EUSEC
EU SECURITY CERTIFICATION

European Security Certification Framework

EU-SEC Framework Final Version

V 1.0

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE:	DELIVERY DATE:
30.06.2019	30.09.2019
AUTHOR:	PARTNERS CONTRIBUTED:
CSA	
DISSEMINATION LEVEL:	NATURE OF THE DELIVERABLE:
PU	R
INTERNAL REVIEWERS:	
Fabasoft, NIXU	

*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 increasingly codifies security assurance, governance and compliance requirements applicable to information systems. In this context, Cloud Service Providers (CSPs) are under renewed pressure to comply with several international and national requirements as well as sector specific regulations. To this end, the market seems to show signs of confusion, fatigue, inefficiency and finally lack of effectiveness. In addition to the requirements burden, the certification schemes' auditing process validating compliance still lacks harmonized and transparent processes and is still substantially manual.

As solution to the aforementioned issues, the EU-SEC consortium aims to develop a framework that combines and integrates under one common infrastructure the models of multiparty recognition between existing cloud security schemes, continuous auditing-based certification and finally privacy-based certification. This framework will provide business and 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 work carried out by the EU-SEC consortium is meant to be an input to the EC and ENISA within the context of the implementation of the EU Cybersecurity Act[1] and in particular for the creation of a Cloud Computing Cybersecurity Certification Framework. This EU-SEC Framework is fully aligned with the recommendation of the of the expert group established by the European Commission, the CSPCert[2].

The main sources for this deliverable are the D2.1: Multiparty Recognition Framework (MPRF), D2.2: Continuous Auditing-based Certification (CABC) Scheme and D2.3: Privacy Code of Conduct (CoC), 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 management, sustainability and extension requirements.

The aforementioned results determine the structure, roles, responsibilities and the processes and activities that will be carried out during the execution of the framework.

1 https://eur-lex.europa.eu/eli/reg/2019/881/oj
2 https://cspcerteurope.blogspot.com/

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
CSA OCF	Cloud Security Alliance Open Certification Framework
D1.2	EU-SEC deliverable of task 1.1 "D1.2 – Security and Privacy Requirements and Controls"
D1.3	EU-SEC deliverable of task 1.2 "Auditing and assessment requirements"
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"
D2.1	EU-SEC deliverable of tasks 2.1 "Multiparty recognition framework for cloud security certifications"
D2.2	EU-SEC deliverable of tasks 2.2 "Continuous auditing certification scheme"
D2.3	EU-SEC deliverable of tasks 2.3 "Privacy code of conduct"
D2.4	EU-SEC deliverable of tasks 2.4 "EU-SEC Framework – First Version"
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"
D3.2	EU-SEC deliverable of tasks 3.2 "Architecture and Tools for Auditing"
D3.3	EU-SEC deliverable of tasks 3.3 "Architecture and Tools for Evidence Storage"
D4.5	Consolidation and analysis report – the MPRF pilot results
D5.3	Requirements and validation criteria report – CABC pilot results
EU	European Union

Abbreviation	Description
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 EU-SEC project addresses 3 major issues in cyber-security today.

The first issue addressed in the project is the multiplication of certification requirements that apply to cloud service provider, due to a rapidly changing legal and regulatory landscape. Cloud Service Providers (CSPs) are under considerable pressure to comply with several competing certification schemes, each representing distinct international and national requirements as well as sector specific regulations. At first sight, these numerous certification schemes seem to be particularly heterogeneous, as they are targeting specific application or geographic areas (e.g., national, sectorial, regulatory domains and requirements). Fortunately, cloud-based certification schemes are based on worldwide accepted and widely used standards (e.g., ISO 27000 series of standards). Hence, these competing certification schemes share many commonalities in terms of security domains and requirements. The EU-SEC project conducted a security requirements gap analysis, which shows that security requirements are largely the same across various certifications schemes – 71% of requirements are equivalent, 16% show a partial gap and only 13% present a full gap (for a detailed analysis, see D1.2 – Security and Privacy Requirements and Controls report). Based on these findings, the EU-SEC project created a multi-party recognition framework that aims to exploit these commonalities in order to reduce inefficiencies and favour effective compliance across multiple certification schemes.

The second issue addressed in the project is the inadequate assurance level provided by traditional "point-in-time" certification for potential cloud customers in highly sensitive domains (e.g. finance or healthcare). These customers cannot rely alone on an audit that is performed once or twice a year, and need more continuous visibility on the security of an information system. To this end, the EU-SEC project has developed Continuous audit-based certification (CaC): a new paradigm in cloud assurance whereby instead of certifying a cloud service based on a point-in-time audit[3], we scrutinize it continuously by running regular tests to obtain an uninterrupted level of assurance. As detailed in Deliverable D2.1, this requires us to translate typical high-level control objectives, as defined in [ISO 27002] or CSA [CCM], into Service Level Objectives (SLOs) or Service Quality Objectives (SQOs), which can be regularly validated by automated tools or humans, following concrete and unambiguous metrics. Each

[3] Or "period-in-time" audit.

