EUSEC
EU SECURITY CERTIFICATION

EU-SEC The European Security Certification Framework

PRINCIPLES, CRITERIA AND REQUIREMENTS FOR A MULTI-PARTY RECOGNITION AND CONTINUOUS AUDITING BASED CERTIFICATIONS

Contents

EUSEC
EU SECURITY CERTIFICATION

- Problem Statement
- Objectives
- Approach
- Principles, Criteria, Requirements
- Multiparty Recognition Lifecycle
- Continuous Certification Process
- Continuous Certification Architectures
- Conclusions

Problem Statement

- Challenges due to the proliferation of compliance/certification schemes
  - Compliance assessment costs become an increasing cost for CSPs, and as a consequence of that, an increased cost for cloud users.
  - Lacking comparability and interoperability between existing certification schemes
  - Provision of simple tools to streamline the compliance process and cost reduction

Objectives

EUSEC
EU SECURITY CERTIFICATION

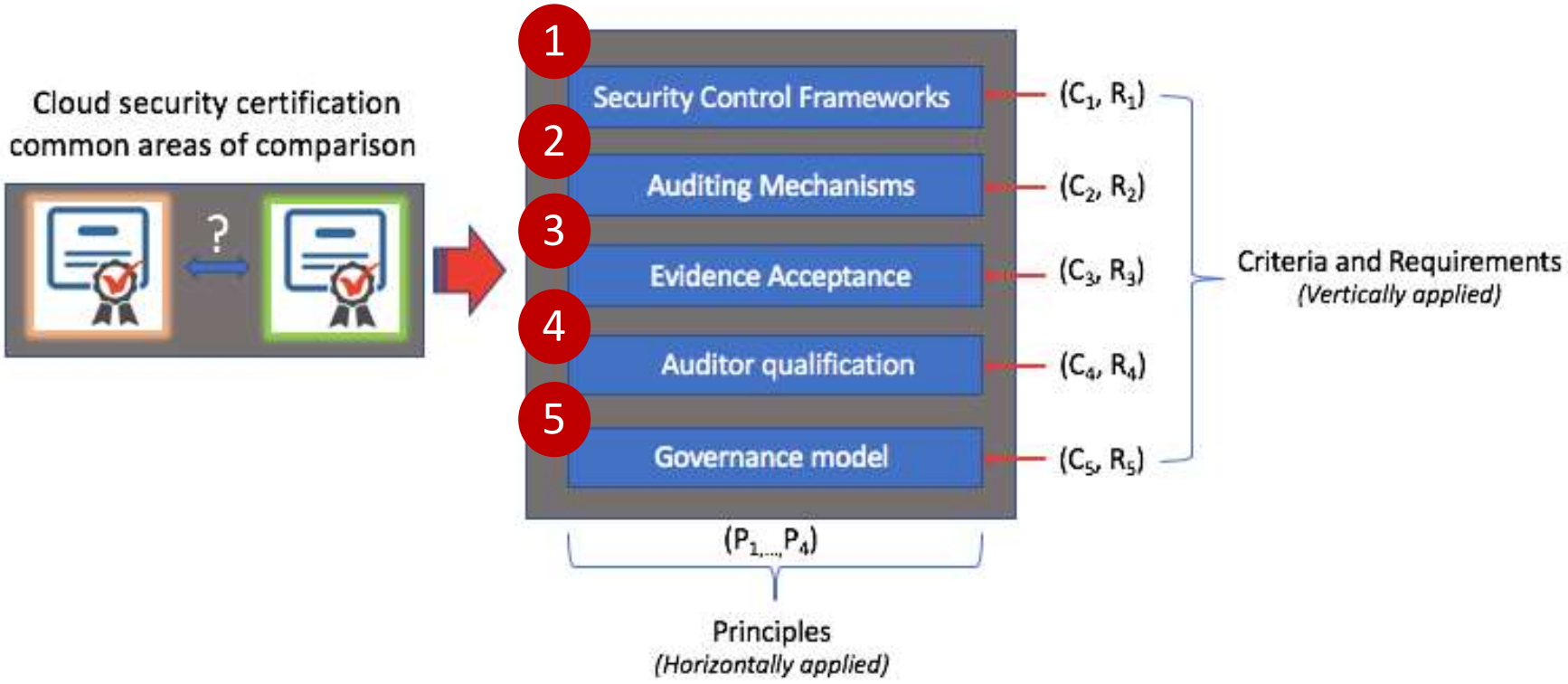
- Define principles, criteria and requirements for the development of the:
  - Multiparty Recognition Framework
  - Continuous Auditing Framework
- Principles serve as foundational propositions for multiparty recognition and continuous auditing
- Requirements act as key mandatory elements toward multiparty recognition and continuous auditing
- Criteria which constitute prerequisites that, if satisfied in full or partial, allow for multiparty recognition
- Define a lifecycle scheme for the future manageability and sustainability of these frameworks

