EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

EU-SEC FRAMEWORK – FIRST VERSION

V 1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE: 30/6/2018	DELIVERY DATE: 30/6/2018
AUTHOR: PwC Germany	PARTNERS CONTRIBUTED: CSA, Fraunhofer Fokus, SI-MPA
DISSEMINATION LEVEL:* PU	NATURE OF THE DELIVERABLE:** R
INTERNAL REVIEWERS: MFSR, Fabasoft	

*PU = Public, CO = Confidential

**R = Report, P = Prototype, D = Demonstrator, O = Other

This project has received funding from
the European Union's HORIZON Framework
Program for research, technological development and
demonstration under grant agreement no 731845

EXECUTIVE SUMMARY

The rapidly changing legal and regulatory landscape has heavily influenced security assurance, governance and compliance. Cloud Service Providers are under a considerable pressure being obliged to comply with several international and national requirements as well as sector specific regulation. Apart from that, the market seems to show signals of inefficiency and lack of effectiveness. The current auditing process still lacks of automation, harmonised rules for various certification schemes and transparency.

As solution to the aforementioned issues, the EU-SEC Consortium aims to develop a framework for the multiparty recognition between existing cloud security schemes which is also able to be implemented continuously in auditing process. The framework will provide ICT-stakeholders with a validated governance structure, a reference architecture, and the corresponding set of tools to improve the efficiency and effectiveness of their current approach to security governance, risks management, assurance and compliance.

The main sources for this deliverable are the D2.1: Multiparty Recognition Framework, D2.2: Continuous Auditing Certification Scheme and D2.3: Privacy Code of Conduct, which are the base elements of the EU-SEC Framework. This deliverable will comprise the interrelationship between each component and the governance structure of the whole framework, which will serve as the guideline for the future management, sustainability and extension requirements.

As result, the governance structure, governance body organisation and governance processes of the EU-SEC Framework are defined and introduced as the first version in this deliverable. The aforementioned results determine the structure, roles, responsibilities and the processes and activities that will be carried out during the execution of the framework.

However, since the EU-SEC Project is currently still on going, this deliverable D2.4 describes only the current stage of the project and serve as a base that still needs to be enhanced and improved. The final version of EU-SEC Framework will be published in deliverable D2.5 "EU-SEC Framework – Final Version" at the last stage of the EU-SEC Project.

ABBREVIATIONS

Abbreviation	Description
BSI C5	Federal Office for Information Security of Germany Cloud Computing Compliance Controls Catalogue
CoC	Code of Conduct
CSP	Cloud Service Provider - A Cloud Service Provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. (http://searchcloudprovider.techtarget.com/definition/cloud-provider)
CSA CCM	Cloud Security Alliance Cloud Control Matrix
D1.2	EU-SEC deliverable of task 1.1 "D1.2 – Security and Privacy Requirements and Controls" (https://cdn0.scrvt.com/fokus/ec7f2111f873547b/e2acb6781bc1/D1.2-Security-and-privacy-requirements-and-controls-V1.2.pdf)
D1.3	EU-SEC deliverable of task 1.2 "Auditing and assessment requirements" (https://cdn0.scrvt.com/fokus/76bc9febc2cdbd61/9f38925d56b3/D1.3-Auditing-and-assessment-requirements-V1.0.pdf)
D1.4	EU-SEC deliverable of tasks 1.3 and 1.4 "Principles, criteria and requirements for a multiparty recognition and continuous auditing-based certifications" (https://cdn0.scrvt.com/fokus/15cde3d2c6267d70/82ed8f0cc69c/D1.4-multiparty-recognition-V-1.0.pdf)
D2.1	EU-SEC deliverable of tasks 2.1 "Multiparty recognition framework for cloud security certifications" (https://cdn0.scrvt.com/fokus/c93d8a5da1653b36/c2c115c26501/D2.1-Multiparty-Recognition-Framework-v1.0.pdf)
D2.2	EU-SEC deliverable of tasks 2.2 "Continuous auditing certification scheme" (https://cdn0.scrvt.com/fokus/e15833550549fea0/8c4b39eb9add/EU-SEC-D2.2-Continuous_auditing_certification_scheme_V1.pdf)

Abbreviation	Description
D2.3	EU-SEC deliverable of tasks 2.3 "Privacy code of conduct" (https://cdn0.scrvt.com/fokus/1911860fecc21cff/a71af483c4b0/D2.3_Privacy_Code_of_Conduct_v1.0_Final.pdf)
D2.4	EU-SEC deliverable of tasks 2.4 "EU-SEC Framework – First Version" (this document)
D2.5	EU-SEC deliverable of tasks 2.4 "EU-SEC Framework – Final Version"
D3.1	EU-SEC deliverable of tasks 3.1 "Architecture for Security Controls" (https://cdn0.scrvt.com/fokus/8683a2d92a0056dc/d176283a2337/D3.1-Architecture_for_Security_Controls.pdf)
D3.2	EU-SEC deliverable of tasks 3.2 "Architecture and Tools for Auditing" (https://cdn0.scrvt.com/fokus/fa3733c001400c98/65ffd7127e45/D3.2_Architecture_and_Tools_for_auditing-V1.pdf)
D3.3	EU-SEC deliverable of tasks 3.3 "Architecture and Tools for Evidence Storage" (https://cdn0.scrvt.com/fokus/a4d43be2ff052ddb/c6e938e046b3/D3.3-Architecture_and_tools_for_evidence_storage.pdf)
EU	European Union
EU-SEC	European Security Certification Framework (http://www.sec-cert.eu/)
EU-GDPR	European Union General Data Protection Regulation (2016/679) (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
ISO	International Organisation for Standardization (https://www.iso.org/home.html)
ISO/IEC 19086	ISO/IEC 19086:2016 Information technology – Cloud computing – Service level agreement (SLA) framework (https://www.iso.org/standard/67545.html)
ISO/IEC 27001:2013	ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements (https://www.iso.org/isoiec-27001-information-security.html)
PLA CoP	Privacy Level Agreement Code of Practice
RfC	Request for Change
SLO	Service Level Objective
SQO	Service Qualitative Objective

TERMINOLOGY AND DEFINITION

Term	Definition	Source
Assessment	Refers in this document to risk assessment, which overall process of *risk identification [ISO Guide 73:2009, definition 3.5.1], risk analysis [ISO Guide 73:2009, definition 3.6.1]* and *risk evaluation [ISO Guide 73:2009, definition 3.7.1]*.	ISO Guide 73:2009, definition 3.4.1
Accreditation	Accreditation assures users of the competence and impartiality of the body accredited.	http://www.iaf.nu/
Audit	Systematic, independent and documented process for obtaining *audit evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled	ISO/IEC 19011:2011, 3.1
Audit criteria	Set of policies, procedures or requirements used as a reference against which audit evidence is compared Note 1: Policies, procedures and requirements include any relevant Service Qualitative Objectives (SQOs) or Service Level Objectives (SLOs).	ISO/IEC 19011:2011, 3.2
Audit evidence	Records, statements of fact or other information which are relevant to the *audit criteria* and verifiable.	ISO 9000:2005, definition 3.9.4
Auditee	Organisation being audited.	ISO 9000:2005, definition 3.9.8
Auditor	Person who conducts an audit.	ISO/IEC 19011:2011, definition 3.8
Authority	A trusted party that is responsible for the correct organisation of a certification scheme, including the accreditation of auditors and keeping a registry of certified cloud services.	EU-SEC D2.1

Term	Definition	Source
Authorised Auditor	An auditing organisation/auditor authorised by the certification authority/scheme owner to conduct assessments against the requirements of the scheme. A certification body is considered as an authorised auditor.	EU-SEC D2.1
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	https://www.iso.org/certification.html
Certification scheme	The set of rules, requirements and mechanisms that govern the process of certifying a process or a product. NOTE: In this document we use interchangeably "certification scheme" and "compliance scheme" noting that in the real term practise often time the term "certification scheme" is used when referring to ISO-based certification while the term "compliance scheme" is used when referring to ISAE 3000 audits.	EU-SEC D1.4
Cloud Service Provider	A company offering infrastructure, platform, and/or software services in a cloud.	EU-SEC 2.1
Continuous Auditing	An ongoing assessment process that aims to determine the fulfilment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.	EU-SEC D1.4
Continuous Certification	The regular production of statements indicating that an information system meets a set a predefined of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), each reported at an	EU-SEC D1.4

Term	Definition	Source
	expected frequency through continuous auditing.	
Control	Measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk	ISO/IEC 27000:2016
Information security control	A control, that in general lowers the risk information (and other correlated assets) is exposed to. Security requirements in this context is a set of information security controls, needed to achieve an envisioned level of information security in cloud computing environment.	EU-SEC 2.2
Multiparty recognition	A process for establishing a mutual agreement between certification and compliance scheme owners for recognition of the full or partial equivalence between the certification and/or attestation they govern.	EU-SEC D2.1
Risk	Effect of uncertainty on objectives, where uncertainty is the state of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.	ISO Guide 73:2009, definition 3.9.2
Security requirement	Customers have security requirements. In the procurement phase customers usually check which security requirements are met by the security objectives of the provider. This process is often referred to as due-diligence	ENISA MSM-DSP
SLO	Service Level Objective - a commitment a Cloud Service Provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale service (ISO/IEC 19086-1:2016, 3.5).	ISO/IEC 19086-1:2016, 3.6

Term	Definition	Source
SQO	Service Qualitative Objective - a commitment a Cloud Service Provider makes for a specific, qualitative attribute of a cloud service, where the value follows the nominal scale or ordinal scale service.	ISO/IEC 19086-1:2016, 3.6

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

The rapidly changing legal and regulatory landscape have heavily influenced security assurance, governance and compliance. Cloud Service Providers (CSPs) are under a considerable pressure being obliged to comply with several international and national requirements as well as sector specific regulation. At first sight, numerous certification schemes seem to be uniquely heterogeneous, as they are targeting wider or specific application areas (e.g., national, sectorial, regulatory domains and requirements). Fortunately, cloud-based certification schemes are based on world-wide acceptable and widely used standards (e.g., ISO 27000 series of standards). Hence, their very core security domains and requirements are rather homogeneous from a perspective of security semantics equivalency.

Apart from that, the market seems to show signals of inefficiency and lack of effectiveness. The current auditing process do not exploit automation and harmonised compliance rules for various certification schemes. The development of this scheme is driven by the need of improving traditional point in time certification, since this is the most common approach of getting assurance over the proper implementation of security requirements. A better approach would be continuous auditing, which enables the Cloud Service Provider to have precise statements on the compliance status at any time over the whole timespan, in which the continuous auditing process is executed. It achieves the always up-to-date compliance status by increasing the frequency of the auditing process and – for the purpose of the project – emphasises on automating the verification of controls.

Transparency also comes under the current issues in cloud certification and auditing process. Data protection compliance is becoming increasingly risk-based. Data controllers and processors are accountable for determining and implementing in their organisations appropriate levels of protection for the personal data they process. Therefore, an agreement or a Code of Conduct that can guarantee cloud customers of any size with a tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions) and a guidance to comply with European Union General Data Protection Regulation (EU-GDPR) are highly required.

With the support from Horizon 2020 (H2020), a funding program created by the European Union to support and foster research in the European Research Area, the European Security Certification Framework (EU-SEC) Consortium aims to solve the aforementioned issues by:

- improving the effectiveness and efficiency of existing approaches for assurance and compliance,
- creating a framework under which existing certification and assurance approaches can co-exist,
- providing stakeholders in the ICT security ecosystem with a validated governance structure, a reference architecture, and the corresponding set of tools, and
- enhancing trustworthiness and transparency in the ICT supply chain through business cases developed and piloted by industrial partners.

1.1. SCOPE AND OBJECTIVES

The scope of this work is the definition and the structure of the EU-SEC Framework, its execution processes and governance model, which are operated by the EU-SEC Governance Body. This deliverable is based on the existing EU-SEC Deliverables: "D2.1 – Multiparty Recognition Framework for Cloud Security Certification", "D2.2 – Continuous Auditing Certification Scheme" and "D2.3 – Privacy Code of Conduct". The results from the aforementioned deliverables are consolidated in this document as main components of EU-SEC Framework. For that reason, EU-SEC Framework has three main pillars, namely:

- Multiparty Recognition Framework
- Continuous Auditing Certification Scheme
- Privacy Code of Conduct

The EU-SEC Framework's governance will aggregate the governance requirements of the respective models defined in deliverables D2.1, D2.2 and D2.3 and integrating them into a single well-defined structure. The structure will consist of interrelated processes, governance bodies with assigned roles and responsibilities, and granularly defined activities, which will be the support towards the methodical and systematic management of the framework and its long-term sustainability. Multiparty recognition principles, rules and processes, privacy extensions, rules and mechanisms for continuous auditing based certification, guidance for real-world deployment, are all unique components that will be considered in the new EU-SEC Framework's governance structure.

Principles, rules and requirements have already been identified in deliverables D2.1, D2.2 and D2.3, and act as indispensable components of the EU-SEC Framework. These will be taken into account throughout their integration process into the EU-SEC Framework's architecture and governance structures. The effort is not trivial as it requires an in depth understanding of the

developed models and respective activities, actors, roles and responsibilities, tools used and establishing possible dependencies between them. The exercise may reveal additional requirements to the framework such as defining additional activities that might be needed for leveraging the intercommunication between the three framework/schemes at the architectural and governance levels.

The specific objectives of the work have been identified as follows:

- To define the EU-SEC Framework's architecture throughout the specification of its underlying components and the interrelationships between them based on the existing works (i.e., D2.1, D2.2, and D2.3). These components involve tools, processes, actors with roles and responsibilities and respective activities.
- To define the EU-SEC Framework's governance structure to assist toward the future management, sustainability and extension requirements of the established framework.
- To emphasise 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.

Overall, the EU-SEC Framework will contain the following components:

- A reference EU-SEC Framework's architecture and its respective set of tools
- A holistic governance structure that takes the governance requirements from the respective D2.1, D2.2, and D2.3 into account, which will be used to deploy the EU-SEC Framework's underlying architecture/tools and governance bodies
- The principles, rules and requirements from the above referenced deliverables that will be also integrated into the architecture
- Training and awareness raising mechanisms for the dissemination of the framework's output results

1.2. METHODOLOGY

The development of the EU-SEC Framework is driven by the stakeholders needs and follows the three-step lifecycle process proposed in D1.4:

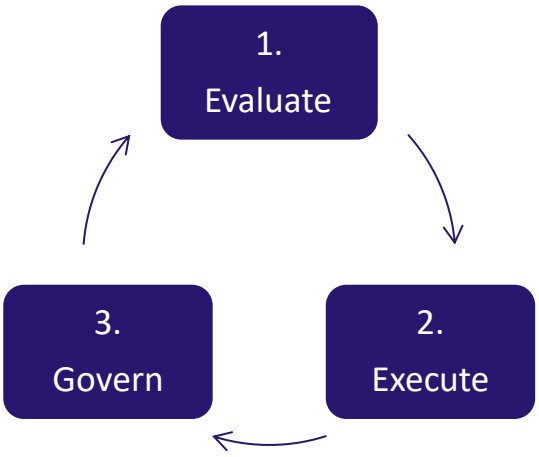

Figure 1: Lifecycle Process

The development of the EU-SEC Framework follows a bottom-up approach. The components of the EU-SEC Framework (D2.1 – Multiparty Recognition Framework, D2.2 – Continuous Auditing Certification Scheme, as well as D2.3 – Privacy Code of Conduct) were designed, established and have become an ecosystem in each case. The main goal and achievement of this deliverable is the integration of all the components mentioned above and their processes into one harmonised framework, so called EU-SEC Framework.