SLO or SQO that is applicable to a cloud service needs to be evaluated periodically, according to a predefined frequency, with an emphasis on automation wherever possible.

The third issue addressed in the project is the increased need for clear assurance from CSPs when it comes to data protection compliance. Data controllers and processors are accountable for determining and implementing appropriate levels of protection for the personal data they process in their organisations. The EU-SEC project supports the creation of an agreement or a Code of Conduct that can provide 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 guidance to comply with European Union General Data Protection Regulation (EU-GDPR).

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,
- enhancing trustworthiness and transparency in the ICT supply chain through business cases developed and piloted by the industrial partners,
- providing to ENISA and the European Commission with working framework to use as a foundation to build the cloud computing European Cybersecurity Certification Framework in line with the requirements of the EU Cybersecurity Act,
- offer fundamental components for the creation of a Code of Conduct and a Certification pursuant Art. 40 and of the GDPR.

1.1. SCOPE AND OBJECTIVES

This document is an upgrade of the work presented previously in deliverable D2.4 It aims to provide 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.

Since the previous version, essential feedback from the pilot exercises of the project, namely, deliverables D4.5: Consolidation and analysis report – the MPRF pilot results and D5.3:

Requirements and validation criteria report – CABC pilot results, has been considered and used for building a new improved governance structure.

Furthermore, recent developments for the establishment of an EU-wide cybersecurity certification framework under the umbrella of the European Cybersecurity Act, have triggered new ideas that are also reflected in the new organizational structure of the framework's governance.

As such, this deliverable presents a new governance structure where CSA and its working groups play a more substantial role in the governance, management and standardisation of the framework's activities. This structure is supported by cloud certification stakeholders (e.g., EU regulators, agencies, standard owners) with defined roles and responsibilities that aim to ensure proper guidance and validation of the activities and their outputs.

The change log summarizing changes introduced since D2.4 can be found in Annex A.

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

- To redefine the EU-SEC Framework's governance model throughout the specification of its underlying components, processes and the interrelationships between them based on the lessons learnt and provided feedback from the pilot exercises (D4.5 and D5.3).
- To redefine and align the EU-SEC Framework's governance structure with the recommendations of the CSPCert expert group in the context of the implementation of EU cybersecurity act.
- To integrate into EU-SEC governance, CSA's know-how and best practices on cloud security research and standardisation per each of the key components of the framework: MPRF, CABC and privacy CoC.

The EU-SEC Framework described in the this document contains the following components:

- A reference EU-SEC Framework's architecture and its respective set of tools
- A holistic governance structure built on the governance requirements from the respective D2.1, D2.2, D2.3, D4.5 and D5.3, 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. APPROACH

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

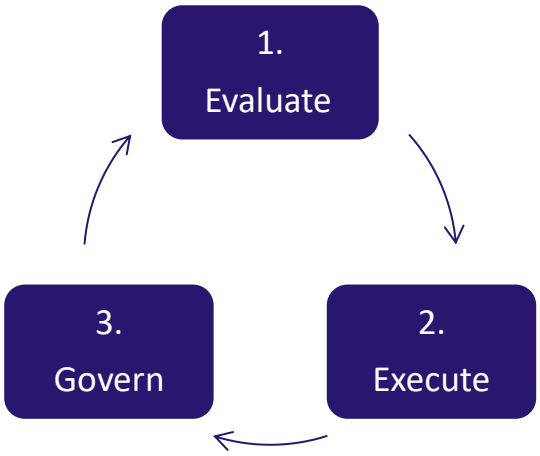

Figure 1: Lifecycle Process

The development of the EU-SEC Framework follows a bottom-up approach. It is composed of three main parts: MPRF (D2.1), CABC (D2.2) and CoC (D2.3) with a unified overarching governance structure. 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.

The EU-SEC Framework defines a governance body with roles and responsibilities to support the maintenance and operation of the framework. The governance model includes a set of processes and activities, which are meant to guide the operation, management, maintenance of the EU-SEC Framework and ensure its efficiency and effectiveness of.

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 model 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 and analyses the pros and cons to provide guidance for future decision-making. Key roles and 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. The processes enable an efficient and effective operation of the framework to handle and integrate the needs from stakeholders and changes in the compliance landscape.

Lastly, Chapter 6 concludes this work, describes the limitations and potential improvement opportunities for the framework's extension and enhancement.

2. EU-SEC FRAMEWORK OVERVIEW

This section introduced the EU-SEC Framework's overall structure. 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 (section 4.2). In order to process their requests 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 for its execution and the other one its governance.