Approach

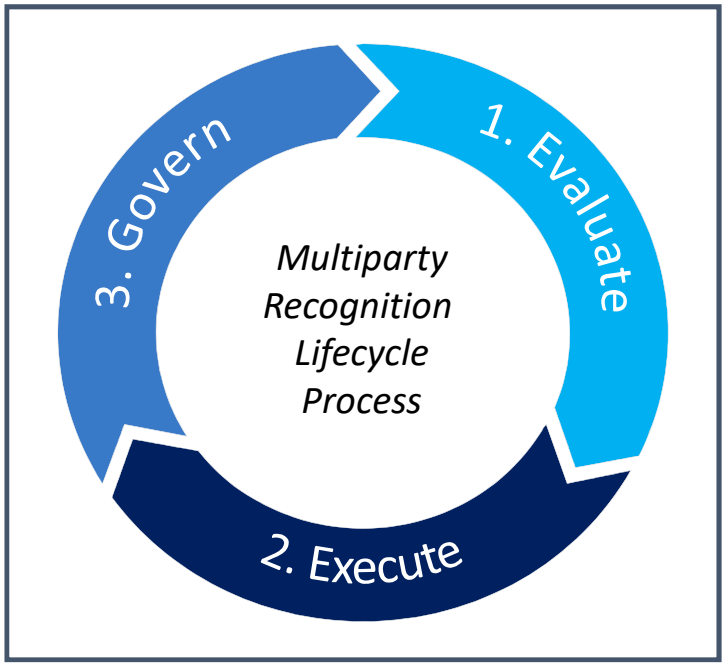
- Comparison analysis and identification of common characteristics found in widely established cloud-based security certifications:
  1. Security controls and requirements
  2. Audit mechanisms
  3. Evidence collection and suitability
  4. Auditors qualifications
  5. Governance models
- Identification of stakeholders for frameworks' governance
- Definition of principles, criteria and requirements as prerequisites for the operation of the continuous auditing and multiparty recognition frameworks

Principles, Criteria, Requirements

- Define and apply “Criteria” and “Requirements” vertically per each of the 5 certification areas
- Define and apply “Principles” horizontally to include all 5 areas of certification



Multiparty Recognition Lifecycle



1. Evaluate:

Candidate scheme is evaluated against criteria and principles to be found non-/eligible for the multiparty recognition