Within the EU-SEC Framework, a governance body organisation is proposed with roles and responsibilities to support the maintenance and operation of the framework. The governance model is established with governance processes and activities, which ensure the efficiency and effectiveness of the operation, management, maintenance, and governance of the EU-SEC Framework. The EU-SEC Framework proposed in this deliverable is the first version of the framework and provides the baseline for the future extension and implementation of the EU-SEC Organisation and its governance processes.

1.3. STRUCTURE

In order to provide a thorough insight on the EU-SEC Framework, this document is structured as follows:

Chapter 2 gives an overview of the EU-SEC Framework, including the overall EU-SEC Framework's structure, its main components and its three-step lifecycle process of "Evaluate, Execute, and Govern".

Chapter 3 introduces the necessity of EU-SEC Framework's governance with support of research theories, the governance enablers and requirements for the governance body. This chapter provides the theoretical foundation for the design and establishes the governance body organisation addressed in chapter 4.

Chapter 4 proposes several operational model considerations for the EU-SEC Framework's governance body organisation, and analyses the pros and cons to provide guidance for future decision making on governance body establishment. The key roles and their responsibilities are also defined in this chapter to ensure the execution and governance of the EU-SEC Framework.

Chapter 5 introduces the five main governance processes of the EU-SEC Framework's governance structure. The processes enable an efficient and effective operation and maintenance of the framework to handle and integrate the needs from stakeholders and changes in the compliance landscape.

At last, Chapter 6 concludes the achievements of the work, describes the limitations and provides additional recommendations for future possibilities for the framework's extension and finalisation.

2. EU-SEC FRAMEWORK OVERVIEW

The development of the EU-SEC Framework follows the three-step lifecycle process proposed in D1.4: Evaluate, Execute, and Govern. The steps of the lifecycle provide a guidance on the maintenance of the EU-SEC Framework. In addition, the lifecycle suggests a path for continuous improvement based on changes in the market as well as feedback based on real life implementation of the framework.

In this section, an overall EU-SEC Framework's structure will be introduced to give an overview on how the EU-SEC Framework is established. Then, each step of the lifecycle process is introduced to give a deeper insight into how the EU-SEC Framework is operated and maintained.

2.1. EU-SEC FRAMEWORK STRUCTURE

The development and operation of the whole framework are driven by stakeholder needs, which aim to make the current cloud certification landscape more effective and efficient. The stakeholders have different roles and responsibilities for the framework as outlined in the other deliverables, for example in "D2.1 – Multiparty Recognition Framework for Cloud Security Certification" (section 4.2). In order to process their requests and demands in a structured manner, the framework comprises phases, processes, and systems (hereafter: components), which were combined and integrated in three lifecycle steps, one for the evaluation of the framework, one comprises the execution and the other one for the governance of the framework.

The EU-SEC Framework comprises the following 3 main components:

- Multiparty Recognition Framework
- Continuous Auditing Certification Scheme
- Privacy Code of Conduct

The EU-SEC Framework's lifecycle process is built up around these three main components. In Figure 2, the EU-SEC Framework is shown in the three-step lifecycle process, which covers the three main components.

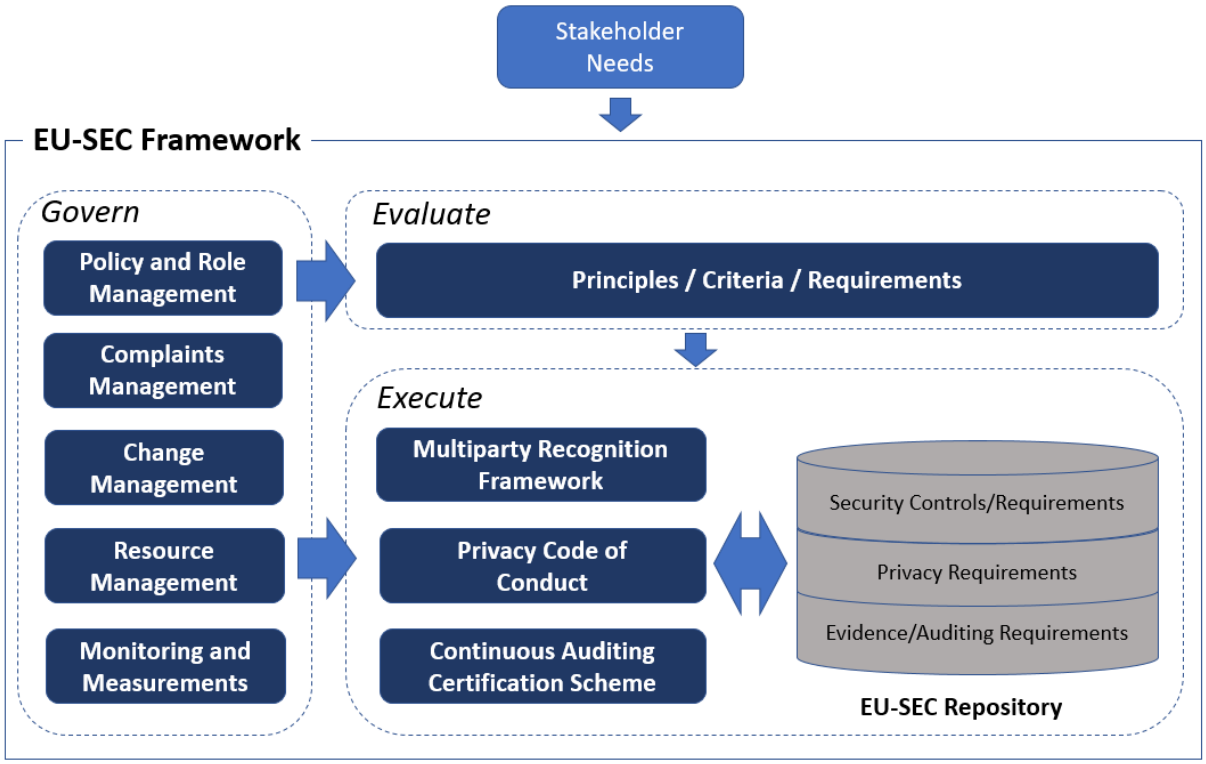

Figure 2: EU-SEC Framework

Evaluate Domain of the EU-SEC Framework

The criteria, principles and requirements, on which the EU-SEC Framework components are based upon, were identified, analysed and defined for the foundation of the EU-SEC Framework. The criteria, principles, and requirements draw the basic line for the Execute and Govern domains of the EU-SEC Framework.

The criteria, principles and requirements were defined in the Deliverable D1.4: "Principles, Criteria and Requirements for a Multi-party Recognition and Continuous Auditing Based Certification". In this deliverable, five criteria, four core principles, and 31 requirements for mutual recognition between different third-party-audit-based certification schemes were identified (D1.4, section 2). These four core principles also apply for the continuous auditing-based certification framework. Additionally, a list of requirements for the creation of a continuous auditing-based certification framework were established as well (D1.4, section 4.3).

In section 2.2, we will revisit the Evaluate domain of EU-SEC Framework with key principles, criteria, and requirements.

Execute Domain of the EU-SEC Framework

The establishment of EU-SEC Framework follows a bottom-up development approach. Three main components of EU-SEC are initially identified as follows:

- Multiparty Recognition Framework: it focuses on the development of the multiparty recognition between existing cloud security certification schemes, based on the security controls/requirements repository established in D1.2, which has analysed and collected security controls and requirements from well-known international and national certification schemes.
- Continuous Auditing Certification Scheme: it focuses on the always up-to-date compliance status by increasing the frequency of the auditing process and automating the verification of controls. The continuous auditing framework identifies the requirements for evidence and auditing.
- Privacy Code of Conduct: it focuses on the privacy-based certification and self-assessments done by CSPs, which result to the establishment of the privacy posture of their services. As the outcome of privacy code of conduct, a privacy-based self-assessments and certification are validated by signed adherence statements.

In this phase, the main focus is to execute each component in the EU-SEC Framework according to the respective principles, criteria and requirements defined in the Evaluate phase.

The execution of the EU-SEC Framework is based on two levels. The first one is on the component level, which means, each component of the EU-SEC Framework is running individually and independently as an ecosystem. The second level is the EU-SEC Framework level, which means that parts of the components (often the repositories) are interacting with each other as a whole during the execution. For example, the multiparty recognition framework has built up an EU-SEC Framework's security controls/requirements repository to support the multiparty recognition tasks and the achievement of improvement of CSP certification efficiency. The multiparty recognition framework runs on its own. Meanwhile, the security requirements serve the continuous auditing framework to build up the EU-SEC Framework's toolchain and evidence management architecture. All of them as a whole, is the EU-SEC Repository.

The execution of these three EU-SEC Framework components are addressed in D2.1 Multiparty Recognition Framework for Cloud Security Certification, D2.2 Continuous Auditing Certification Scheme, and D2.3 Privacy Code of Conduct.

In section 2.3, we will revisit the essential part of the execution of three EU-SEC components.

Govern Domain of the EU-SEC Framework

After the EU-SEC Framework and its components have been designed and established in the respective deliverables D2.1, D2.2 and D2.3, the next important step is to ensure that the operation of the framework is efficient, effective and following the framework lifecycle process. Through continuous monitoring and improving, it is aimed that the EU-SEC Framework will be on top of the rapidly changing cloud certification market.

Five main governance processes are designed to achieve the goals, namely policy and role management, resource management, complaint management, change management, and monitoring. These governance processes are integrated with and extended based on the governance processes developed within the Multiparty Recognition Framework, Continuous Auditing Certification Scheme and Privacy Code of Conduct. These processes intended to guide the operation activities, assign necessary resource, collect issues and events from the execution of the EU-SEC Framework and continually improve the framework.

The governance of EU-SEC Framework is introduced firstly in section 2.4, and addressed in details in sections 3, section 4, and section 5.

2.2. EVALUATE DOMAIN

Each component in EU-SEC Framework is based on a set of criteria, principle and requirements. Those serve as the fundamental elements of each component, which also determine how the framework or the component(s) is supposed to be executed. The criteria, principles and requirements for a Multiparty Recognition and the Continuous Auditing Based Certification have been already defined in D1.4. Certain analysis methodology was used there in order to determine the appropriate criteria, principles and requirements for those components, e.g.: comparison analysis and identification of common characteristics found in widely established certification schemes.

For Multiparty Recognition Framework, five common key certification scheme components are used as criteria for comparing security certifications:

- Security Controls and Requirements
- Audit Mechanisms
- Evidence Collection and Suitability
- Auditors Qualifications

- Governance Models.

Four principles, that seem necessary to conduct any form of assessment in order to support certification and can be applied to the aforementioned principles, were also defined in D1.4 – which are:

- Repeatability Principle
- Equivalence Principle
- Relevancy Principle
- Trustworthiness Principle

Based on this information, the requirements were able to be identified and linked to the above-mentioned principles and criteria. There are in total 31 requirements defined in D1.4 for Multiparty Recognition Framework. The defined criteria, principles and requirements support on the evaluation of whether a new candidate scheme meets the necessary criteria and principles to be eligible to participate in the multiparty recognition process.

The Privacy Code of Conduct aims at increasing the level of transparency and accountability from the privacy point of view. The Privacy Code of Conduct is a voluntary mechanism of adherence to EU-GDPR requirements and transparency. Although there are no criteria, principles or requirements defined for the Privacy Code of Conduct, the collection of privacy requirements follows the similar approach as for the Multiparty Recognition Framework.

In the Continuous Auditing Certification Scheme, aforementioned four core principles apply, which are the same as defined for the Multiparty Recognition Framework in D1.4. The requirements in this component are categorised in three different auditing approaches: Continuous Auditing-Based Certification Base Requirements (13 requirements), Automatable Auditing Requirements (8 requirements) and Non-Automatable Auditing Requirements (7 requirements). The four principles and 28 requirements provide the base of the evaluation, whether continuous auditing certification scheme applies.

The sets of the criteria, principles and requirements are the base of the EU-SEC Framework. Hence, these criteria, principles and requirements must be evaluated and reviewed, in order to ensure that the execution is possible and does not contradict any other possible aspect.

2.3. EXECUTE DOMAIN

The execution domain comprises the whole "Execute" phase of the process scheme in Figure 2. It contains the processes for the Multiparty Recognition Framework as defined in D2.1, section 3.2, the Continuous Auditing Certification Scheme as defined in D2.2, section 3, and the Privacy Code of Conduct defined in D2.3, section 3.3. The execution is directed by the applicable EU-SEC requirements defined in "D1.3 – Auditing and Assessment Requirements" and "D1.4 Principles, Criteria and Requirements for a Multiparty Recognition and Continuous Auditing Based Certifications", and is based on the security and privacy requirements and controls collected in "D1.2 – Security and Privacy Requirements and Controls".

In this section we revisit essential notions for each of the three main pillars of the EU-SEC initiative. By using the methodologies defined for each component, the component frameworks are established based on following repositories:

- EU-SEC security controls / requirements repository (for Multiparty Recognition Framework),
- EU-SEC evidence / auditing requirements (for Continuous Auditing Certification Scheme),
- EU-SEC privacy requirements repository (for Privacy Code of Conduct).

The execution of the processes for the Multiparty Recognition Framework and the Continuous Auditing Certification Scheme is supported by tools, which were designed and specified in the D3.1 Architecture for Security Controls, D3.2 Architecture and Tools for Auditing, and D3.3 architecture and Tools for Evidence Storage. There are currently no processes defined for the PLA CoC. The Multiparty Recognition Framework will be supported by the EU-SEC Security Requirements Repository. This repository will serve the EU-SEC toolchain. As the actual development and implementation of these systems will be tested in the pilots in work package 4 and work package 5, their integration in the EU-SEC Framework may be subject to change.

2.3.1. MULTIPARTY RECOGNITION FRAMEWORK

Nowadays, organisations (e.g. Cloud Service Providers) are investing a considerable amount of resources in compliance audits due to certification proliferation. This excessiveness adds confusion among users, as they may not understand the differences between various certification schemes. Furthermore, the existence of several EU national certification schemes, rather than creating the conditions for the flourishing of the Digital Single Market, creates

potential market barriers instead for Small and Medium-sized Enterprises (SMEs) that cannot afford to invest resources in multiple certifications.

These issues initiated the idea of multiparty recognition, which enables the comparison-making process and the identification of the common security denominators. The goal is to create a framework, under which existing certification and assurance schemes can co-exist. Multiparty recognition will enable an already certified CSP to acquire an additional cloud security certification by proving compliance only to that new certification's delta of security requirements (i.e., the requirements not already covered by the acquired certification[s]). The expected benefits to the Cloud Service Providers and relevant stakeholders within the EU market are non-trivial. These involve investment and time cost-effectiveness, increased transparency, awareness and trust with respect to cloud security certifications.

The "delta" of security requirements between two certification schemes can be deducted after performing a comparison analysis (known as a methodical mapping and gap analysis) between them, as thoroughly described in previous works (see D1.2 and D1.4). Such a comparison is done by leveraging the CSA Cloud Control Matrix, which is taken as the security controls framework of reference and used as the term of comparison between the security requirements included in other relevant standards, best practises and National laws and regulations (ISO27001, BSI C5, Slovenian National requirements, etc.). Other comparison activities with respect to certification-based elements such as evidence collection and audit criteria and requirements are also included in the analysis.