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

- Multiparty Recognition Framework (MPRF)
- Continuous Auditing Certification Scheme (CABC)
- Privacy Code of Conduct (CoC)

Figure 2 shows the framework's 3-step lifecycle, covering the three main components mentioned above:

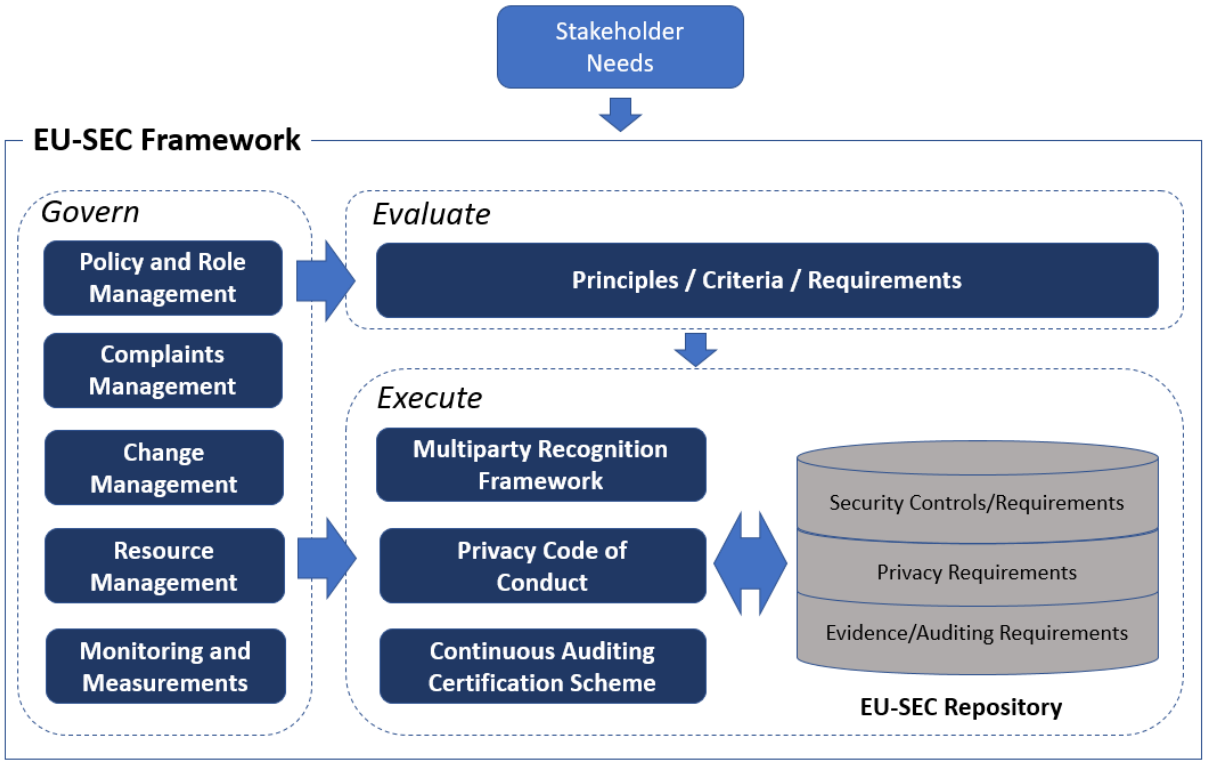

Figure 2: EU-SEC Framework

We detail these three main lifecycle steps in the following sections (2.2, 0 and 2.4).

2.2. EVALUATE STEP

Each component in EU-SEC Framework was built following a set of criteria, principle and requirements.

The criteria, principles and requirements for a Multiparty Recognition Framework and the Continuous Auditing Based Certification have been already defined in D1.4 and are briefly summarized here.

For the Multiparty Recognition Framework, five key domains are used compare security certification schemes:

- Security Requirements
- Audit Mechanisms
- Evidence Collection and Suitability
- Auditors Qualifications
- Governance Models.

EU-SEC identified four core principles that are necessary to conduct any form of assessment in order to support certification:

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

By analysing the application of these four principles in the five key domains above, we created a set of 31 requirements applicable to the Multiparty Recognition Framework. These 5 key domains, 4 core principles and 31 requirements form the criteria, principles and requirements that are used to evaluate whether a new certification scheme can be added in the multiparty recognition process.

In the case of Continuous Auditing-based Certification the same aforementioned four core principles defined for the Multiparty Recognition Framework apply. However, the requirements are instead structured in three different requirement domains: Continuous Auditing-Based Certification Base Requirements (13 requirements), Automatable Auditing Requirements (8 requirements) and Non-Automatable Auditing Requirements (7 requirements). These four principles and 28 requirements provide the basis for the evaluation a continuous auditing certification scheme.

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 GDPR requirements and transparency. As such, the main criteria for the definition of requirements in the CoC is the GDPR itself, associated with legal commentary provided in the past by the Article 29 working party and today by the European Data Protection Board (see Article 64 of the GDPR).

2.3. EXECUTE STEP

The execution step encompasses the processes for the Multiparty Recognition Framework (see D2.1, section 3.2), Continuous Auditing-based Certification (see D2.2, section 3), and the Privacy Code of Conduct (see D2.3, section 3.3).

