EU-SEC The European Security Certification Framework

EU-SEC Framework

Contents

EUSEC
EU SECURITY CERTIFICATION

- Background
- Scope and Objectives
- EU-SEC Framework Structure
- Governance Enablers
- Governance Body Structure
- Governance and Processes
- Governance
- Conclusions

Scope and Objectives

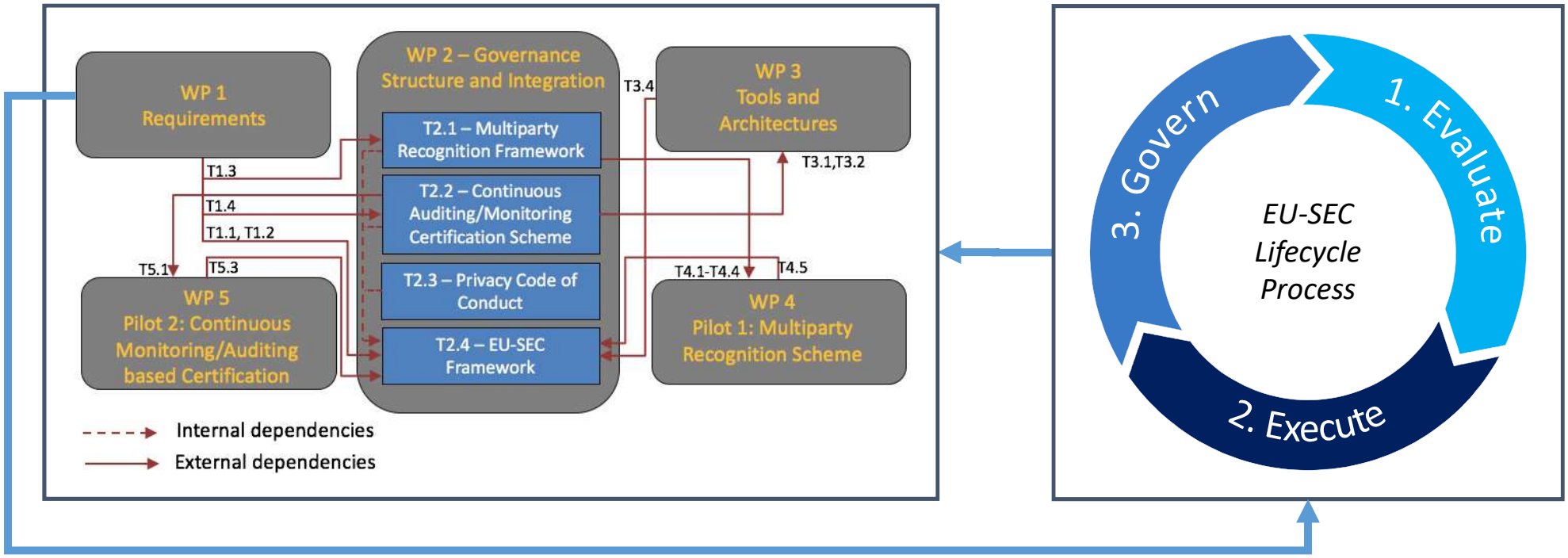
Scope:

- Involves activities for the identification and integration of WP2 three models/schemes into a unified EU-SEC architecture, these are:
  - The Multiparty Recognition Framework
  - Continuous Monitoring/Auditing Certification Scheme
  - The Privacy Code of Conduct
- Involves activities for the definition of a holistic approach towards Governance which will address all EU-SEC actors, components and the interrelationships between them

Objectives:

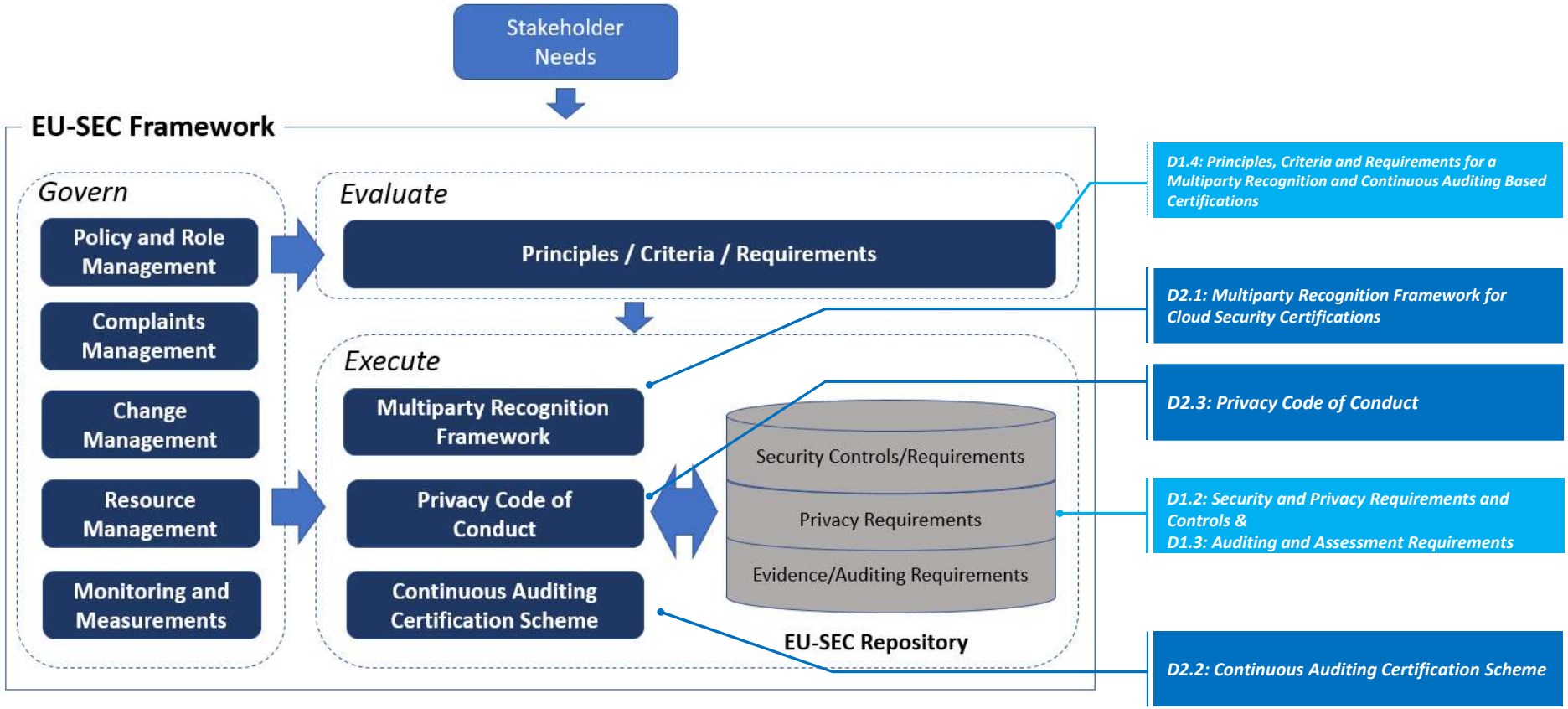
- Define the EU-SEC Framework's architecture throughout the specification of its underlying components and the interrelationships between them
- Define the EU-SEC Framework's governance structure to assist toward the future management, sustainability and extension requirements
- Emphasize that the EU-SEC Framework succeeds in tackling challenges related to cloud security certification and ensuring its cost-effectiveness, transparency and trust among the relevant stakeholders

EU-SEC Framework
Background



A lifecycle process was established in D1.4 (WP1), which initially implies to all EU-SEC Framework Components