In brief, the multiparty recognition framework is comprised of several distinctive components:

- The operational and governance processes
- The governance bodies, with roles and responsibilities
- The principles, criteria and requirements for multiparty recognition
- The repository of security, privacy, evidence and audit requirements

These components are organised and multilaterally interact within a 3-step lifecycle "Evaluate-Execute-Govern", which defines the starting and ending points of the multiparty recognition activities (see D1.4 and D2.1). The "evaluate" step of the life cycle includes the framework's assessment activities that take place before any execution activity. In this step, a request for multiparty recognition between two certification schemes will be assessed for compliance against the framework's established principles, criteria and requirements.

The actual multiparty recognition comparison activities take place within the pure operational context of the framework, that is, the "execute" step of the lifecycle. The operational phase is

defined by five ordered activities as shown in Figure 3 (see the five ordered light blue chevrons). Finally, the "govern" step, is dedicated to the governance of the multiparty recognition framework. It defines the organisational, managerial and maintenance activities for all incorporated components, based on which all activities taking place within the other two life cycle steps become possible. Two main processes have been defined in governance, the change and complaint management processes.

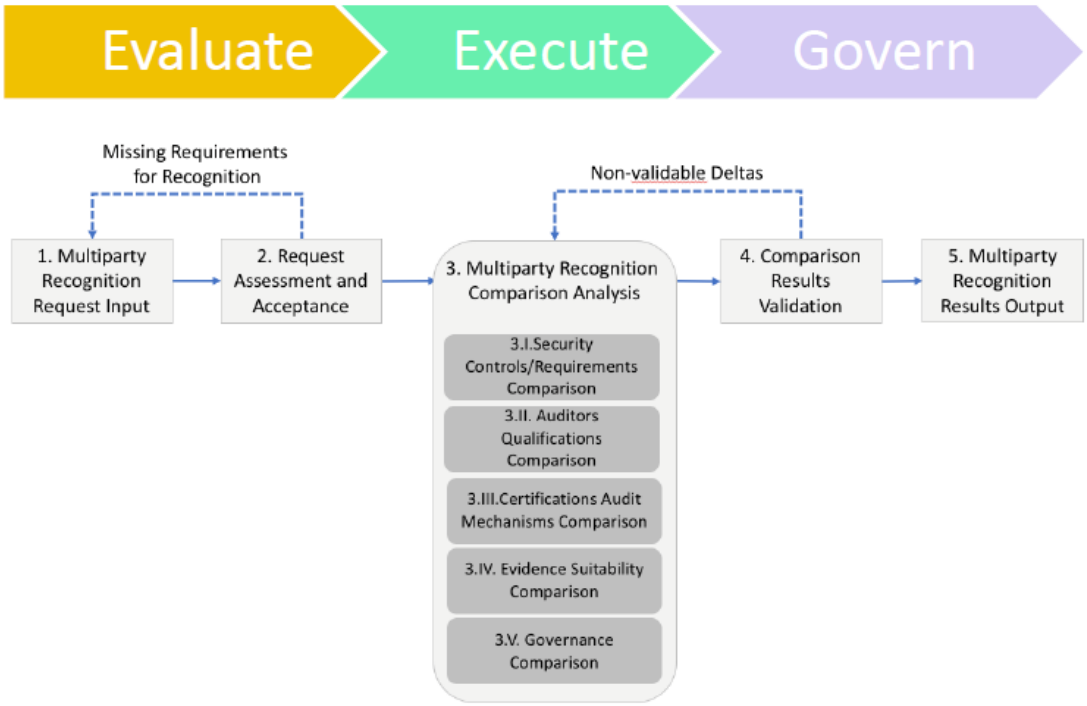

Figure 3: Multiparty Recognition Framework Process Diagram

2.3.2. CONTINUOUS AUDITING CERTIFICATION SCHEME

Continuous auditing introduces an enhancement for the traditional "point-in-time" certification by increasing the assessment frequency via automation and the continuous workflow. Continuous auditing is capable of giving assurance on the certification status continuously. It is an approach of breaking down controls to their characteristic objectives and providing suitable evidence on their fulfilments.

In terms of continuous auditing, certification is approached as a set of controls. Key to a successful continuous auditing setup is this break down, which is addressed in the EU-SEC Framework as the process of operationalisation. This process has to be performed by the CSP individually and adequately according to their organisation and IT-infrastructure. The EU-SEC Framework offers guidance on operationalising the controls applied to the organisations' need

for security and defines characteristics of automatable and non-automatable controls. Continuous auditing operates in phases and enables a trustworthy implementation, so that it provides assurance on compliance to all stakeholders. Details are provided in previous works (see D1.4 and D2.2).

Thus, continuous auditing in the context of EU-SEC Framework is an extension of the traditional understanding. It is still based on and derived from existing standards, in particular ISO/IEC 19086, which defines the notions of Service Qualitative Objective (SQO) and Service Level Objective (SLO). Continuous auditing introduces the more frequent assessment of a control. Therefore, it requires some degree of automation, otherwise it results in unreasonable high costs. Unfortunately, a fully automated audit is currently an unattainable goal. Current audit frameworks do not lend themselves to automation and we need to consider what can be automated and what still requires human intervention. By the implementation of a particular instance of continuous auditing as well as an IT-infrastructure (according to the circumstances) for an organisation, it is suggested to – whenever possible – use tools and automate processes that will evaluate audit criteria automatically.

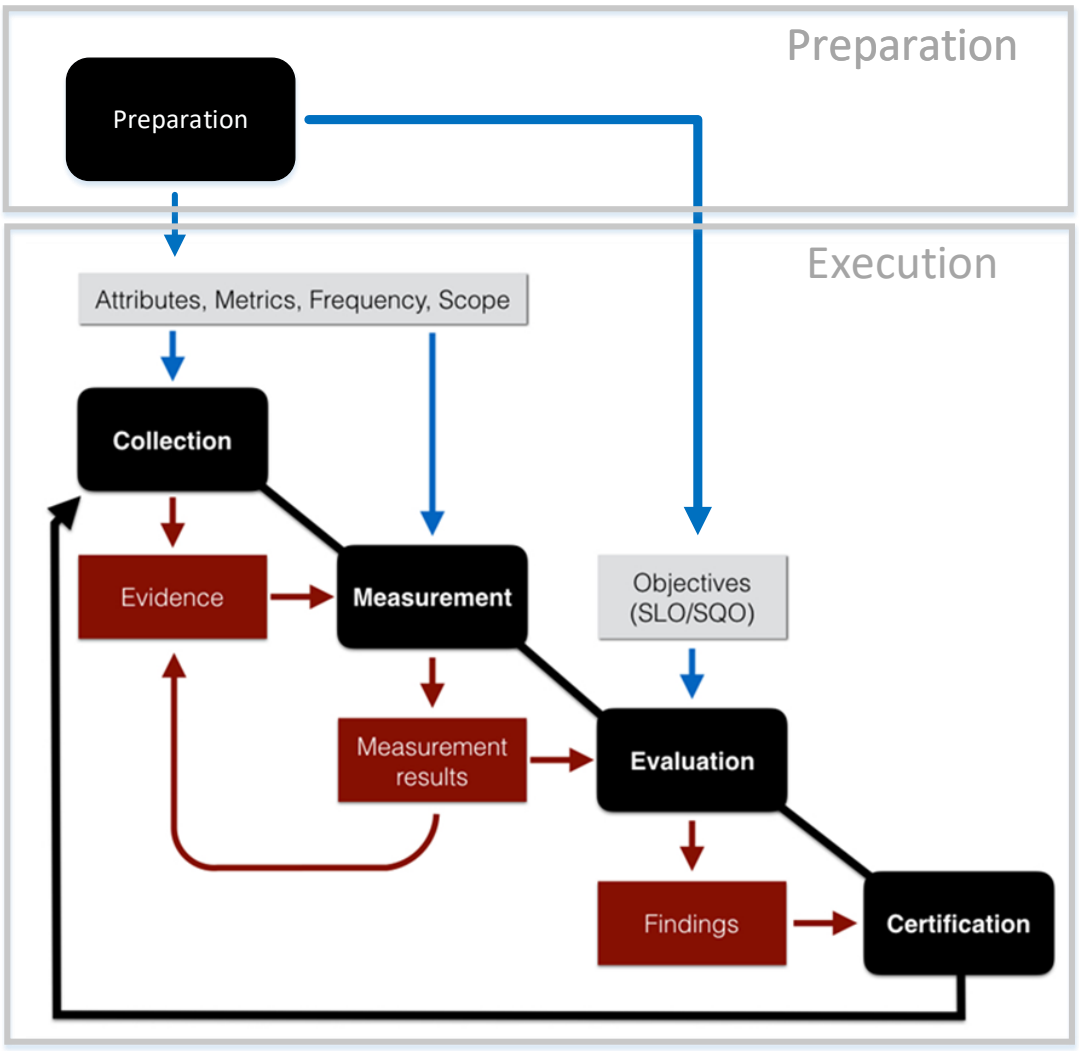

Figure 4: Model of Continuous Auditing Phases

From an architectural point of view continuous auditing can be broken down into 5 phases (See Figure 4).

The first phase has to be performed once at the initialisation. In the preparation phase, the proper operationalisation of the selected set of controls takes place. Key actions in this phase are the definition of the scope, the identification of the objectives (SQO and SLO) associated to each control, the determination of the frequencies at which each objective should be checked, the definition of attributes and metrics, as well as the identification of points where the measurements should be taken.

After continuous auditing is implemented, all other four phases are executed continuously. "Collection" facilitates the collection of data for the automated assessment as well as for the non-automated assessment. Collection of data is driven by the metric that has been chosen to provide input about an attribute. In the context of continuous auditing, data is referred to as

evidence. The measurement phase describes the processing that transforms the collected raw data into a usable measurement result.

In the context of continuous auditing a measurement result quantifies or qualifies an attribute. Attributes require the measurement result to be in a particular format or representation. This way of conducting the measurement and interpreting the raw data is usually defined in a metric. In the evaluation phase, the compliance status and the certification goal are determined by evaluating the controls. The evaluation phase is about compiling information on controls from attributes. The result of the evaluation has to be published according to the chosen continuous auditing certification scheme.

The EU-SEC framework proposes three models for continuous auditing. Each model provides a different level of assurance by covering requirements of continuous auditing with various levels of scrutiny. The three models that we define and are represented in the Figure 5 are:

1. Continuous self-assessment is an assessment of a cloud service that is performed regularly by the auditee, with results being published at a predefined frequency, under the supervision of a governing body.
2. Extended Certification with Continuous Self-assessment combines a "point-in-time" certification conducted by an external auditor with the continuous self-assessment. We qualify this "point-in-time" certification as "extended" because it is based on a traditional third audit party audit with assessment activities that are further broadened to cover the processes, governance and tools used for the self-assessment.
3. Continuous Certification consists of a combination of a point-in-time certification and a continuous audit that are both conducted by an accredited external auditor. The point-in-time certification serves as a "reference" starting point and is followed by continuous audits, the findings of which are reported at a predefined frequency to the Governing Body.

Figure 5: Assurance stack

2.3.3. PRIVACY CODE OF CONDUCT

EU-SEC Consortium has established the Privacy Code of Conduct (Privacy CoC) as a guidance and a compliance tool to Cloud Service Providers that need to adhere to the requirements of the EU-GDPR as well as a mechanism to cloud customers to evaluate the privacy posture of a Cloud Service Provider and the level of privacy that could be offered by a cloud service. The Privacy CoC will play a fundamental role in the context of the EU-SEC framework since it will be the tool that helps addressing one of the main limitations of existing certifications for cloud services, i.e., focusing almost exclusively on information security and not providing a means to show compliance with privacy requirements.

Privacy CoC is composed of two essential components. The first is the Privacy Level Agreement Code of Practice (PLA CoP), which can be considered as the "technical standard" and includes a set of controls that a CSP should implement in order to establish adherence to the EU-GDPR requirements. The second component is the governance structure, which describes the governance bodies and the processes in place in order to guide the revision of the Privacy CoC's technical document, to drive and monitor the mechanisms of adherence to the Privacy CoC.

The Privacy CoC is a voluntary mechanism of adherence to EU-GDPR requirements and transparency and will provide two levels of assurance:

- The Privacy CoC Self Attestation and
- The Privacy CoC Third Party Certification

Currently, the Privacy CoC deals only with the Business-to-Business (B2B) scenario, considering cloud customers as companies rather than individuals (as opposed to Business-to-Consumer,

or B2C scenarios) and addresses two types of customer situations: the cloud customer is the data "controller" and the CSP is the data "processor" or both the cloud customer and the CSP are data controllers. Therefore, it is recommended to the users of the Privacy CoC to carefully evaluate the respective privacy roles of the parties involved on a case-by-case basis in order to clearly identify related obligations.

The Privacy Requirements in the Privacy CoC are classified as follows:

1. CSP Declaration of Compliance and Accountability
2. CSP Relevant Contacts and Its Roles
3. Ways in Which Data Will Be Processed
4. Recordkeeping
5. Data Transfer
6. Data Security Measures
7. Monitoring
8. Personal Data Breach
9. Data Portability, Migration and Transfer Back
10. Restriction of Processing
11. Data Retention, Restitution and Deletion
12. Cooperation with the Cloud Customer(s)
13. Legally Required Disclosure
14. Remedies for Cloud Customer(s)
15. CSP Insurance Policy

More information regarding the governance and adherence mechanisms of the Privacy CoC can be found in D2.3 Privacy Code of Conduct.

2.4. GOVERN DOMAIN

The base for the Govern domain of the EU-SEC Framework was defined in "D1.4 Principles, Criteria and Requirements for a Multiparty Recognition and Continuous Auditing Based Certifications" (section 3.1), which introduced a lifecycle process composed of three main steps, as shown in Figure 1. This lifecycle was also the basis for "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (section 4) and "D2.2 Continuous Auditing Certification Scheme" (section 6).

In D1.4, the essential elements of governance were also defined, including the permanent monitoring, updating of procedures, reacting to recent changes, addressing the stakeholder's needs, etc. Based on the input from D1.4, the EU-SEC Framework's governance is established to ensure the efficiency and effectiveness of operation of the framework. Furthermore, it ensures that the framework's execution is following the framework lifecycle process and meeting the rapidly cloud certification market changing.

Five main governance processes are designed to achieve the goals, namely:

- **Policy and role management:** it focuses on the definition and establishment of EU-SEC policies and procedures to provide guidance to management and operational activities.
- **Resource management:** it focuses on the human, IT and financial resource planning and allocation to ensure the ongoing operations of the EU-SEC Framework.
- **Complaint management:** it focuses on the collection of the feedbacks and complaints regarding the EU-SEC Framework to understand better the stakeholders' needs. The collection could be used as input for the further improvement of the EU-SEC Framework.
- **Change management:** it focuses on identification and implementation of necessary changes in the EU-SEC Framework, including the changes in each EU-SEC Framework component, security and privacy requirements repository and in the EU-SEC operation and governance processes. The actions taken will further improve the EU-SEC Framework.
- **Monitoring and measurements:** it focuses on the periodically and continuously monitoring of the EU-SEC Framework from an operational and management perspective to detect deficiencies and drive corrective actions.

These governance processes are designed to guide the operation activities, assign necessary resources, collect issues and events from the execution of the EU-SEC Framework and improve the framework continuously.

The governance processes are described in section 5 in details.

3. INTRODUCTION TO EU-SEC FRAMEWORK'S GOVERNANCE

The following sections outline the need for governance, the enablers for an efficient and effective governance and how these enablers contribute to the framework. Meanwhile, the requirements for the governance body are defined and described to build up the guideline for the design and the establishment of the EU-SEC Governance Body Organisation.