In this section we revisit the essential tools/parts for each of the main components of the EU-SEC project:

- EU-SEC security requirements repository (for Multiparty Recognition Framework),
- EU-SEC evidence and 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-based Certification 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.

2.3.1. MULTIPARTY RECOGNITION FRAMEWORK

As already mentioned in this document, the goal of the MPRF is to create a framework, under which existing certifications and assurance schemes can co-exist. Multiparty recognition will enable a CSP that has already a cloud security certification or attestation to acquire an additional one by proving compliance only to the "delta" of security requirements between the existing and the new certification (i.e., the difference between the requirements of certification A and certification B). The expected benefits for the CSP as well as for the other relevant stakeholders (customers, auditors, etc) 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 deduced after performing a gap analysis between them (see D1.2 and D1.4). Such a comparative analysis 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.

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:

1) Security controls/requirements comparison;
2) Auditor qualification comparison;

3) Certification audit mechanism comparison;
4) Evidence suitability comparison;
5) Governance comparison.

2.3.2. CONTINUOUS AUDITING-BASED CERTIFICATION

Continuous auditing introduces an enhancement of a traditional "point-in-time" certification by increasing the assessment frequency via automation and the continuous workflow. In this approach, first, security control objectives need to be translated into a set of quantifiable or qualifiable security attributes and objectives (SLOs & SQOs), and second, evidence that these objectives are fulfilled needs to be continuously provided.

The key to a successful continuous auditing setup is this translation of controls into quantifiable or qualifiable attributes and objectives, which is addressed in the EU-SEC Framework as the process of operationalisation. This process has to be performed by the CSP 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 traditional certification not a replacement. 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 unreasonably high costs.