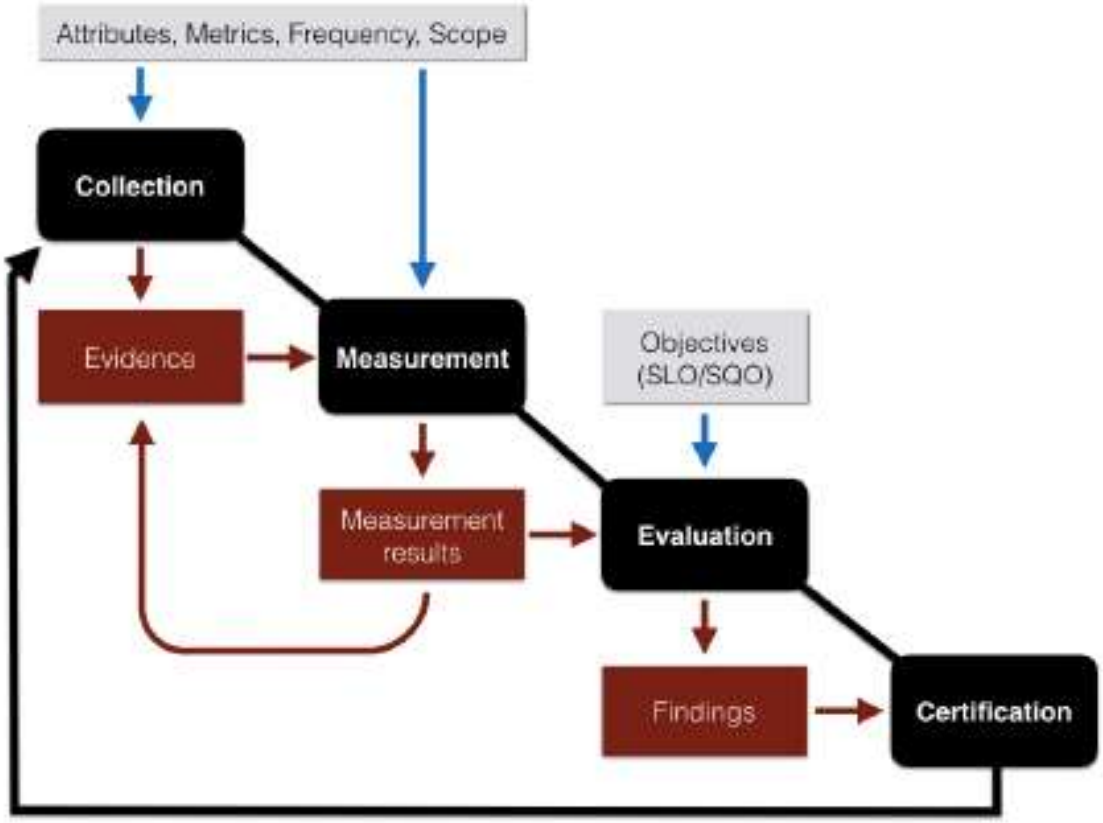
2. Execute:

Enables the comparison and recognition between different auditing standards

3. Govern:

Ensures continuous improvement, maintenance and future sustainability of the framework

Continuous Certification Process



- Collection

Describes the collection of data from information systems by auditing tools and humans

- Measurement

Describes the processing of evidence in order to produce measurement results

- Evaluation

Describes the evaluation of SLOs and SQOs

- Certification

Describes the publication of a statement confirming or not that an information system satisfies a set of predefined requirements

Continuous Certification Architectures

EUSEC
EU SECURITY CERTIFICATION

Approach 1: continuous self-assessment

- The CSP collects service data using its own monitoring tools and personnel, makes self-assessments of security or privacy SLOs/SQOs and produces the results
- The governing body maintains a public registry of certified cloud services, which can be consulted freely by cloud customers.

Approach 2: extended certification with continuous self-assessment

- The CSP performs a traditional (non-continuous) certification, followed by a continuous self-assessment.
- An external auditor is that who perform a point in-time certification

Approach 3: continuous certification

- The CSP performs a traditional (non-continuous) certification, followed by a continuous self-assessment.
- An external auditor, which performs a point in-time certification as well as a continuous audit-based certification
- The CSP uses auditing tools and processes that have been “vetted” by an external auditor, and continuously provides measurement results to the governing body

Conclusions

EUSEC
EU SECURITY CERTIFICATION

- Proposed criteria, principles, and requirements as building blocks of the EU-SEC multiparty recognition framework
  - 5 criteria, 4 core principles, and total of 31 requirements for mutual recognition
- A process lifecycle of the multiparty recognition approach ensures the multiparty recognition framework reflects the up-to-date security certifications and standards
- Highlighted 3 continuous audit-based certification models ranging from a continuous self-assessment to a full continuous certification
- Provided a list of requirements for the creation of a continuous auditing-based certification framework
  - Requirements take both into consideration automated and non-automated continuous auditing processes