3.1. THE NEED FOR GOVERNANCE

The cloud computing compliance and certification market is rapidly changing day to day. New international or national standards or additional security and privacy requirements are developed and brought to market to mitigate new risks identified through the development of cloud computing and technology. The EU-SEC Framework with all its main components (Multiparty Recognition Framework, Continuous Auditing Certification Scheme, and Privacy Code of Conduct), as well the tools and processes supporting the framework aims to always reflect the current status of the cloud computing certification and scheme needs, as well as the stakeholder needs.

In order to address those needs, conditions and requirements have to be evaluated and acted upon in a structured governance approach, which allows determining balanced, agreed-on objectives to be achieved; setting direction through prioritisation and decision-making; and monitoring performance and compliance against agreed-on direction and objectives. The desired governance approach comprises the components of the governance domain described in section 2.1. The effective and efficient work of these components depends on a set of "Governance Enablers" derived from COBIT 5 that are described in the following section.

3.2. GOVERNANCE ENABLERS AND THEIR CONTRIBUTION TO THE EU-SEC FRAMEWORK

The following seven "Governance Enablers" are factors that, individually and collectively, influence the effective and efficient work of the components in the Governance Domain of the

EU-SEC Framework and they will contribute to the overall objective of addressing stakeholder needs. They are derived from COBIT 5, good-practice framework for IT management and IT governance created by the international professional association ISACA.

3.2.1. PRINCIPLES, CRITERIA AND REQUIREMENTS

Principles, criteria and requirements are the vehicle to translate the desired behaviour into practical guidance for the execution of the EU-SEC Framework (comprises "D1.4 Principles, Criteria and Requirements for a Multiparty Recognition and Continuous Auditing Based Certifications", "D2.1 Multiparty Recognition Framework for Cloud Security Certification", "D2.2 Continuous Auditing Certification Scheme" and "D2.3 Privacy Code of Conduct"). It will ensure that the Multiparty Recognition Framework and the Continuous Auditing Scheme will be executed in accordance with established requirements.

Principles provide the foundation for an effective governance. Hence, they are reflected on each level of the governance. Five main principles apply to the governance of whole EU-SEC Framework, as an extension of the principles defined in D1.4:

- **Accountability:** Responsibilities are carried out by different governing bodies. Accountable/Governing Bodies are set to identify gaps, suggest improvements and initiate processes.
- **Transparency:** Assuring transparency and integrity throughout the governance of events and triggers is a crucial goal, in order to provide assurance on all levels.
- **Trustworthiness:** If the process is not trusted, the resulting outcome will have lower value. Trustworthiness is achieved by a combination of mechanisms, notably the use of independent governing bodies, which are formally established.
- **Awareness:** It is crucial to be able to respond to events (especially exceptions) at any time. Furthermore, awareness on responsibilities as well as the EU-SEC Framework's performance are very important as well.
- **Stakeholder-Benefit:** The EU-SEC Framework has to be beneficiary for the stakeholders.

3.2.2. ORGANISATIONAL STRUCTURES

Organisational structures as the key decision-making entities consist of reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives to be defined in section 4. The organisational structures will contribute to effective and efficient decision-making, e.g. when it comes to the evaluation of complaints, changes or requests for multiparty recognition.

The organisation has to facilitate the bodies and structures that execute this governance and operate EU-SEC Framework. As an enabler for governance the organisational structure has the following requirements:

- Stakeholders within the organisation can be external or internal and include all entities related and affected by EU-SEC Framework's operation. Thus, it is required that the stakeholders obtain consents on the individual role in the organisation. The role has to be specific with regard to the characteristics which include decision making, advising and influencing capabilities.
- A proper mandate, well-defined operating principles and the application of EU-SEC Framework's principles and guidelines are the goals for the operational structure enabler.
- The lifecycle has to be defined and establishes the creation, existence, adjustment and if required the disbanding of the current organisational structure.
- Practical arrangements for the operation of the structure have to be defined such as: frequencies of meetings, documentation, housekeeping rules, etc.
- The composition between external and internal stakeholders has to be made.
- Span of control, which is basically the boundaries of the organisational decision rights has to be defined.
- Decisions that the structure is allowed to take have to be clarified, and rights have to be granted.

3.2.3. PROCESSES

Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving objectives. Processes are defined as a collection of practices influenced by other enablers such as principles and guidelines. Processes are taking inputs from several sources such as all kinds of information as well as other processes and manipulating those inputs to produce outputs like changes or communication activity results. In the case of the EU-SEC Framework, the inputs are generally characterised by its objective thriving forces and the outputs are either leveraging on the ambitions or its supporting goals. Processes have to be designed with a set of goals.

These goals inside EU-SEC are considered under the following categories:

- Intrinsic goals for the processes must have a certain quality that is in line with EU-SEC Project's ambitions and goals as well as its principles, guidelines and practices.

- To comply with contextual goals, processes are required to be customised and adapted to EU-SEC's specific situations. The process also has to be relevant, effective, understandable and easy applicable.
- Accessibility goals require all process to be accessible to those who need it.
- Security goals require the processes to remain confidential and be exposed only to the required participants. Public available processes have to be declared as such.

Another requirement to processes demands them to consider internal and external stakeholder interests. Internal stakeholders include the body executing this governance structure as well as staff and volunteers. External Stakeholder to the EU-SEC organisation are all entities that are affected by its actions and targeted directly via the EU-SEC Project's goals.

The governance processes are addressed in section 5.

3.2.4. ARCHITECTURE AND TOOLS

Architecture and Tools include the infrastructure, technology and applications that provide the framework with information technology processing for the services. The architecture and tools are described in D3.1, D3.2, and D3.3, which are designed and implemented to support the processes of the Continuous Auditing Scheme.

Architecture and Tool's capabilities are referring to the necessary services and their integration in the EU-SEC Framework governance. Those services enable communication and other capabilities. For the services to work inside the EU-SEC governance it's required to define a proper architecture. Services can be provided by external or in-house parties, such as internal IT departments. Internal and external stakeholders have to be granted access to the tools according to their level of involvement. Goals for services have to be established by defining terms of services. Other requirements for architecture and tools used in the EU-SEC Organisation are:

- Define services as architecture components
- Define components in a way that allows the reuse of those in similar applications.
- Define decision guidelines for when to buy a solution or when to build
- Thrive for a simple architecture and the usage of open standards

3.2.5. INFORMATION

Information is pervasive throughout the framework and it is required for keeping it well governed. Information is key to the governance of the EU-SEC Framework. Thus, information handling has to be defined as a crucial part of the governance. Each sort of information has to be considered as relevant to the EU-SEC Framework, regardless whether the information is structured or unstructured, obtained automatically or manual or formalised or uniformalised.

As part of enabling governance, it is necessary to define an information handling capability that:

- transforms data into information and then into knowledge,
- creates values for EU-SEC Framework from this knowledge,
- establishes values drive processes for EU-SEC Framework, and
- generates data throughout those processes that it can be considered information.

It is also necessary to identify which EU-SEC Framework's stakeholder is interested in which kind of information. This might require to define roles and responsibilities based on the information the particular stakeholder is dealing with. Another aspect that has to be defined respective to information is in which way it is handled. Some possibilities are:

- Information is produced by the stakeholder
- Information is stored and maintained by the stakeholder.
- Information is processed by the stakeholder
- Information is consumed by the stakeholder

Information has to be accurate, objective and believable in order to be a suitable intrinsic quality. Other aspects like relevancy, completeness, currency, appropriate amount, interpretability, understandability and ease of manipulation have to be fulfilled as well. With extend to security and accessibility, it is crucial that information is available only to authorised parties. For those authorised parties, the information has to be available or easy and quick to retrieve.

3.2.6. CULTURE, ETHICS AND BEHAVIOUR

Culture, ethics and behaviour (e.g., towards taking risks, following policies or negative outcomes) have to be created, encouraged and maintained by defining and communicating rules and norms (e.g. "D2.3 Privacy Code of Conduct"), running awareness campaigns and providing incentives and rewards. Culture, ethics and behaviour will ensure that the individuals

or groups responsible for the execution of the framework act with integrity in pursuit of achieving the goal for trustworthiness.

Culture, ethics and behaviour define the set of individual and collective behaviours inside the EU-SEC Organisation. Those are mainly driven by the principles and guidelines of EU-SEC Framework. They must be introduced to internal and external stakeholders. For the EU-SEC Organisation, it is required to address these issues specific to a certain external stakeholder like national bodies, regulators or supervising bodies. It is also required to enforce the implementation on other external third parties acting on behalf of EU-SEC Organisation for the organisation's interest. Organisational ethics and the expectations to the individuals working for the organisation have to be defined as well. Individual behaviour determines the organisation's culture. This requires the following subjects to be addressed:

- Resolution on how much risk EU-SEC Organisation can absorb and which risk it is willing to take.
- Agreement on the individual commitment of people towards following policies.
- Agreement upon the organisations behaviour towards negative outcomes.

3.2.7. PEOPLE, SKILLS AND COMPETENCIES

People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions. They are required to perform process activities and take decisions in organisational structures to govern and execute the framework.

Tasks inside the EU-SEC Organisation require the highest level of suitability with regard to assigning the right people. This begins with the definition of the roles of the stakeholders. External stakeholders are relatively easier to be chosen, but a distinct skill set is required to choose/hire these following roles:

- Partners
- Recruiters
- Trainers
- Developers
- Technical IT specialists

The main goal in assigning people is to ensure that the individual competencies match the required skill. Therefore, the required skills and competencies have to be determined for

operation of the EU-SEC Organisation, which should relate to education and qualification levels.

3.3. GOVERNANCE BODY REQUIREMENTS

The organisation managing the EU-SEC Framework (hereafter referred to as "Governance Body") has to be capable of executing the governance described in this document. This requires a form of management that has to be defined and implemented according to the needs, ambitions and requirements of the EU-SEC Framework. This does not necessarily require the establishment of a new organisation. As long as it is capable of executing this governance as an existing entity, it is equally suitable of facilitating the EU-SEC Framework.

Suitable management requires organisational structures, reporting lines, authorities, and responsibilities, especially within the following domains:

- Supervision
- Finance
- Technology
- Public relations, incl. working group management

To ensure the operation effectiveness of activities in these domains, their execution has to be assessed. This requires pro fund monitoring performance and compliance checking, which includes the following actions:

- Identification and definition of indicators for performance
- Frequent monitoring of those indicators
- Establishing management reviews
- Establishing internal and external audits

4. GOVERNANCE BODY ORGANISATION

The requirements for the EU-SEC Governance Body described in section 3.3 require an organisation with defined structures, reporting lines, authorities, and responsibilities. These are influenced by the operational model for the execution of EU-SEC framework after go-live.

The following sections will outline baseline considerations for the operational model along three options, which will be discussed by the consortium members in the course of the ongoing project.

4.1. OPERATIONAL MODEL CONSIDERATIONS

The previous deliverables have introduced the EU-SEC Governance Body as the overall function and trusted party who is responsible for designing, executing, and coordinating the EU-SEC Framework. This requires an operational model, for which the members of the EU-SEC Consortium have not yet taken a decision. As of June 2018, three options are under consideration:

- Option 1 - The members of the consortium will build a new organisation
- Option 2 – CSA[1] will take the role of the Governance Body
- Option 3 – ENISA[2] will take the role of the Governance Body

The decision will be taken within the next 12 months after an in depth analysis of the pros and cons specific to each option.

4.2. ROLES AND RESPONSIBILITIES WITHIN THE EU-SEC GOVERNANCE BODY

This section outlines the design of the EU-SEC Governance Body under the assumption of a flexible and agile governance suitable for young developing organisations. The governance

[1] Cloud Security Alliance, member of the project consortium
[2] European Union Agency for Network and Information Security

body will comprise several roles with assigned responsibilities. These are described along the domains for governance and execution as introduced in section 2.

4.2.1. ROLES AND RESPONSIBILITIES FOR THE GOVERNANCE DOMAIN

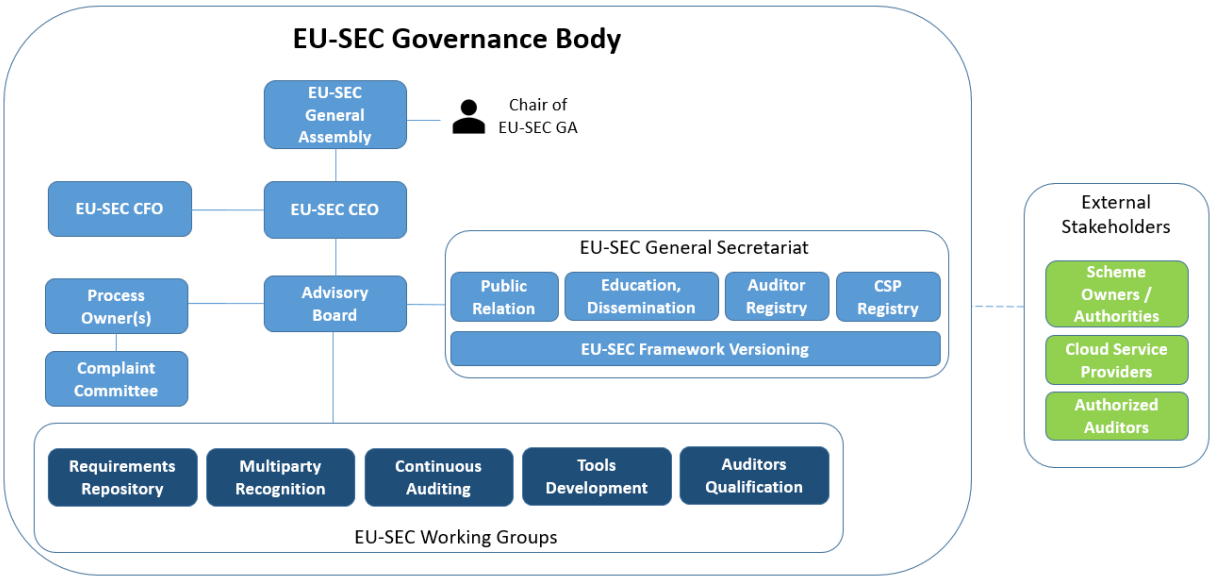

Figure 6: EU-SEC Governance Body

In the governance domain, the EU-SEC governance body is responsible for the design and maintenance of the EU-SEC framework based on stakeholder needs and for directing all requirements to the multiparty recognition framework and continuous auditing scheme

Under the assumption, that members of the consortium build a new organisation (see Option 1 above), the following roles (incl. boards and committees) will likely be defined to constitute the EU-SEC Governance Body. If the consortium decides that an existing organisation will take the framework, some of the roles may be adjusted. These adjustments will be reflected in final version of the EU-SEC Framework (D2.5).

EU-SEC General Assembly

The EU-SEC Assembly constitutes of EU-SEC consortium members.

Role	Responsibilities
EU-SEC General Assembly	• Elects the Chair of EU-SEC Assembly • Appoints the EU-SEC Chief Executive Officer (CEO) • Appoints the EU-SEC Chief Financial Officer (CFO) • Decides about EU-SEC policy and new members

	• Adopts the annual report and annual activities plan • Adopts the working groups' major changes proposals

Chair of EU-SEC General Assembly

The EU-SEC Assembly President is the public representative of the EU-SEC.

Role	Responsibilities
Chair of EU-SEC General Assembly	• Represents the EU-SEC General Assembly, serving as an ambassador of the organisation and advocating its mission to internal and external stakeholders • Calls and presides the meetings of the General Assembly

EU-SEC Chief Executive Officer (CEO)

The EU-SEC CEO is the public representative and takes the legal responsibility of the EU-SEC organisation.