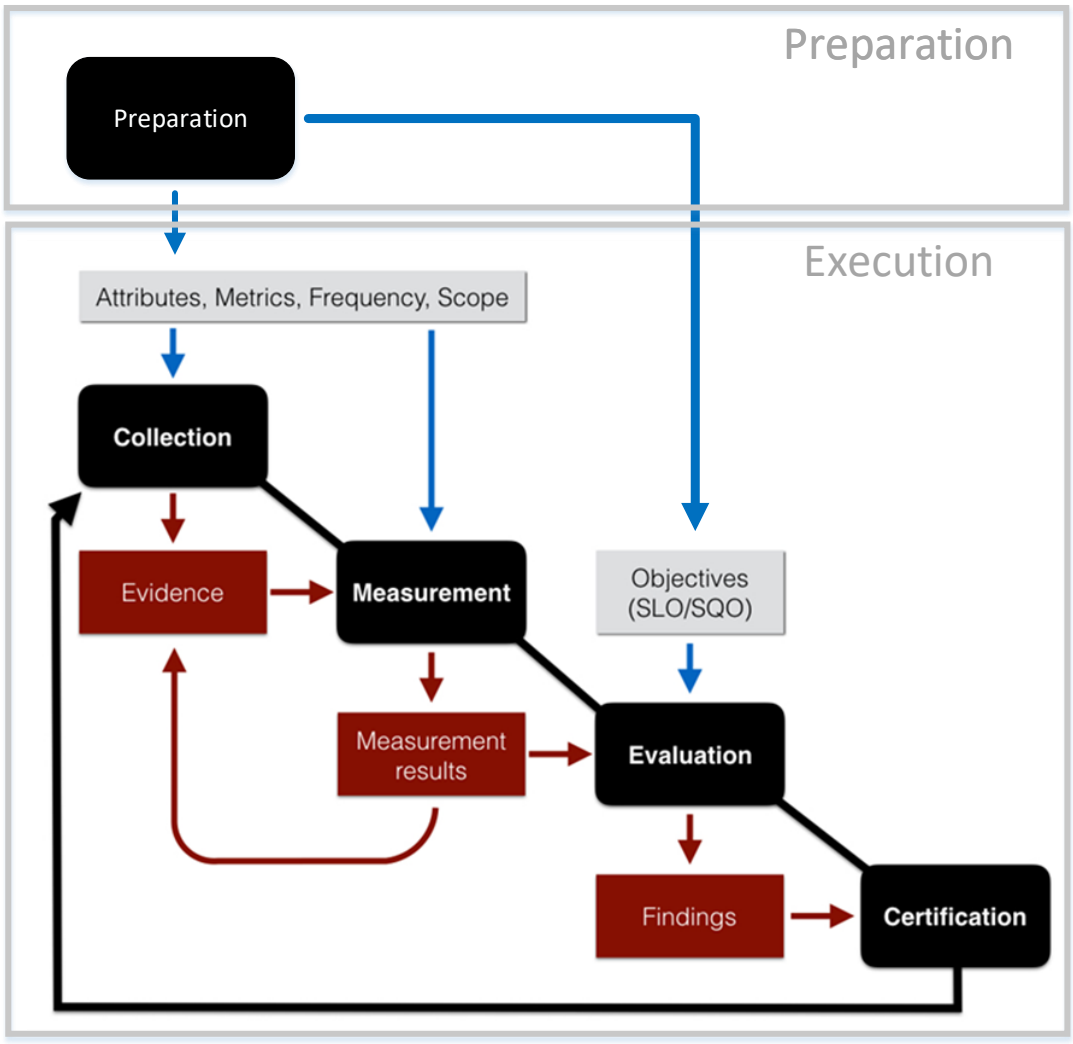

Figure 3: Model of Continuous Auditing Phases

From an architectural point of view continuous auditing can be broken down into 5 phases (See Figure 3).

The first phase has to be performed once at the initialisation. In the preparation phase, the proper operationalisation of the selected controls takes place. Key actions in this phase are the definition of the scope, the identification of the attributes and 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.

Once a continuous audit begins, all other four phases are executed continuously. The "Collection" described the collection of data for the automated assessment as well as for the non-automated assessment. 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 a security attribute. Attributes require the measurement result to be in a pre-defined format or representation. This way of conducting the measurement and interpreting the raw data is defined by 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 CABC 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 4 are:

1. **Continuous self-assessment**: 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**: the combination of a "point-in-time" certification conducted by an external auditor with a continuous self-assessment conducted by the auditee alone. 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**: 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 4: Assurance stack

2.3.3. PRIVACY CODE OF CONDUCT

The 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 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 plays a fundamental role in the context of the EU-SEC Framework since it is 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 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 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 STEP

The Govern step includes all the essential elements of governance, 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 effective and efficient operation of the framework. Furthermore, it ensures that the framework's execution is following the framework lifecycle process and staying relevant in the face of possible changes in the cloud certification market.

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.

2.5 FEEDBACK FROM PILOT EXERCISES AND REVIEWS

This section includes the summary of the relevant input collected during the implementation of the initial version of the EU-SEC Framework as defined in D2.4.

The pilot exercises and the feedback from the Advisory Board provided useful input for the validation, revision and improvement of the framework and its governance structure.

Multiparty recognition framework

Through the pilot exercises the auditors and auditees had an opportunity to use and test the MPRF and its requirements repository. Their main challenge was to understand the preliminary interpretations and expert opinions with regards to the mapping of the security requirements. A qualified group of experts provided guidance throughout the requirements comparison activities and ensured the quality of the provided results. A detailed analysis of the pilot results is provided in D4.5.

In this context, the EU-SEC governance body (presented in section 4) has been adapted to address the above challenge. The EU-SEC governance body now comprises three groups: the CSA working groups, the cloud certification stakeholders and the consulting groups. While the role of the CSA working groups is to ensure the management and proper execution of the framework, the remaining two groups are expected to validate the framework's results and provide guidance to stakeholders.

Continuous auditing and monitoring framework

The continuous audit-based certification pilot mainly aimed to test the technical feasibility of continuous audit-based certification, as embodied through an integrated toolchain constructed by several partners in the EU-SEC project. The pilot validated the key requirements of the continuous auditing-based certification, confirming the soundness of the initial approach. In summary, no changes have been applied to the initial framework as a result of the continuous auditing pilot. A detailed analysis of the pilot results is provided in D5.3.

Privacy code of conduct

The PLA CoC, as defined in D2.3, has been updated based on the review feedback received from the EU-SEC project reviewers as well as from discussions with Data Protection Authorities (DPAs). The update of the code of conduct touches upon the requirements which are felt to be key for the cloud computing sector, rather than address all GDPR requirements.

The PLA [V3] specifies the application of the GDPR in the cloud environment, primarily with regard to the following categories of requirements:

- Fair and transparent processing of personal data;
- The information provided to the public and to data subjects (as defined in Article 4 (1) GDPR);
- The exercise of the rights of the data subjects;

- The measures and procedures referred to in Articles 24 and 25 GDPR and the measures to ensure security of processing referred to in Article 32 GDPR;
- The notification of personal data breaches to Supervisory Authorities (as defined in Article 4 (21) GDPR) and the communication of such personal data breaches to data subjects; and
- The transfer of personal data to third countries.

3. INTRODUCTION TO EU-SEC FRAMEWORK'S GOVERNANCE MODEL

This chapter outlines why a governance structure is needed, what are the governance enablers and how they contribute to the effectiveness and efficiency of the framework. In addition, this chapter describes the requirements for the framework's governance bodies.

The role of the EU-SEC Framework governance structure is to ensure that the framework, in its three components (Multiparty Recognition Framework, Continuous Auditing Certification Scheme, and Privacy Code of Conduct) is implemented according to its rules and requirements, that its execution is monitored, and objectives are reached and that it remains relevant in the face of exogenous and endogenous factors.