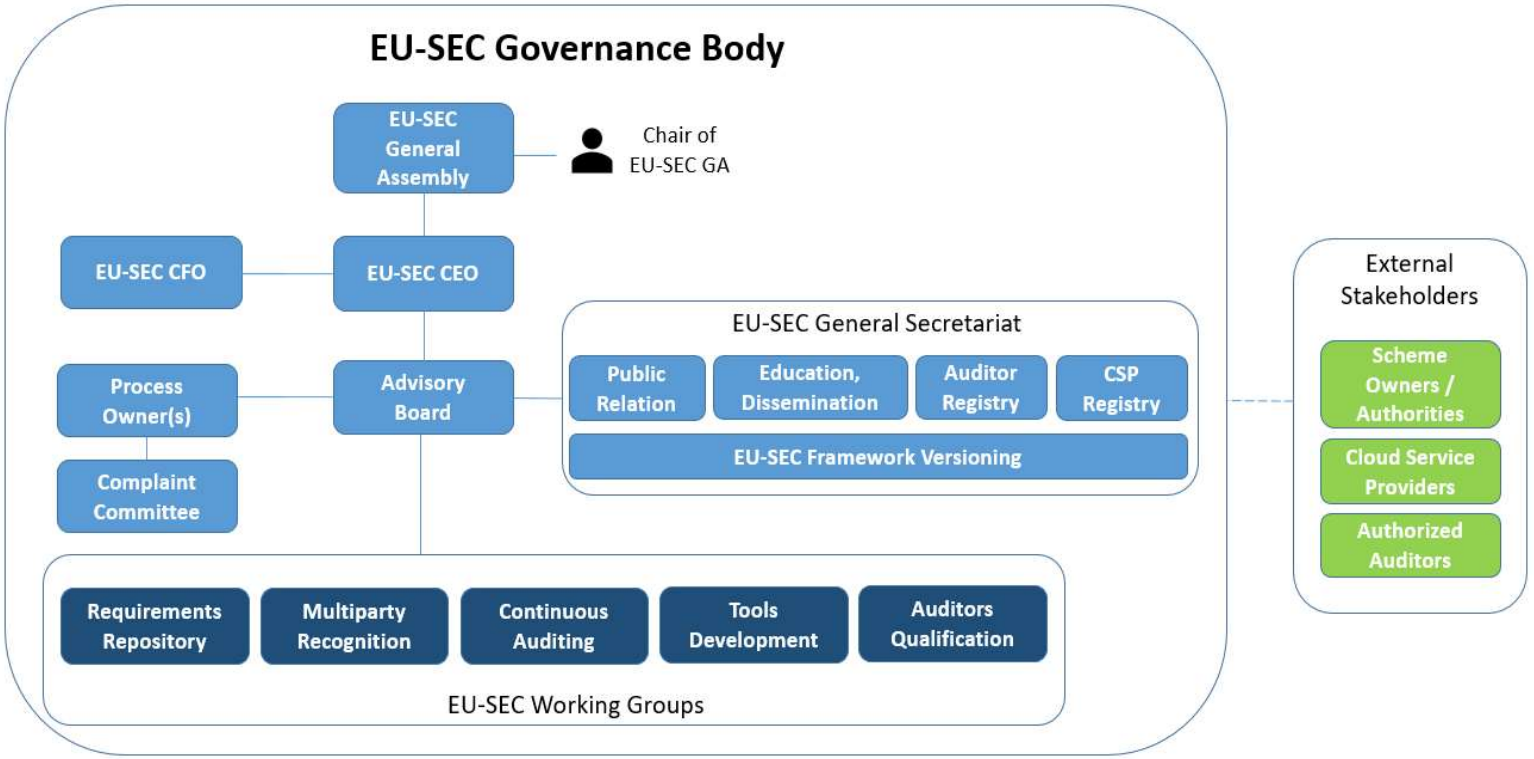
EU-SEC Framework
Structure



EU-SEC Framework
Governance Enablers (aligned with COBIT 5)

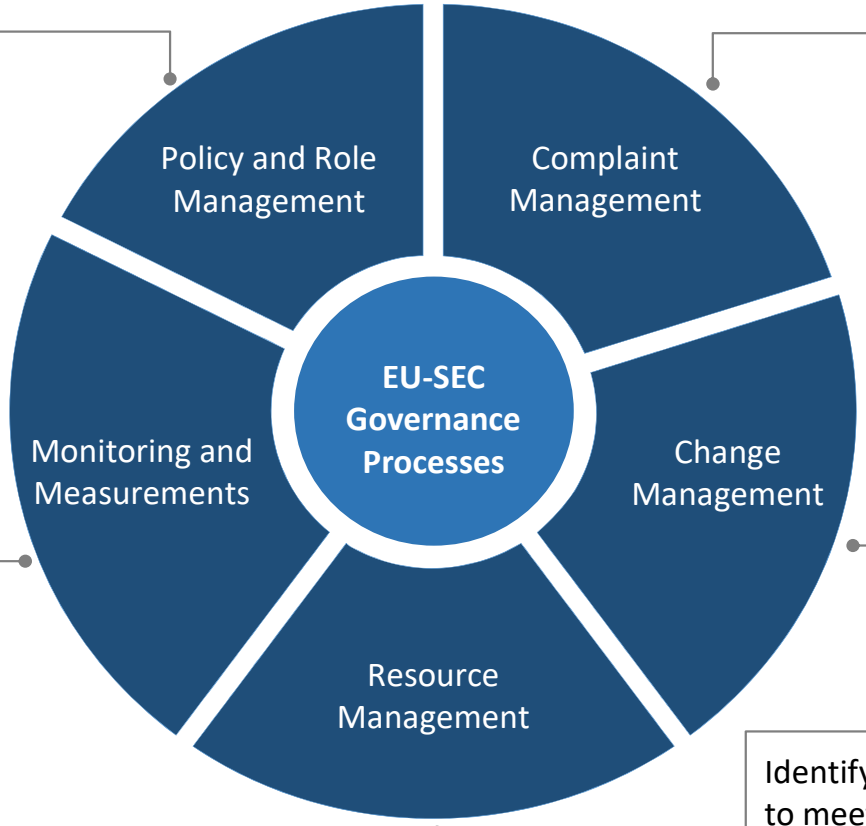
EUSEC
EU SECURITY CERTIFICATION

EU-SEC Framework
Governance Body (Illustration of Option 1)



This current model fits Option 1 best and therefore is still subject to change.