Role	Responsibilities
EU-SEC CEO	• Represent the EU-SEC • Legally responsible • Decision-maker • Reports to EU-SEC General Assembly • Coordinates external parties (Scheme owner, CSP, Auditors) • Presides the Advisory Board and coordinates the different working groups • Business development: analyses the market, assess marketing opportunities and determine measures for further business area development

EU-SEC Chief Financial Officer (CFO)

The EU-SEC CFO is the responsible person for the management of the EU-SEC Organisation's finances.

Role	Responsibilities
EU-SEC CFO	• Reports to EU-SEC General Assembly

	• Establishment of financial planning • Decision-maker on budget and financial resource allocation • Maintenance of record-keeping • Execution of financial reporting

EU-SEC Advisory Board

The EU-SEC Advisory Board consists of representatives (managers) of working groups. Supports the Change Management Process, approves and prioritises requested changes and suggests the improvements of EU-SEC governance.

Role	Responsibilities
EU-SEC Advisory Board	• Accepts relevant cases from Complaint Committee • Approves requested changes • Prioritises requested changes • Prepares updates for educational and dissemination material • Suggests the improvements of EU-SEC governance

EU-SEC Complaint Committee

The EU-SEC Complaint Committee handles and processes the reported complaints, suggestions and incidents regarding the EU-SEC framework and ensures the proper operation of the process and provide solutions to improve the framework. It reports to EU-SEC Advisory Board on the operation of the process with recommendations for improvement.

Role	Responsibilities
EU-SEC Complaint Committee	• Ensures that the complaints-handling process and objectives are established within the EU-SEC organisation • Ensuring that the complaints-handling process is planned, designed, implemented, maintained, operated and continually improved in accordance with the requirements set out in section 5. • Ensuring that information about the complaints-handling process is communicated to stakeholders, complainants, and, where applicable, other parties directly concerned in an easily accessible manner • Establishing a process of performance monitoring, evaluation, and reporting for complaints management • Reporting to EU-SEC Advisory Board on the complaints-handling process, with recommendations for improvement

EU-SEC General Secretariat

The EU-SEC General secretariat performs different supporting roles of EU-SEC governance.

Role	Responsibilities
Public Relations	• External communication • Performs promotions for EU-SEC • Maintains a favourable public image • Defines and maintains external communication standards
Education and Dissemination	• Prepares and maintains the education and dissemination material • Organises the education and dissemination events • Publishes guidelines
Auditor Qualification Registry	• Maintains the Auditor Qualification Registry
Certified CSPs Registry	• Maintains the EU-SEC certified Cloud Service Provider registry
EU-SEC Framework Versioning	• Cares about updating EU-SEC Framework versioning in all relevant material and communication • Informs the stakeholders about EU-SEC Framework changes

EU-SEC Process Owner

The EU-SEC Process Owner is responsible for the processes that are assigned to him/her. The process owner must ensure that the process is being executed properly. The owner reports to EU-SEC Advisory Board on the operation of the process with recommendations for improvement. The title is specified according to the process they are assigned to, e.g.: Head of Change Management, Head of Complaint Management, Head of Monitoring and Measurements, Head of Policy and Role Management, Head of Resource Management.

Role	Responsibilities
EU-SEC Process Owner	• Ensures that the process execution is carried out effectively • Handles the occurring problem within the process • Establishing a process of performance monitoring, evaluation, and reporting for EU-SEC Advisory Board

4.2.1.1. WORKING GROUPS

In order to maintain all the components and topic within the EU-SEC Framework, the Working Groups are required to take the responsibilities to ensure the operation of each component of and a certain topic of the EU-SEC Framework.

The following Working Groups are required for the operation of the EU-SEC Framework and its components and support the governance processes and activities:

- **Requirements Repository Maintenance**

  The EU-SEC requirements repository maintenance group evaluates the EU-SEC Framework continuously regarding new requirements, updates and maintains the repository.

- **Multiparty Recognition Analysis**

  The Multiparty Recognition Analysis working group identifies and collects new cloud certification and compliance schemes, regulations, standards and future market trends.

- **Continuous Auditing Certification**

  The Continuous Auditing Certification working group identifies and collects new demands for continuous auditing to improve and to maintain the EU-SEC continuous auditing certification scheme. Prepares the recommendations on data formats and data exchanges to enable measurability through external auditors.

- **Tools Development**

  Tools Development working group ensures the functionality of the used tools and ensures the further development and maintenance of these tools.

- **Auditor Qualification / Registration / Accreditation**

  The auditor qualification, registration and accreditation working group selects and validates auditors regarding their qualifications, registers the auditor within the EU-SEC Framework and hands over an accreditation certificate to the auditor.

4.2.1.2. EXTERNAL STAKEHOLDERS

The external stakeholders are not directly involved in the governance of the EU-SEC framework. However, they are very important to provide valuable inputs for its ongoing maintenance and future development.

- **Scheme Owner / Authority**
  The Scheme Owner / Authority has no additional roles and responsibilities as mentioned in "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (section 4.2) and "D2.2 Continuous Auditing Certification Scheme" (section 6.1).

- **Cloud Service Provider**
  The Cloud Service Provider has no additional roles and responsibilities as mentioned in "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (section 4.2) and "D2.2 Continuous Auditing Certification Scheme" (section 6.1).

- **Authorised Auditors**
  The Authorised Auditors has no additional roles and responsibilities as mentioned in "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (section 4.2) and "D2.2 Continuous Auditing Certification Scheme" (section 6.1).

4.2.2. ROLES AND RESPONSIBILITIES FOR THE EXECUTION DOMAIN

In the execution domain, the EU-SEC Governance Body has different roles and responsibilities for multiparty recognition framework and continuous auditing scheme. The different roles and responsibilities are outlined in "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (section 4.2) like organisation and operation of all defined governance processes as well as coordinating working groups and "D2.2 Continuous Auditing Certification Scheme" (section 6.1) like qualifying external auditors to perform audits as well as establishing rules for recognition of external auditors.

5. GOVERNANCE PROCESSES

The cloud computing certification and compliance landscape is rapidly changing these days. New international or national standards and additional security and privacy requirements are developed and brought to market to mitigate new risks, which are identified through the development of cloud computing and technology. The EU-SEC Framework with all its main components (multiparty recognition framework, continuous auditing certification scheme, and privacy code of conduct), as well as the tools and processes that support the framework aims to reflect the current status of the cloud computing compliance and scheme needs, as well as the stakeholder needs.

An EU-SEC Framework governance structure must be defined to enable an efficient and effective operation of the framework, and to handle and integrate the needs from stakeholders and changes in the compliance landscape. Based on our goals, the EU-SEC Framework governance structure with five governance processes are designed and introduced in this section.

Since the discussion on how the EU-SEC Governance Body Organisation will be set up is still on-going, the governance model introduced in D2.4 is the model in the current stage of EU-SEC Project. After the decision regarding the EU-SEC Governance Body Organisation has been settled, the EU-SEC Framework should be adjusted according to the defined organisation structure and stakeholders' needs, and details of the governance processes could be modified and extended to utilise the EU-SEC Framework. The final version of EU-SEC Framework will be published in the next deliverable D2.5 "EU-SEC Framework – Final Version" at the last stage of the EU-SEC Project.

5.1. POLICY AND ROLE MANAGEMENT

Policies reflect management's statement of what should be done to effectively control the organisation and its operation. The management's statements shall be stated in communications, or implied through management's actions and decisions. Procedures consist of actions that implement a policy. Policies can be created in form of guidelines, rules, regulations, etc. On the other hand, roles indicate the responsible person for the defined aspects in the policies. Both of them are highly important for the governance, as it decides the principles and the responsible people of the governed system.

Policy and role management aims to create a harmonised system with guidance to operate, manage and govern the organisation. The policy and role management process comprises seven activities – starting from setting the goals of the organisation until the reassessment of the policies and procedures.

5.1.1. GENERAL POLICY AND ROLE MANAGEMENT PRINCIPLES AND REQUIREMENTS

The following principles and related requirements are derived from the Committee of Sponsoring Organisations of the Treadway Commission (COSO) "Internal Control - Integrated Framework" Principle 12, which outlines the necessity that the organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

"Principle 12: The organization deploys control activities through policies that establish what is expected and procedures that put policies into action."

Table 1: Principles and Related Requirements for Policy and Role Management

PRINCIPLE	REQUIREMENT
Policies and Procedures	Establishes policies and procedures to support deployment of management's directives.
Responsibility and Accountability	Establishes responsibility and accountability for executing policies and procedures.

PRINCIPLE	REQUIREMENT
Timeliness	Responsible personnel performs control activities in a timely manner as defined by the policies and procedures.
Corrective Action	When deviation from policies and procedures is identified, responsible personnel investigate and act on matters identified as a result of executing control activities.
Competence	Policies and procedures require that competent personnel with sufficient authority perform control activities with diligence and continuing focus.
Periodic Reassessment	Management periodically reviews the policies and procedures with defined control activities to determine their continued relevance, and refreshes them when necessary.

5.1.2. POLICY AND ROLE MANAGEMENT PROCESS

The policy and role management process comprises seven activities as outlined in the table below:

Table 2: The policy and role management process card: the inputs, the activities and the outputs.

Policy and Role Management Process	
Inputs (upstream)	- Objectives of the EU-SEC project and EU-SEC Framework - EU-SEC project outcomes (submitted deliverables) - Request / requirements from Multiparty Recognition Framework - Request / requirements from Continuous Auditing Scheme - Request / requirements from Privacy Code of Conduct - Request from Change Management - Request from Complaint Management - Request from Resource Management - Current and future demands
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

Policy and Role Management Process	
	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. Reassess and update the policies and procedures periodically
Outputs (downstream)	- EU-SEC policies and procedures in written form

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 3. The policy and role management process activities' mapped to roles and responsibilities.

Policy and Role Management Process		**Activities**						
		#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**
Roles	EU-SEC CEO	C	R	R	A	A/R	A	A
	EU-SEC CEO Office	C	R	R	R	C/I	R	R
	EU-SEC General Assembly	A	A	A	R	C/I	I	C/I
	Advisory Board	C/I	C/I	C/I	C/I	A/R	I	C/I
	Subject-matter Expert (business units)	C/I	C/I	C/I	C/I	C/I	I	C/I
	Subject-matter Expert (external)	C/I	C/I	C/I	C/I	C/I	I	C/I
	Target Audience of policies and procedures	I	I	I	I	I	I	I
R – Responsible, **A** – Accountable, **C** – Consulted, **I** – Informed								

The policy and role management process activities and the underlying sub-activities are described in more detail in the subsections below.

5.1.2.1. ACTIVITY #1: SET THE GOALS AND DIRECTIVES OF THE EU-SEC ORGANISATION

Abstract: The goals and directives must be defined firstly to provide direction of how EU-SEC Organisation functions and how the EU-SEC Framework is governed.

Table 4. The Policy and Role Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1	
List of the activities: *1# The EU-SEC General Assembly shall set the goal of the business and the directives of the EU-SEC Organisation. Only with a clear objectives definition, the profound instructions and guidance could be established to concrete the requirements and measures on to achieve the business objectives.* *2# The goals and directives must be documented in a formal way, approved by the EU-SEC General Assembly and regularly assessed to reflect always the current business status.*	
Inputs (upstream)	**Outputs (downstream)**
1# EU-SEC project objectives 2# EU-SEC project outcomes (submitted deliverables) 3# Request / requirements from Multiparty Recognition Framework 4# Request / requirements from Continuous Auditing Scheme 5# Request / requirements from Privacy Code of Conduct 6# Current and future demands	1# Documented and approved EU-SEC organisation business goals and directives.

5.1.2.2. ACTIVITY #2: ESTABLISH THE ORGANISATIONAL STRUCTURE AND REPORTING LINE

Abstract: The organisational structure shall be established and the reporting lines shall be defined to operate the EU-SEC Framework and perform the governance activities.

Table 5. The Policy and Role Management Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2
List of the activities: *1# The EU-SEC Organisation has to facilitate the bodies and organisational structures that operate EU-SEC Framework and execute the governance. The basic requirements on the organisational structure are addressed in section 3.3.*

Activity #2	
2# *The EU-SEC Organisation has to define reporting lines as basis of decision making process and definition of responsibilities and accountabilities. The reporting lines ensure the information flow within the organisation, which are essential for important decision making and governance of the EU-SEC Framework.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documented and approved EU-SEC Organisation business goals and directives. 2# EU-SEC Project objectives 3# Request / requirements from Multiparty Recognition Framework 4# Request / requirements from Continuous Auditing Scheme 5# Request / requirements from Privacy Code of Conduct 6# Request from Change Management 7# Request from Complaint Management 8# Request from Resource Management 9# Current and future demands	1# EU-SEC organisational structure 2# EU-SEC organisation reporting line

5.1.2.3. ACTIVITY #3: DEFINE THE RESPONSIBILITY AND ACCOUNTABILITY OF ROLES AND GROUPS

Abstract: After the organisational structure has been established, responsibilities and accountabilities of each role and group must be defined to ensure the clear distribution of duties and effective and efficient organisation operation.

Table 6. The Policy and Role Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: 1# *The EU-SEC General Assembly must define the responsibility and accountability of roles, groups and business units, which are established in organisational structure. The responsibilities shall align with the business goals and directives defined in the activity #1.* • *Working areas or groups* • *Functionalities and duties* • *Collaboration and communication*	
Inputs (upstream)	**Outputs (downstream)**

Activity #3	
1# Documented and approved EU-SEC organisation business goals and directives. 2# EU-SEC project objectives 3# EU-SEC organisational structure 4# EU-SEC organisation reporting line 5# Request / requirements from Multiparty Recognition Framework 6# Request / requirements from Continuous Auditing Scheme 7# Request / requirements from Privacy Code of Conduct 8# Request from Change Management 9# Request from Complaint Management 10# Request from Resource Management 11# Current and future demands	1# EU-SEC organisational structure with defined responsibility and accountability for each role, group, and business unit.

5.1.2.4. ACTIVITY #4: ESTABLISH POLICIES AND PROCEDURES TO SUPPORT DEPLOYMENT OF EU-SEC'S DIRECTIVES

Abstract: Policies and procedures must be established to support deployment of EU-SEC's directives, realise the business goals, and guide the organisation operation and governance.

Table 7. The Policy and Role Management Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4
List of the activities: 1# *The EU-SEC CEO Office together with EU-SEC Advisory Board and EU-SEC General Assembly identifies the policies and procedures need to be established. Following policies are recommended to EU-SEC Organisation, while other policies may also be relevant as well, and shall be assessed by needs.* • *Human Resource Management Policy* • *IT service management policy* • *Asset and information security policy* • *Procurement management policy* • *Change management policy* • *Complaint management policy* • *Communication management policy* • *Data privacy policy*

Activity #4	
2# A template of policy and procedure must be established and covers the essential aspects: • *Goals,* • *Scope of application,* • *Roles and responsibilities, including requirements for the qualification of the personnel and the establishment of substitution arrangements,* • *Coordination of different roles, internal groups and external partners,* • *Procedures or measures to realise and achieve the goals,* • *Security architecture and safeguards for the protection of data, IT applications and IT infrastructures,* • *Safeguards for the compliance with legal and regulatory requirements (compliance).* *3# The policies and procedures are established in a written form. While establishing the policies and procedures, the following aspects shall be considered:* • *Business goals and directives,* • *Best practices for policy management* • *Consulting the subject-matter experts (e.g. experts from business units, experts for policy management, etc.)* *4# The established policies and procedures shall be firstly reviewed by the relevant parties to ensure the policies and procedures represent the current status of EU-SEC Organisation.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documented and approved EU-SEC organisation business goals and directives. 2# EU-SEC project objectives 3# EU-SEC organisational structure 4# EU-SEC organisation reporting line 5# Policies and procedures best practices 6# Request / requirements from Multiparty Recognition Framework 7# Request / requirements from Continuous Auditing Scheme 8# Request / requirements from Privacy Code of Conduct 9# Request from Change Management 10# Request from Complaint Management 11# Request from Resource Management 12# Current and future demands	1# EU-SEC policies and procedures in written form

5.1.2.5. ACTIVITY #5: APPROVE THE POLICIES AND PROCEDURES BY EU-SEC CEO AND ADVISORY BOARD

Abstract: Policies and procedures must be approved before they are published and implemented.