The envisioned 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, which are described in the following section. It outlines what the governance enablers are and how they contribute to the effectiveness and efficiency of the framework and it describes the requirements for the framework's governance bodies.

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

The following seven "enablers" are factors that, individually and collectively, influence the effective and efficient integration of the components within EU-SEC Framework's governance, contributing to the overall objective. They are derived from COBIT 5, a good-practice framework for IT management and IT governance, created by the international professional association ISACA.

3.1.1. PRINCIPLES, CRITERIA AND REQUIREMENTS

Principles, criteria and requirements are the vehicle to translate behaviour into practical guidance for the execution of the EU-SEC framework. It will ensure that the MPRF and the CABC will be executed in accordance with the 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 an independent governance, 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 benefit stakeholders.

3.1.2. ORGANISATIONAL STRUCTURES

Organisational structures, as the key decision-making vehicles, consist of reporting lines, and appropriate authorities and responsibilities created in the pursuit of the objectives 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 structure aims to facilitate the governance and operation of the EU-SEC Framework. As an enabler for governance the organisational structure has the following requirements:

- Stakeholders within the framework can be external or internal and include all entities related and affected by its 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 clearly defined, and appropriate rights have to be granted.

3.1.3. PROCESSES

Processes describe an organised set of practices and activities that aim to achieve certain goals. They are influenced by other enablers such as principles and guidelines. Processes take inputs from several sources, including raw information as well as the output of other processes, and manipulate those inputs to produce outputs like changes or communication activity results.

The goals of EU-SEC processes are considered under the following categories:

- Intrinsic goals for the processes must have a certain quality that is in line with EU-SEC Framework's principles, guidelines and practices.
- To comply with contextual goals, processes are required to be customised and adapted to EU-SEC Framework's specific context. The process also must 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. Publicly available processes have to be declared as such.

The processes consider internal and external stakeholder interests. Internal stakeholders include the body executing the governance structure as well as staff and volunteers. External stakeholders to the EU-SEC Framework are all entities that are affected by its activities and targeted directly via the framework's goals.

The governance processes are addressed in section 5 of this document.

3.1.4. ARCHITECTURE AND TOOLS

Architecture and tools include the infrastructure, technology and applications that provide the framework with the information technology necessary to attain its goals. 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 tools' capabilities are referring to the necessary services and their integration in the EU-SEC Framework's governance. Those services enable communication and other capabilities. For the services to work in EU-SEC's governance it is required that a proper architecture is defined. Services can be provided by external or in-house parties, such as internal IT departments. Internal and external stakeholders must be granted access to the tools according to their level of involvement. Goals for services must be established by defining terms of services. Other requirements for architecture and tools used in the EU-SEC framework 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

3.1.5. 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 must 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 either automatically or manually, 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 the EU-SEC Framework,
- establishes value drive processes, 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 defining roles and responsibilities based on the information the particular stakeholder is dealing with.

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

3.1.6. 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 within the EU-SEC framework. Those are mainly driven by the principles and guidelines of the EU-SEC Framework. They must be introduced to internal and external stakeholders. 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 the EU-SEC Framework can absorb and the level of risk it is willing to accept.
- Agreement on the individual commitment of people towards following policies.
- Agreement upon the organisation's behaviour towards negative outcomes.

3.1.7. 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 within the EU-SEC Framework 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 must be determined for operation of the framework, which should relate to qualification levels.

3.2. GOVERNANCE BODY REQUIREMENTS

The body managing the EU-SEC Framework (hereafter referred to as "Governance Body") must be capable of executing the governance described in this document. This requires a form of management that must be defined and implemented according to the requirements of 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 must be assessed. This requires 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 EU-SEC Governance Body described in section 3.2 requires an operational model with defined structures, reporting lines, authorities, and responsibilities to achieve its goals.

The following sections outline the baseline considerations for such an operational model.

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

The EU-SEC governance body is responsible for the design and management of the EU-SEC Framework, directing the requirements of the MPRF and the CABC scheme as well as the CoC.