EU-SEC Framework
Governance Process



Guidance to operate, manage and govern the organisation.

Structure and organize the constructive processing of requests and complaints

Identify goals, define important aspects to ensure the effectiveness of the EU-SEC governance process, policies and procedures.

Reduce risks, cover the complete life cycle of the change

Identify, allocate and ensure resources to meet the current and future requirements in a cost-effective manner.

EU-SEC Framework
Governance Process: Policy and Role Management

Objectives

Policy and role management aims to create a harmonised system with guidance to operate, manage and govern the organisation.

Principles

- Policies and Procedures
- Responsibility and Accountability
- Timeliness
- Corrective Action
- Competence
- Periodic Reassessment

Activities

1. Set the goals and directives of the EU-SEC Organisation
2. Establish the organisational structure and reporting line
3. Define the responsibility and accountability of roles and groups
4. Establish policies and procedures to support deployment of EU-SEC's directives
5. Approve the policies and procedures by EU-SEC CEO and Advisory Board
6. Publish and communicate the policies and procedures with all relevant parties
7. Publish and communicate the policies and procedures with all relevant parties

EU-SEC Framework
Governance Process: Complaint Management

EUSEC
EU SECURITY CERTIFICATION

Objectives

Complaint management aims to structure and organise the constructive processing of requests and complaints about the framework that may be raised by internal and external stakeholders.

Principles

- Visibility
- Accessibility
- Responsiveness
- Objectivity
- Charges
- Confidentiality
- Customer-focused approach
- Responsibility & Accountability
- Continual improvement

Activities

1. Receive complaint and acknowledge receipt
2. Assess validity and severity (relevance, impact and urgency)
3. Identify solution for the request or complaint
4. On-going communication
5. Communicate solution
6. Implement solution
7. Close complaint

EU-SEC Framework
Governance Process: Change Management

EUSEC
EU SECURITY CERTIFICATION

Objectives

Change management aims to reduce risks, cover the complete life cycle of the change and all affected stakeholders.

Principles

- Holistic Applicability
- Complete Coverage
- Responsibility & Accountability

Activities

1. Initiate change
2. Assess the impact
3. Authorise change request
4. Plan and schedule change
5. Execute change
6. Approve change
7. Implement change
8. Perform post-implementation review

EU-SEC Framework
Governance Process: Resource Management

EUSEC
EU SECURITY CERTIFICATION

Objectives

The resource management is necessary to identify, allocate and ensure that resources are right-sized to meet the current and future requirements in a cost-effective manner.

Principles

- Quantifiable
- Forecast
- Communication
- Up-to-date

Activities

1. Assess availability, performance and capacity
2. Establish the organisational structure and reporting line
3. Define the responsibility and accountability of roles and groups
4. Establish policies and procedures to support deployment of EU-SEC's directives

EU-SEC Framework
Governance Process: Monitoring and Measurements

Objectives

The Monitoring and Measurements Process is necessary to identify goals together with stakeholders, define important aspects and to ensure the effectiveness of the EU-SEC governance process, policies and procedures. It is also necessary to ensure the compliance with internal and external requirements.

Principles

- Object
- Frequency
- Responsibility & Accountability
- Measurable
- Comparable

Activities

1. Define the monitoring KPIs and measurements
2. Perform KPIs monitoring and measurements with defined frequency
3. Compare the monitoring results with the expectation and identify the deviations
4. Report monitoring deviations
5. Follow-up on deviations

Conclusions

- The EU-SEC Framework's structure brings the outcomes of Deliverables D2.1, D2.2 and D2.3 into one harmonized framework
- The EU-SEC Framework's governance model with 5 governance processes demonstrate the first version of the EU-SEC Framework's governance structure and governance activities.
- Version D2.4 of the EU-SEC framework is expected to be updated into version D2.5 by integrating feedback from:
  - WP4 Pilot 1: Multiparty Recognition Scheme
  - WP5 Pilot 2: Continuous Auditing/Monitoring based Certification
  - WP3 Tools and Architectures