Table 8. The Policy and Role Management Process Activity #5 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #5	
List of the activities: *1# The EU-SEC CEO and Advisory Board receive the policies and procedures, and give a final approval. In case of rejection, reasons shall be provided to guide for further improvement. After rework on the policies and procedures, final approval shall be obtained.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documented and approved EU-SEC organisation business goals and directives. 2# EU-SEC organisational structure 3# EU-SEC organisation reporting line 4# Policies and procedures best practices 5# EU-SEC policies and procedures in written form 6# Request / requirements from Multiparty Recognition Framework 7# Request / requirements from Continuous Auditing Scheme 8# Request / requirements from Privacy Code of Conduct 9# Request from Change Management 10# Request from Complaint Management 11# Request from Resource Management 12# Current and future demands	1# Approved EU-SEC policies and procedures in written form

5.1.2.6. ACTIVITY #6: PUBLISH AND COMMUNICATE THE POLICIES AND PROCEDURES WITH ALL RELEVANT PARTIES

Abstract: Policies and procedures shall be made available for the relevant parties, so these can provide the guidance and directives for the EU-SEC Framework's operation, management and governance.

Table 9. The Policy and Role Management Process Activity #6 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #6	
List of the activities: *1# The publication channel is decided and communication plan are established.* • *Publication channel: a document management system or internal storage, where the EU-SEC policies and procedures are stored, and can be accessed by the audience.* • *Communication plan: how the new established policies and procedures are made aware to the target audience, e.g. through Email, workshop, or awareness training, etc.* *2# Establish the publication channel for EU-SEC policies and procedures.* *3# Execute the communication plan to inform the publication of the EU-SEC policies and procedures.*	
Inputs (upstream)	**Outputs (downstream)**
1# Approved EU-SEC policies and procedures in written form	1# Established publication channel for EU-SEC policies and procedures 2# Executed communication with target audience on the EU-SEC policies and procedures

5.1.2.7. ACTIVITY #7: REASSESS AND UPDATE THE POLICIES AND PROCEDURES PERIODICALLY

Table 10. The Policy and Role Management Process Activity #7 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #7	
List of the activities: *1# The existing policies and procedures are reassessed on regular basis, to ensure they represent the current status of EU-SEC Organisation, the EU-SEC General Assembly needs, and further market demand.* *2# Deviations identified shall be updated into the EU-SEC policies and procedures.* *3# Approve and publish the updated policies and procedures according to section 5.1.2.5 and 5.1.2.6.*	
Inputs (upstream)	**Outputs (downstream)**
1# Approved EU-SEC policies and procedures in written form 2# Approved change request to apply a change to an existing policy	1# Updated EU-SEC policies and procedures in written form

5.2. COMPLAINT MANAGEMENT

Information obtained through complaints-handling activities can lead to improvements in the services provided by the EU-SEC framework and, where the complaints are properly handled, can improve the reputation of the organisation behind EU-SEC.

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. The process was initially designed in "D2.1 Multiparty Recognition Framework for Cloud Security Certification" (hereafter "Multiparty Recognition Complaints Process"). This section outlines the complaint management in a more general manner along with the relevant Governance Enablers.

The following Governance Enablers were identified as key for an effective and efficient complaint management:

- **Principles, Criteria, and Requirements** to translate the desired behaviour as outlined in ISO 10002:2014 for complaint management into practical requirements for the EU-SEC framework, which is outlined in section 5.2.1.
- **Processes** that comprise a set of practices and activities to ensure an effective and efficient complaints-handling in accordance with the principles and requirement, which is outlined in section 5.2.2.
- **Architecture and Tools** to track complaints and facilitate communication, for which this deliverable will outline high-level requirements for the functionality of a Complaint Management System (see section 5.2.2).
- **Culture, ethics and behaviour**, which are required to achieve the principles of objectivity and customer-focused approach, see section 5.2.2.

5.2.1. GENERAL COMPLAINT MANAGEMENT PRINCIPLES AND REQUIREMENTS

The following principles and related requirements are derived from the international standard ISO 10002:2014 for complaints handling and shall address the following important aspects of complaints management:

- Defining EU-SEC leadership involvement and commitment through adequate acquisition and deployment of resources, including personnel training;
- Recognising and addressing the needs and expectations of complainants;

- Analysing and evaluating complaints in order to improve the framework;
- Auditing of the complaints-handling process;
- Reviewing the effectiveness and efficiency of the complaints-handling process.

Table 11: Principles and related Requirements for Complaint Management

PRINCIPLE	REQUIREMENT
Visibility	Information about how and where to complain shall be well published to internal and external stakeholders and interested parties on the EU-SEC website and official documents as deemed appropriate (e.g. reports)
Accessibility	The complaints management process shall be easily accessible to all complainants. Information shall be made available on the details of making and resolving complaints. This information shall be easy to understand. Complainants shall receive information and assistance in making complaints (e.g. forms to raise complaints)
Responsiveness	Receipt of each complaint shall be acknowledged to the complainant immediately by the Complaint Management System (standard answer text) or in verbal form. Complaints shall be addressed promptly in accordance with their urgency. The total pass-through time for each step shall be in accordance with the severity of the complaint. The complainants shall be treated courteously and be kept informed of the progress of their complaint through the complaints-handling process.
Objectivity	Each complaint shall be addressed in an equitable, objective, and unbiased manner through the complaints-handling process. The individuals involved in the process shall place emphasise on solving the problem and not on assigning blame. Rewards and incentives will enforce this behaviour.
Charges	Access to the complaints-handling process shall be free of charge to the complainant.

PRINCIPLE	REQUIREMENT
Confidentiality	The process shall be designed to protect the complainant's identity and the content and circumstances of the complaint as far as it is reasonably possible to solve the problem. The need-to-know-principle shall be the guiding principle in collecting information and providing access to this information. Information shall be protected from disclosure, which will be supported by access controls for the Complaint Management System.
Customer-focused approach	The organisation shall adopt a customer-focused approach towards the stakeholders, should be open to feedback including complaints, and shall show commitment to resolving complaints by its actions.
Responsibility & Accountability	The organisation shall ensure that accountability for and reporting on the actions and decisions of the organisation with respect to complaints handling is clearly established by the EU-SEC Complaint Committee.
Continual improvement	The continual improvement of the complaints-handling process and the quality of products shall be a permanent objective of the organisation.

A Complaint Management System (COMS) is required to track complaints and facilitate communication with the complainant. The tool has to fulfil the following functional requirements that were derived from the aforementioned general complaint management principles and requirements.

Table 12: Functional Requirements for a Complaint Management System

PRINCIPLE	FUNCTIONAL REQUIREMENTS
Visibility & Accessibility	The COMS shall be web-based and allow an integration with the EU-SEC website to ensure it is easily accessible to all complainants.
Responsiveness	After a complaint is recorded in the COMS, the complainant shall immediately receive an automated acknowledgement. A unique identifier is assigned to each complaint.

PRINCIPLE	FUNCTIONAL REQUIREMENTS
	The COMS shall support the EU-SEC Complaint Committee to maintain an ongoing communication with the complainant in accordance with the severity level of the complaint. The COMS shall allow the complainant to accept or reject proposed solutions.
Confidentiality	Technical access control measures (user access and authentication management) are available to support the least privilege and need-to-know principles. Information related to complaints is encrypted during transmission and storage.
Responsibility & Accountability	Mandatory fields in the COMS ensure that necessary information is collected when a new complaint is recorded (esp. for complainant contact information and details to support the identification of a solution) Each complaint is assigned to a dedicated individual or group of the EU-SEC Complaint Committee. Notification measures ensure that newly recorded complaints are processed in a timely manner as defined for the activities of the process.
Continuous improvement	The COMS shall provide reporting functions to support the EU-SEC Complaint Committee in monitoring and review activities, e.g. by providing number or proportions of • complaints received within a period of time, • complaints resolved at the point at which they are made, • complaints incorrectly prioritised (severity), • complaints acknowledged after agreed time, • complaints resolved after agreed time, • repeat complaints or recurrent problems that have not been complained about, or • improvements in procedures due to complaints.

PRINCIPLE	FUNCTIONAL REQUIREMENTS
	The COMS shall also provide the ability to collect anonymous feedback from the complainant about his or her satisfaction with the complaints-handling activities

The requirements to support the adherence for the "objectivity" and "customer-focused approach" principles shall be met by establishing and monitoring collective and individual goals for the EU-SEC Complaint Committee and its members. The goals and associated incentives and rewards shall be proposed by the EU-SEC Advisory Board and established by the EU-SEC General Assembly. Example goals should consider numbers or portions about the efficiency and effectiveness of the complaint management process, e.g.

- portion of complaints resolved in time,
- portion of proposed solutions not rejected by complainant (actively accepted or no response after a period of time),
- portion of complaints closed after solution was carried out, or
- satisfaction of the complainant with the complaints-handling activities.

5.2.2. COMPLAINT MANAGEMENT PROCESS

The complaint management process is built up based on the description of the Multiparty Recognition Complaints Process. This process is extended in the EU-SEC Framework view, in order to handle the complaints and issues reported regarding any components and aspects of the EU-SEC Framework.

The complaint management process comprises seven activities as outlined in the table below:

Table 13. The complaint management process card: the inputs, the activities and the outputs.

Complaint Management Process	
Inputs (upstream)	Expression of dissatisfaction (Complaint) raised by a person, organisation, or its representative (Complainant)
Activities (core)	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
Outputs (downstream)	Record of the complaint in the Complaint Management System

The following roles of the EU-SEC Governance body have responsibilities for the complaints management process:

- **EU-SEC Complaint Committee**
- **EU-SEC Advisory Board**
- **Working Groups (as applicable for the complaint)**

The responsibilities are presented in the Responsibility Assignment Matrix per assigned activity, below.

Table 14. The Complaint Management Process activities mapped to roles and responsibilities.

Roles	**Complaint Management Process Activities**						
	#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**
EU-SEC Complaint Committee	A R	A R	A R	A R	A R	A R	A R
EU-SEC Advisory Board	-	-	C	-	-	-	-
Working Groups	-	-	C	-	-	-	-
Complainant	I	-	I	I	I	-	R
R – Responsible, **A** – Accountable, **C** – Consulted, **I** – Informed							

The complaint management process activities and the underlying sub-activities are described in more detail in the subsections below.

5.2.2.1. ACTIVITY #1: RECEIVE COMPLAINT AND ACKNOWLEDGE RECEIPT

Table 15: The Complaint Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1	
List of the activities: *1# The complaint management process is triggered when the EU-SEC Complaint Committee receives a complaint that was either submitted in electronic form (via email or a complaint form on the EU-SEC website) or verbally.* *2# An appointed individual of the EU-SEC Complaint Committee captures the complaint in the Complaint Management System for further processing, including all relevant details of the complaint and contact data of the complainant.* *3# The Complaint Management System will automatically assign a unique identifier and send a standardised acknowledge receipt to the complainant.*	
Inputs (upstream)	**Outputs (downstream)**
1# Contact data of the complainant 2# The required information and all relevant details of the complaint	1# Documentation of the complaint in the Complaint Management System 2# Complaint Receipt for the complainant

5.2.2.2. ACTIVITY #2: ASSES VALIDITY AND SEVERITY (RELEVANCE, IMPACT AND URGENCY)

Table 16: The Complaint Management Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2	
List of the activities: *1# The EU-SEC Complaint Committee assesses the validity of the received complaint and the severity, based on the relevance (incl. frequency of occurrence), impact and urgency for EU-SEC Framework. The initial assessment is performed within 1 business day after the complaint was raised. The severity is documented in the Complaint Management System. One example severity as follows:* • *Low/Minor: Complaint to be processed within 14 days* • *Medium/Normal: Complaint to be processed within 7 days* • *High/Severe: Complaint to be processed within 5 days*	
Inputs (upstream)	**Outputs (downstream)**
1# Documentation of the complaint in the Complaint Management System	1# Documentation of the complaint in the Complaint Management System with the severity grade.

5.2.2.3. ACTIVITY #3: IDENTIFY SOLUTION FOR THE REQUEST OR COMPLAINT

Table 17: The Complaint Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: 1# *The EU-SEC Complaint Committee investigates the complaint and provides a decision or action (solution) to solve the complaint. Support is obtained from the EU-SEC Advisory Board or dedicated working groups as deemed applicable for the nature of the complaint. The level of investigation should be commensurated with the severity of the complaint.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documentation of the complaint in the Complaint Management System with the severity grade.	1# Documentation of the complaint in the Complaint Management System with the severity grade and the proposed solution.

5.2.2.4. ACTIVITY #4: ON-GOING COMMUNICATION

Table 18: The Complaint Management Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4	
List of the activities: 1# *The EU-SEC Complaint Committee maintains regular communication with the complainant including information on the progress, while the necessary assessments and solution design, development and implementation takes place. The frequency of the communication should be commensurate with the severity of the complaint. One example of frequency of communication as follows:* • *Low/Minor: every 4 days* • *Medium/Normal: every 2 days* • *High/Severe: daily*	
Inputs (upstream)	**Outputs (downstream)**
1# Documentation of the complaint in the Complaint Management System with the severity grade.	1# Actual status on the progress for the complainant.

5.2.2.5. ACTIVITY #5: COMMUNICATE SOLUTION

Table 19: The Complaint Management Process Activity #5 Card to Detailed Sub-Activities, Inputs and Outputs.

<table>
<tr><th colspan="2">Activity #5</th></tr>
<tr><td colspan="2">List of the activities:
1# As soon as a solution is identified, the EU-SEC Complaint Committee communicates the proposed solution to the complainant. If the complainant accepts the proposed solution, then the decision or action is carried out and recorded (Activity #6).

2# If the complainant rejects the proposed solution, the complaint remains open. In such cases the EU-SEC Complaint Committee informs the EU-SEC Advisory Board and initiates the identification of alternative solutions. Activities 3 to 5 are repeated as deemed appropriate in the circumstances. The EU-SEC Complaint Committee continues to monitor the progress of the complaint until all reasonable internal and external options of recourse are exhausted or the complainant is satisfied.

3# If no solution can be identified (e.g. the EU-SEC Complaint Committee revises its initial conclusion about the validity of the complaint) or can be implemented within economically justifiable borders and risks, this is communicated as well.</td></tr>
<tr><th>Inputs (upstream)</th><th>Outputs (downstream)</th></tr>
<tr><td>1# Documentation of the complaint in the Complaint Management System with the severity grade and the proposed solution.</td><td>1# If the solution can be identified:
Documented proposed solution
➔ If the solution is accepted: Execution request for the proposed solution.
➔ If the solution is rejected: Updated documentation of the complaint in the Complaint Management System.
2# If no solution can be identified:
Notification for the complainant, that no solution was able to be identified.</td></tr>
</table>

5.2.2.6. ACTIVITY #6: IMPLEMENT SOLUTION

Table 20: The Complaint Management Process Activity #6 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #6	
List of the activities: *1# After the complainant accepted the proposed solution, necessary actions are carried out as required.* *2# When a change is required to implement the proposed solution for the complaint, the EU-SEC Complaint Committee creates an RfC.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documented proposed solution	1# Execution request for the proposed solution. 2# RfC in case of a required change process.