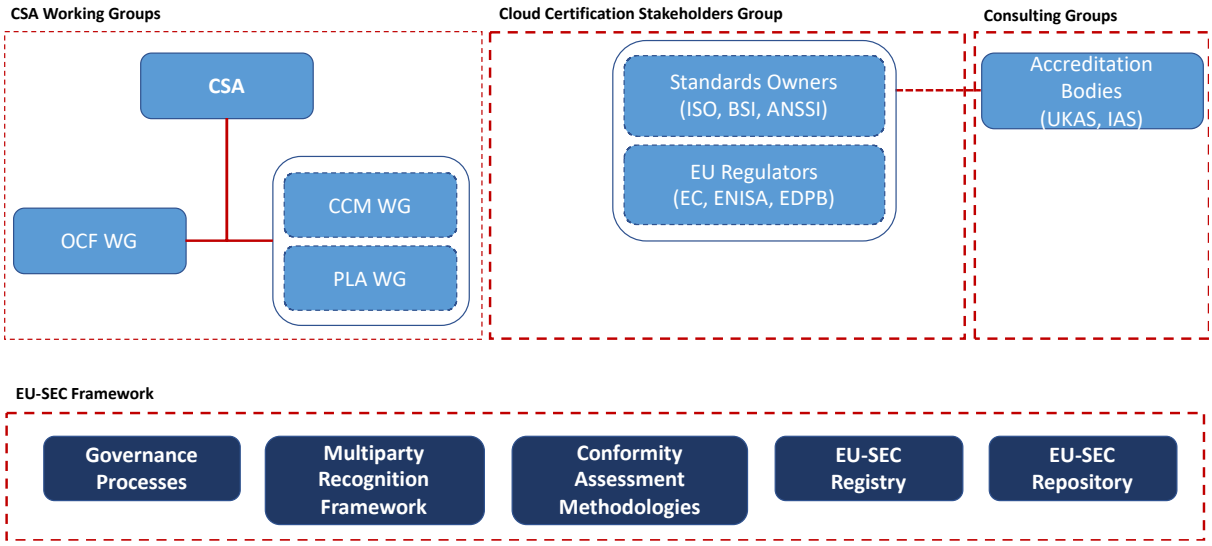

Figure 5: EU-SEC Framework Governance Body

The EU-ESC governance body is comprised of three entities, the **CSA working groups**, the **cloud certification stakeholders** and the **consulting groups**. The first two entities are the main entities supporting the framework, while the **consulting groups** are considered in a more informal consultation role. The **CSA working groups** will manage the EU-SEC Framework's activities and governance of the EU-SEC components and their activities with the objective to obtain the endorsement from stakeholders, since the goal is to make the framework as a viable solution for compliance with the EU Cybersecurity Act. The role of the **Cloud Security**

Stakeholders group is to provide guidance and eventually endorse the work the **CSA Working Groups**, as shown in Figure 5.

The **CSA working groups** entity is comprised of the CSA, OCF, CCM and PLA working groups, while the **cloud certification stakeholders group** includes the individual bodies of standard owners and EU regulators/agencies, such as EC, ENISA and EDPB.

The **consulting groups** mainly comprises accreditation bodies such as UKAS or IAS, which have a long standing experience in certification schemes and which can provide valuable insights to all stakeholders in the framework.

The EU-SEC Framework components under governance are:

- The governance processes, as presented in detail in the section 5 of this document
- The MPRF, used for the security and privacy requirements comparison and mutual recognition between different cloud security standards (see D2.1)
- The conformity assessment methodologies applicable to 1) the privacy CoC and 2) CABC schemes (see D2.2 and D2.3).
- The EU-SEC registry is a public repository of certified CSPs, based on the concept of the CSA STAR Registry[4].
- The EU-SEC Repository holds the results of the MPRF and its respective requirements comparison activities.

All governance entities and underlying working groups or bodies have distinct roles and responsibilities, defined interrelationships and interact with the EU-SEC components, as presented below.

CSA

CSA, as a no-for-profit organization, supports and oversees the implementation of the EU-SEC framework and establishes synergies with the stakeholders group with respect to the framework's activities (e.g., standards' multiparty recognition). The collaboration between CSA and the stakeholders group aims at ensuring transparency and integrity throughout the development of standards, certification implementation and management.

4 https://cloudsecurityalliance.org/star/, accessed on 23/07/19.

