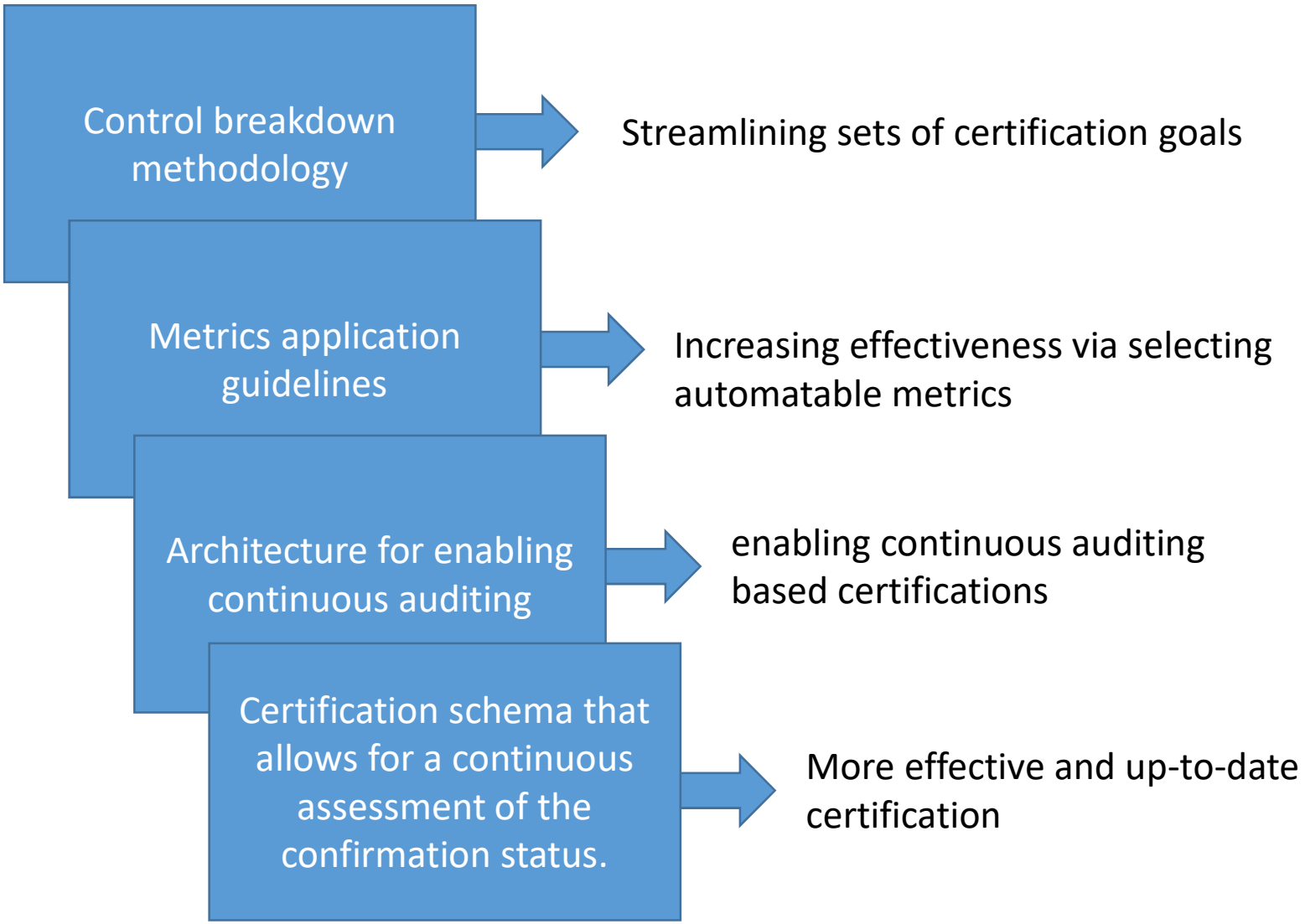
- New and more effective Methodology
- Easy to use
- Addresses automation and non Automation

- Applicable for:
  - automatable measurements
  - manual measurements

- Easy to implement phases
- Highly automatable process

- User gets a consciously updated compliance status
- 3 Models with different degrees of asurement

Conclusion


Control breakdown methodology
Streamlining sets of certification goals
Metrics application guidelines
Increasing effectiveness via selecting automatable metrics
Architecture for enabling continuous auditing
enabling continuous auditing based certifications
Certification schema that allows for a continuous assessment of the confirmation status.
More effective and up-to-date certification