5.2.2.7. ACTIVITY #7: CLOSE COMPLAINT

Table 21: The Complaint Management Process Activity #7 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #7	
List of the activities: *1# After the solution is implemented, the EU-SEC Complaint Committee informs the complainant by requesting to close the complaint in the Complaint Management System.* *2# If the complainant does not actively reject the request or response within 15 days, the complaint is closed automatically.* *3# If the complainant rejects the request, a rationale has to be provided and the process starts from new with Activity #2.*	
Inputs (upstream)	**Outputs (downstream)**
1# Notification, that the solution is implemented.	1# Request to close complaint for the complainant. 2# Closed complaint record in the Complaint Management System

5.3. CHANGE MANAGEMENT

Change management is the foundation of improving the EU-SEC Framework. It shall analyse the necessity of changes, and maximise the likelihood of successfully implementing changes to the framework in a controlled manner, including organisation, processes and IT systems. Change management aims to reduce risks, cover the complete life cycle of the change and all affected stakeholders.

5.3.1. GENERAL CHANGE MANAGEMENT PRINCIPLES AND REQUIREMENTS

The following principles and related requirements are derived from ISACA's guidance "COBIT® 5: Enabling Processes" which outlines goals and management practices in accordance with related standards such as ISO 20000 for IT Service Management.

Table 22: Principles and related Requirements for Change Management

PRINCIPLE	REQUIREMENT
Holistic Applicability	The change management process shall be applicable for all types of changes to EU-SEC's organisation, processes and IT systems to ensure the impact and the involvement required from each stakeholder is assessed.
Complete Coverage	The change management process shall ensure that all relevant changes are identified, assessed, approved and recorded, including the definition of fall-back procedures for aborting and recovering from unsuccessful changes and unforeseen events and covering emergency changes to enable the implementation of changes needed to resolve an incident in a quickly and controlled manner.
Responsibility & Accountability	The organisation shall ensure that responsibility and accountability for actions and decisions of the organisation with respect to change management is clearly established by the EU-SEC Advisory Board.

5.3.2. CHANGE MANAGEMENT PROCESS

The change management process is built up based on the description of the Multiparty Recognition Change Management Process. This process is extended in the EU-SEC framework view, in order to handle all the change requests regarding any components and aspects for the EU-SEC Framework.

The change management process comprises seven activities as outlined in the table below:

Table 23. The change management process card: the inputs, the activities and the outputs.

Change Management Process	
Inputs (upstream)	- Actions to be carried out as part of a solution for a complaint - Risk mitigation actions - Change proposals by EU-SEC working groups
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
Outputs (downstream)	- Result of the change assessment and corresponding updates of the framework

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 24. The Change Management Process Activities' Mapped to Roles and Responsibilities.

Change Management Process		**Activities**							
		#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**	**#8**
Roles	Change Requestor	R/A	-	I	-	I	R	I	-
	Change Assessment Task Force	-	R	C	-	-	-	-	R
	Change Implementation Team	-	-	-	-	R	-	R	C
	EU-SEC Advisory Board	-	A	A/R	A/R	A	A/R	A/R	A
	EU-SEC CEO	-	-	R	-	-	R	-	
	EU-SEC Emergency Response Team	-	-	R	-	-	-	-	C
	EU-SEC General Secretariat	R	-	R	-	-	R	-	-
	EU-SEC Working Groups	-	C	R	-	C	R	I	-
R – Responsible; **A** – Accountable, **C** – Consulted, **I** – Informed									

The change management process activities and the underlying sub-activities are described in more detail in the subsections below.

5.3.2.1. ACTIVITY #1: INITIATE CHANGE

Abstract: The change management process is triggered by recording a Request for Change.

Table 25. The Change Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1
List of the activities: 1# *The Change Requestor (e.g. member of an EU-SEC Working Group or the EU-SEC Advisory Board) initiates the change management process by creating a Request for Change (RfC) in the change management ticketing system or by submitting the request via email to the EU-SEC General Secretariat. The RfC includes the following information:* • *Summary of the change* • *Rationale for the change (e.g. expected benefit, reference to a complaint)* • *Contact information of the Change Requestor (name, organisation, email address)* 2# *If the change was submitted via email, the EU-SEC General Secretariat generates the RfC based on the information in the email. Missing information is obtained as required to perform a qualified assessment (activity #2). After the RfC is created, the Change Requestor obtains a receipt including the ID of the corresponding ticket.*

Activity #1	
Inputs (upstream)	**Outputs (downstream)**
1# Actions to be carried out as part of the solution for a complaint 2# Actions identified during post-implementation review of another change 3# Change proposals by EU-SEC working groups 4# Opened ticket from another process management	1# RfC in status "submitted" in the change management ticketing system

5.3.2.2. ACTIVITY #2: ASSESS THE IMPACT

Abstract: The impact and associated risk of the change is assessed and the change classified and prioritised accordingly.

Table 26. The Change Management Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2
List of the activities: 1# *The Change Assessment Task Force of the EU-SEC Advisory Board determines the scope of the envisioned change by identifying the components of the EU-SEC Framework (organisation, processes and IT systems), the various stakeholders who are affected and their required involvement. The EU-SEC Advisory Board consults subject matter experts of these stakeholders (e.g. working group members) as required for a qualified impact assessment.* 2# *If the Change Assessment Task Force considers the RfC as appropriate and in line with EU-SEC's proclaimed ambition, actions for suitable information and communication are identified that motivate and inspire stakeholders to desire and authorise the change. Otherwise, the EU-SEC Advisory Board prepares information to convince the identified stakeholders that they should not authorise it for further design, development, acquisition or configuration (Activity #3).* 3# *The Change Assessment Task Force assesses the risk associated with the change, based on:* • *The current readiness and ability of the affected components (identified in Activity #1 to adopt the change);* • *The impact on these components;* • *The likelihood of adversely affecting any of these components by implementing the change;* • *Security, legal, contractual and compliance implications associated with the change;* • *Inter-dependencies amongst other changes;*

Activity #2	
• *The possibility of fall-back procedures for aborting and recovering from unsuccessful change implementations and unforeseen events.* 4# *Based on the risk assessment, the Change Assessment Task Force categorises the RfC either as Minor, Regular, Major, or Emergency Change in accordance with the following definitions:* • *Minor: A change with limited impact on components of the EU-SEC Framework, a clear extent of actions for design, development, acquisition or configuration and with a low likelihood (< 33%) of adverse effects;* • *Major: A change with significant impact on components of the EU-SEC Framework, a significant extent of actions for design, development, acquisition or configuration or with a high likelihood (> 66%) of adverse effects;* • *Emergency: A change that must be implemented as soon as possible, for example, to prevent or resolve a major incident or implement a security patch for an extremely critical vulnerability;* • *Regular: A change that is not a Minor, Major or Emergency Change (e.g. change with limited impact, but a medium likelihood of adverse effects).* 5# *Based on the organisational and technical implications to implement the change, the resources required and the applicable legal, contractual and compliance requirements, the Change Assessment Task Force prioritises the RfC in accordance with the following definitions:* • *Low: for non-urgent changes to be implemented within 6 months after authorisation;* • *Medium: for changes with normal urgency to be implemented within 3 months after authorisation;* • *High: for urgent changes to be implemented within 4 weeks after authorisation;* • *Critical: for very urgent Emergency Changes to be implemented immediately.*	
Inputs (upstream)	**Outputs (downstream)**
1# RfC in status "submitted" in the change management ticketing system	1# RfC in status "assessed" in the change management ticketing system

5.3.2.3. ACTIVITY #3: AUTHORISE CHANGE REQUEST

Abstract: The change is authorised prior to further design, development, acquisition or configuration.

Table 27. The Change Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: *1# The EU-SEC Advisory Board* reviews the change categorisation by the Change Assessment Task Force (activity #2) and proposes the change for authorisation to initiate further actions for design, development, acquisition or configuration or non-authorisation.* *2# If the change categorisation is considered to be not appropriate, the EU-SEC Advisory Board consults the Change Assessment Task Force and applies changes as appropriate to ensure a change authorisation that is commensurate with the impact and risk of the change.* *3# The EU-SEC General Secretariat obtains the authorisation in accordance with the change categorisation.* • *Minor change: EU-SEC Advisory Board** • *Regular change: EU-SEC Advisory Board* + Working Groups responsible for the components affected by the change* • *Major change: EU-SEC Advisory Board* + Working Groups responsible for the components affected by the change + EU-SEC CEO* • *Emergency change: EU-SEC Emergency Response Team.* *4# If the authorisation is refused, the rationale for the decision is recorded with the RfC and the EU-SEC Advisory Board informs the Change Requestor accordingly via appropriate communication channels (e.g. email).* ** Segregation of duties must be maintained to ensure an effective change authorisation:* • *The change requestor must not be involved in the authorisation.* • *Those members of the EU-SEC Advisory Board, which participated in the Change Assessment Task Force that executed activity #2 must not be involved in taking decisions about the change categorisation and the authorisation (only for consultation).*	
Inputs (upstream)	**Outputs (downstream)**
1# RfC in status "assessed" in the change management ticketing system	1# RfC in status "authorised" or "rejected" in the change management ticketing system

5.3.2.4. ACTIVITY #4: PLAN AND SCHEDULE CHANGE

Abstract: A team and necessary actions for change design, development, acquisition or configuration are planned and scheduled.

Table 28. The Change Management Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4	
List of the activities: 1# *After the RfC is authorised, the EU-SEC Advisory Board assembles an effective Change Implementation Team that includes appropriate members from the working groups affected by the change with the capacity to spend the required amount of time and contribute knowledge and expertise, experience, credibility and authority. External parties are considered as considered appropriate to provide an independent view or to address skill gaps.* 2# *For changes that affect stakeholder's responsibilities, the EU-SEC Advisory Board develops a change communication plan to communicate such changes in a timely manner. The communication plan considers the stakeholders' behavioural profiles, their information requirements and communication channels. This may involve the Chair of the EU-SEC General Assembly and the EU-SEC CEO to support the communication of the desired vision for the change.* 3# *The EU-SEC Advisory Board identifies required training needed to develop the appropriate skills of those for the design, development, acquisition or configuration of the change and of those affected by it.* 4# *The EU-SEC Advisory Board schedules the implementation date based on the prioritisation of the RfC and the availability of resources in the Change Implementation Team.*	
Inputs (upstream)	**Outputs (downstream)**
1# RfC in status "authorised" or "rejected" in the change management ticketing system	1# RfC in status "planned" in the change management ticketing system 2# Change communication plan

5.3.2.5. ACTIVITY #5: EXECUTE CHANGE

Abstract: The actions planned for design, development acquisition or configuration of the change are executed.

Table 29. The Change Management Process Activity #5 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #5	
List of the activities: *The Change Implementation Team executes the necessary actions for design, development acquisition or configuration of the change. Depending on the components of the EU-SEC Framework affected by the change (organisation, processes or IT systems), specific activities are performed:* a) For changes to the organisation or processes: *1# The Change Implementation Team develops a plan for operation and use of the change. This includes the identification and leveraging of quick wins, the definition of milestones and associated deliverables, need for documentation (e.g. procedures), mentoring, training coaching and knowledge transfer and the definition of acceptance criteria and indicators to monitor success.* *2# The Change Implementation Team executes the plans for communication (as defined in activity #4) and for operation and use. The indicators for success are monitored (e.g. how people feel about the change) to initiate remedial actions as appropriate.* *3# The Change Implementation Team reviews the deliverables to meet the acceptance criteria and promotes them for go-live/operational use/publication.* b) For changes to IT systems: *1# The Change Implementation Team establishes separate environments for development, test and production and implements appropriate access controls to ensure that only authorised personnel can migrate changes between environments. Data in the test environment is representative of the production and sanitised as required to comply with applicable regulatory requirements. Developers do not have access to production.* *2# The Change Implementation Team creates an implementation* *3# Members of the Change Implementation Team independent from development design appropriate test plans for all relevant functional and technical requirements (e.g. unit, integration, regression, performance, security, and user acceptance testing), including clear criteria for measuring the success.* *4# Test plans are approved prior execution by relevant stakeholders.* *5# Test plans are executed by appropriate personnel, which maintains records about the test execution and results. Identified errors are logged and analysed by the Change Implementation Team. Errors are remediated or formally accepted, the decision is documented by the Change Implementation Team.* *6# The Change Implementation Team specifies fall-back and recovery procedures.* *7# The Change Implementation Team initiates actions to update relevant documentations.* *8# When testing is finished, relevant errors are remediated or accepted and relevant documentation is appropriately updated, the Change Implementation Team promotes the change (and associated deliverables) for implementation in production.*	
Inputs (upstream)	**Outputs (downstream)**

Activity #5	
1# RfC in status "planned" in the change management ticketing system 2# Change communication plan	1# RfC in status "executed" in the change management ticketing system 2# Operation and use plan 3# Implementation plan 4# Test plans 5# Test execution records 6# Deliverables as applicable for the change (e.g. source code, documentation, deployment packages)

5.3.2.6. ACTIVITY #6: APPROVE CHANGE

Abstract: Deliverables promoted for production or release are approved.

Table 30. The Change Management Process Activity #6 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #6	
List of the activities: *1# After the Change Implementation Team promoted the deliverables for production or release, the EU-SEC General Secretariat obtains the approval in accordance with the change categorisation.* • *Minor change: EU-SEC Advisory Board* + Change Requestor* • *Regular change: EU-SEC Advisory Board* + Change Requestor + Working Groups responsible for the components affected by the change* • *Major change: EU-SEC Advisory Board* + Change Requestor + Working Groups responsible for the components affected by the change + EU-SEC CEO* • *Emergency change: No approval is required at this point in the process as necessary actions shall be initiated immediately. Post-implementation reviews are conduced to review whether the change categorisation was appropriate in the circumstances and to minimise the likelihood of re-occurrence by initiating corrective actions based on a root cause analysis (activity #8).* *2# The EU-SEC Advisory Board reviews the execution of the communication plan to ensure that all relevant stakeholders affected by the change received appropriate information. If communication is required prior implementation, actions are initiated to ensure the communication is provided in a timely manner.* ** Segregation of duties must be maintained to ensure an effective change approval:* *Those members of the EU-SEC Advisory Board, which participated in the Change Implementation Team that executed activity #5 must not be involved in the approval.*	
Inputs (upstream)	**Outputs (downstream)**
1# RfC in status "executed" in the change management ticketing system 2# Operation and use plan 3# Implementation plan 4# Test plans 5# Test execution records 6# Deliverables as applicable for the change (e.g. source code, documentation, deployment packages)	1# RfC in status "approved" in the change management ticketing system

5.3.2.7. ACTIVITY #7: IMPLEMENT CHANGE

Abstract: The change is implemented.

Table 31. The Change Management Process Activity #7 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #7	
List of the activities: *1# The EU-SEC Advisory Board continues the execution of the communication plan to ensure that all relevant stakeholders affected by the change received appropriate information.* a) For changes to the organisation or processes: *2# The Change Implementation Team executes remaining actions of the operation and use plan to complete the implementation (e.g. go-live of processes, release of updated documents.)* b) For changes to IT systems: *2# The Change Implementation Team executes the implementation plan to implement the change (e.g. deployment in production.)*	
Inputs (upstream)	**Outputs (downstream)**
1# Operation and use plan 2# Implementation plan 3# Deliverables as applicable for the change (e.g. source code, documentation, deployment packages)	1# RfC in status "implemented" in the change management ticketing system

5.3.2.8. ACTIVITY #8: PERFORM POST-IMPLEMENTATION REVIEW

Abstract: A post-implementation is performed to confirm outcomes and results, identify lessons learned, and develop an action plan.

Table 32. The Change Management Process Activity #8 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #8	
List of the activities: 1# *The Change Assessment Task Force of the EU-SEC Advisory Board reviews each change categorised as Major Change and Emergency Change and selected changes categorised as Routine Change to determine whether* • *Expected benefits have been realised,* • *Stakeholder expectations are met,* • *Unexpected events have occurred that may have been caused by the change,* • *The change management process was performed effectively and efficiently* 2# *If the change under review was categorised as emergency change, the Change Assessment Task Force of the EU-SEC Advisory Board reviews the rationale for the change in the RfC to determine whether the change categorisation was appropriate in the circumstances, and performs a root cause analysis to minimise the likelihood of re-occurrence by initiating corrective actions.* 3# *The Change Assessment Task Force of the EU-SEC Advisory Board creates an action plan for identified issues to prevent their re-occurrence in future changes. The action plan is provided to the EU-SEC Advisory Board for review and approval. For actions that require changes, the change management process is initiated.*	
Inputs (upstream)	**Outputs (downstream)**
1# Records and deliverables as applicable for the change under review	1# Action plan

5.4. RESOURCE MANAGEMENT

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.

The EU-SEC Framework contains the following resources:

- Personnel resources: They depend on the EU-SEC governance body organisation structure.
- IT relevant resources: They are the IT resources needed to support the execution, operation and governance of the EU-SEC Framework, e.g. to support the EU-SEC Security Requirements Repository, or to support the continuous auditing for EU-SEC Toolchain and Evidence Management Architecture.
- Financial resources: They support the achievement of personnel and IT relevant resource, which indirectly ensures the operation of the EU-SEC Framework.

Due to the fact that the EU-SEC Governance Body Organisation and its business model are still under discussion, the resource assumption will be addressed in the final version of EU-SEC Framework in D2.5. In this deliverable, we define the principles and requirements for the resource management and the activities within this process.

5.4.1. GENERAL RESOURCE MANAGEMENT PRINCIPLES AND REQUIREMENTS

The following principles and related requirements are outlined as the principles and requirements of the resource management.

Table 33: Principles and related Requirements for Resource Management

PRINCIPLE	REQUIREMENT
Quantifiable	The resource in use and in planning shall be quantifiable to support on understanding of the current state and the needs in further.
Forecast	The resource consumption status and the needs of the resource must be evaluated, and resource forecast shall be made on regular basis from different levels, IT resource, human resource, financial resource, to ensure the new resource adoption on timely manners.

PRINCIPLE	REQUIREMENT
Communication	The information of resource consumption status and needs must be collected from responsible parties to support the decision making.
Up-to-date	The information of resource consumption status and the needs collected must be up-to-data to support the decision making.

5.4.2. RESOURCE MANAGEMENT PROCESS

The resource management process comprises four activities as outlined in the table below:

Table 34: The resource management process card: the inputs, the activities and the outputs

Resource Management Process	
Inputs (upstream)	- Request/requirements from Multiparty Recognition Framework - Request/requirements from Continuous Auditing Scheme - Request from Change Management (Activity #4) - Request from Complaint Management - Requirements from financial management - Current and future demands of resources
Activities	1. Assess availability, performance and capacity 2. Assess EU-SEC business impact 3. Monitor availability, performance and capacity 4. Investigate and address availability, performance and capacity issues
Outputs (downstream)	- Resource, performance and capacity plan - EU-SEC business impact scenarios - Availability, performance and capacity reports - Discrepancy report

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 35: The resource management process activities' mapped to roles and responsibilities

Resource Management Process		**Activities**			
		#1	**#2**	**#3**	**#4**
Roles	Head of Resource Management	R	R	R	R
	Working Group - Continuous Auditing Certification	C	C	C	C
	Working Group - Multiparty Recognition Analysis	C	C	C	C
	Head of other processes	-	C	-	C
	EU-SEC Advisory Board	A	A	A/I	A
	EU-SEC CFO	R	-	C	C
R – Responsible; **A** – Accountable, **C** – Consulted, **I** – Informed					

The resource management process activities and the underlying sub-activities are described in more detail in the subsections below.

5.4.2.1. ACTIVITY #1: ASSESS AVAILABILITY, PERFORMANCE AND CAPACITY

Abstract: The resource management process is triggered by requests and requirements of the stakeholders.

Table 36: The Resource Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1
List of the activities: *1# Consider requirements from the stakeholders. Requirements could be:* • *Adjustment of resources* • *Adjustment of peak seasons for further planning* • *Investigation support for complaints* *2# Create the following plans:* • *Availability Plan – shows up the required resources to ensure the required availability* • *Performance Plan – shows up the required resources to ensure the required performance* • *Capacity Plan – shows up the required resources to ensure the required capacity* 3# *Send plans for approval to EU-SEC Advisory board*

Activity #1	
Inputs (upstream)	**Outputs (downstream)**
1# Request/requirements from Multiparty Recognition Framework 2# Request/requirements from Continuous Auditing Scheme 3# Request from Complaint Management 4# Request from Change Management 5# Future resource invest plan (Activity #4)	1# Availability, performance and capacity plan 2# Request for approval

5.4.2.2. ACTIVITY #2: ASSESS EU-SEC BUSINESS IMPACT

Abstract: Ensures that the impact of unavailable resources is familiar to relevant stakeholders.

Table 37: The Resource Management Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2	
List of the activities: *1# Identify critical processes that endanger the availability, performance and/or capacity* *2# Map identified processes to dependent application and infrastructure* *3# Create risk scenarios based on the identified data* *4# Determine the impact of the scenarios* *5# Ensure that the head of other processes fully understand and agree to the results of this analysis and request feedback to reduce risk of unacceptable risk scenarios*	
Inputs (upstream)	**Outputs (downstream)**
1# Requirements from Multiparty Recognition Framework 2# Requirements from Continuous Auditing Scheme 3# Availability patters 4# Logs of past failures 5# Monitoring data	1# EU-SEC business impact scenarios 2# Request for feedback of unacceptable risk scenarios

5.4.2.3. ACTIVITY #3: MONITOR AVAILABILITY, PERFORMANCE AND CAPACITY

Abstract: Monitor availability, performance and capacity and provide reports.

Table 38: The Resource Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: *1# Monitor relevant resources* *2# Provide regular reports for financial management and EU-SEC Advisory Board*	
Inputs (upstream)	**Outputs (downstream)**
1# Requirements from multiparty recognition framework 2# Requirements from continuous auditing scheme 3# Reports and alerts from monitoring tools for IT resources 4# Data from personnel workload reports created by process owners	1# Availability report 2# Performance report 3# Capacity report

5.4.2.4. ACTIVITY #4: INVESTIGATE AND ADDRESS AVAILABILITY, PERFORMANCE AND CAPACITY ISSUES

Abstract: Identify discrepancies between pre-defined plans and monitoring reports.

Table 39: The Resource Management Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4
List of the activities: *1# Identify discrepancies from pre-defined plans* *2# Provide regular reports for financial management and EU-SEC Advisory Board* *3# Define corrective actions for change management* *4# Define an escalation procedure in case of emergency problems*

Activity #4	
5# *Create future resource invest plan* 6# *Send plan for approval to EU-Sec Advisory board*	
Inputs (upstream)	**Outputs (downstream)**
1# Availability, performance and capacity plan 2# Availability, performance and capacity report	1# Discrepancy report 2# Corrective actions 3# Emergency procedure 4# Future resource invest plan 5# Request for approval

5.5. MONITORING AND MEASUREMENTS

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.

5.5.1. GENERAL MONITORING AND MEASUREMENTS PRINCIPLES AND REQUIREMENTS

The following principles and related requirements are derived from ISO/IEC 27001:2013, which outlines the requirements of monitoring, measurements, analysis and evaluation.

Table 40: Principles and related Requirements for Monitoring and Measurements

PRINCIPLE	REQUIREMENT
Object	The monitoring and measurements process shall define what needs to be monitored, including processes, policies and procedures, etc.
Frequency	The frequency of the monitoring shall be defined, e.g. continuously, daily, weekly, monthly, yearly or ad-hoc, etc. With a clear frequency, the monitoring can be executed as planned and achieve the best performance to detect and identify problems.
Responsibility & Accountability	The organisation shall ensure that responsibility and accountability for actions with respect to monitoring and measurement is clearly established.
Measurable	The methods for monitoring, measurement, analysis and evaluation are determined in a measurable way to ensure valid results.
Comparable	The monitoring results are comparable to the goals through analysis, and the monitoring activity can be concluded with the effectiveness of the monitored objects and measures.

5.5.2. MONITORING AND MEASUREMENTS PROCESS

The monitoring and measurements process comprises five activities as outlined in the table below:

Table 41: The monitoring and measurements process card: the inputs, the activities and the outputs

Monitoring and Measurements Process	
Inputs (upstream)	- Internal and External Requirements - Goals from EU-SEC Advisory Board - Goals from Process Owners/stakeholders - Policies and procedures
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
Outputs (downstream)	- Deviations Reports - Effectiveness Reports

The responsibilities and mapping in accordance with the framework's template, are presented in the table below.

Table 42: The monitoring and measurements process activities' mapped to roles and responsibilities.

Monitoring and Measurements Process		**Activities**				
		#1	**#2**	**#3**	**#4**	**#5**
Roles	Head of Resource Management	C	-	-	I	C
	EU-SEC Advisory Board	A/C	A	A	A	A/C
	Head of Change Management	C	-	-	I	C
	Head of Complaint Management	C	-	-	I	C
	Head of Policy and Role Management	C	-	-	I	C
	Head of Monitoring and Measurements	R	R	R	R	R
R – Responsible; **A** – Accountable, **C** – Consulted, **I** – Informed						

The monitoring and measurements process activities and the underlying sub-activities are described in more detail in the subsections below.

5.5.2.1. ACTIVITY #1: DEFINE THE MONITORING KPIS AND MEASUREMENTS

Table 43: The Monitoring and Measurement Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1	
List of the activities: *1# Collect & Identify goals with EU-SEC Advisory Board and Process Owners.* *2# Define important aspects and monitoring KPIs. The following features should be considered, when defining a KPI:* • *Title of the monitoring KPI/measurement;* • *Description what will be measured;* • *Scope/Applicable Area where the measurement will be implemented;* • *Purpose to describe why the measurement is necessary;* • *Measurement Executor as the responsible person, who will perform the monitoring and measuring;* • *Measurement Method (logical sequence of operations to measure certain indicators);* • *Frequency to define when and how often the measurement will be performed;* • *Indicators with details on the monitored attributes with respect to a specified scale.* *3# Validate periodically the goals and identify new or changed stakeholders* *4# Validate periodically the monitoring KPIs catalogue*	
Inputs (upstream)	**Outputs (downstream)**
1# Goals from policy and role management 2# Goals from complaint management 3# Goals from change management 4# Goals from resource management 5# Goals from EU-Sec advisory board 6# Policies and procedures 7# Internal and external requirements	1# List of important aspects 2# Monitoring KPIs catalogue

5.5.2.2. ACTIVITY #2: PERFORM KPIS MONITORING AND MEASUREMENTS WITH DEFINED FREQUENCY

Table 44: The Monitoring and Measurement Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2	
List of the activities: *1# Implement KPIs monitoring and measurements* *2# Collect monitoring results from monitoring executor or reports from stakeholders* *3# Consolidate results or stakeholder reports* *4# Create monitoring result*	
Inputs (upstream)	**Outputs (downstream)**
1# Monitoring KPI's 2# List of important aspects 3# Stakeholder reports	1# Monitoring result

5.5.2.3. ACTIVITY #3: COMPARE THE MONITORING RESULTS WITH THE EXPECTATION AND IDENTIFY THE DEVIATIONS

Table 45: The Monitoring and Measurement Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: *1# Compare predefined goals with monitoring results* *2# Evaluate effectiveness of monitoring KPIs* *3# Create deviation report that may indicate deficiencies in policies, processes and procedures*	
Inputs (upstream)	**Outputs (downstream)**
1# List of important aspects 2# Monitoring KPIs 3# Monitoring result	1# Deviation report 2# Effectiveness report

5.5.2.4. ACTIVITY #4: REPORT MONITORING DEVIATIONS

Table 46: The Monitoring and Measurement Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4	
List of the activities: *1# Report deviation report to EU-SEC Advisory Board and Process Owners* *2# Report effectiveness report to EU-SEC Advisory Board and Process Owners*	
Inputs (upstream)	**Outputs (downstream)**
1# Deviation report 2# Effectiveness report	1# Deviation report 2# Effectiveness report

5.5.2.5. ACTIVITY #5: FOLLOW UP ON DEVIATIONS

Table 47: The Monitoring and Measurement Process Activity #5 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #5	
List of the activities: *1# Perform follow-up session with stakeholders on deviation report* *2# Identify workarounds together* *3# Create measures together to achieve goals* *4# Report necessary measures to change management*	
Inputs (upstream)	**Outputs (downstream)**
1# Deviation report 2# Stakeholder goals	1# Workarounds for stakeholder 2# Measures for stakeholder 3# Opened ticket for Change Management (if necessary)

6. CONCLUSIONS AND RECOMMENDATIONS

The outcome of this work is the initial EU-SEC Framework, which contains three main components (the Multiparty Recognition Framework, Continuous Auditing Certification Scheme and Privacy Code of Conduct) and the EU-SEC Repository, Governance Body Organisation Structure suggestion, as well as the governance model with five main governance processes to support the efficient and effective operation, and continuous improvement of the framework.

The main goals and achievements of this work are:

- The EU-SEC Framework's structure, which brings the outcomes of Deliverables D2.1, D2.2 and D2.3 into one harmonised framework and build up the structure which could be realised and implemented after the EU-SEC Project has finished.
- The EU-SEC Governance Body Organisation, which could provide a good guidance for the further EU-SEC Organisation.
- The EU-SEC Framework's governance model with five governance processes, which could demonstrate the first version of the EU-SEC Framework's governance structure and governance activities. This could provide the baseline for the future implementation of the governance model around the EU-SEC Framework's components.

Along with the above mentioned achievements, we would like to outline the improvement possibilities in the continuation of the EU-SEC project.

The EU-SEC Framework described in this deliverable does not provide the final stage of the framework, since the EU-SEC Project is still on-going. It brings the first version of how the framework could look like, so that the EU-SEC Project would achieve the goals defined at the first place. With further development and process of the EU-SEC Project, the EU-SEC governance body organisation needs to be defined, based on the options described in section 4.1, and the further discussion among the EU-SEC consortium. The EU-SEC Framework should be adjusted according to reality to meet the stakeholders' needs, and details could be modified and added to utilise the EU-SEC Framework. The outcomes and feedbacks through the execution of work package 3 "Tools and architectures", work package 4 "Pilot 1 – Multiparty recognition scheme", as well as work package 5 "Pilot 2 – Continuous Monitoring/Auditing based certification".

The final version of EU-SEC Framework will be published in another deliverable D2.5 "EU-SEC Framework – Final Version" at the last stage of the EU-SEC Project.