OCF Working Group

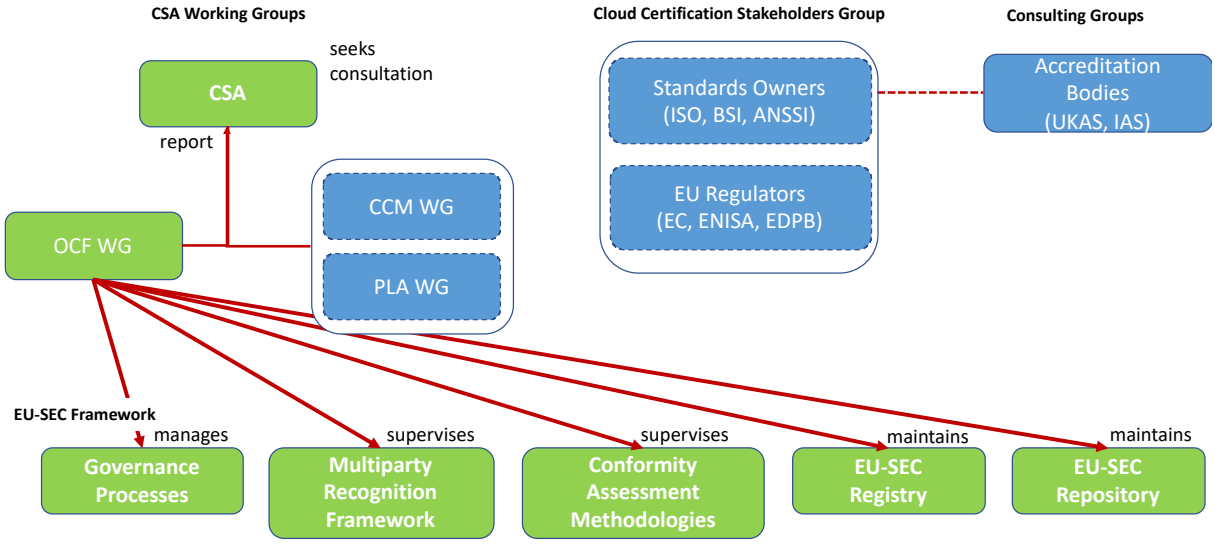

Figure 6: Overview of CSA and OCF WG relationships with EU-SEC framework components and bodies

The Open Certification Framework (OCF) Working Group (WG) is comprised and led by subject matter experts from the cloud security standardisation and certification community. The objective of the WG within the scope of EU-SEC will be the identification of news trends, standards, best practices and legal and regulatory requirements (e.g. EU Cybersecurity Act) in cloud security certification and their integration within certification solutions (i.e. self-assessment, third-party certification and attestation, and continuous auditing) already existing within the EU-SEC Framework and the CSA OCF.

As shown in Figure 6, the OCF interacts with all EU-SEC components. Its main role lies under the management of governance processes (introduced in section 5). The EU-SEC multiparty recognition activities and compliance assessment methodologies are supervised by the working group with guidance and eventual endorsement from the stakeholders group to increase the efficiency and effectiveness of EU-wide cloud security certification. The compliance assessment methodologies supervised by this group include in particular those defined for continuous audit based certification (CABC). Finally, the OCF WG ensures that the EU-SEC registry and repository are well maintained and up to date following the latest developments in the cloud certification landscape and works of the EU-SEC framework.

Table 1: OCF WG Roles and Responsibilities

Role	Responsibilities
EU-SEC Framework: Governance, multi-party recognition and continuous auditing	- Maintains EU-SEC governance and processes - Manages EU-SEC conformity assessment schemes and supervises their activities - Manages EU-SEC MPRF and supervises its activities - Seeks for consultation from the stakeholders group on standards mutual recognition results - Maintains the EU-SEC repository - Reports back to CSA top management - Defines conformance assessment requirements for continuous audit-based assessments (metrics, processes, guidance, etc.).

CCM and PLA Working Groups

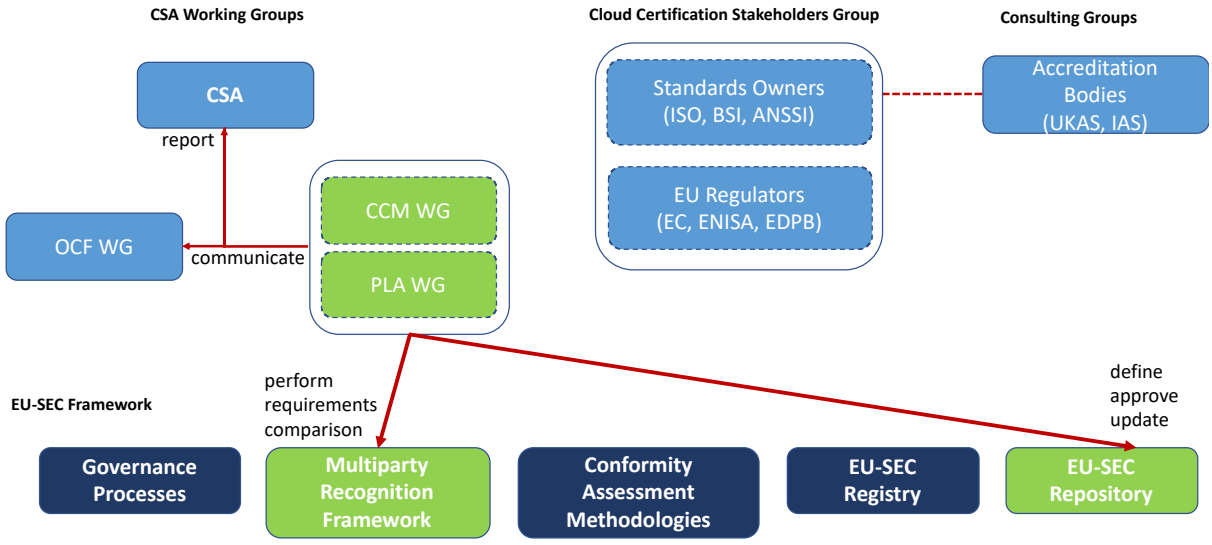

Figure 7: Overview of CCM and PLA WGs relationships with EU-SEC framework components

The CCM working group is responsible for performing requirements comparison analysis between cloud security standards. It is comprised of cloud security experts (cloud security practitioners, auditors, etc.) coming directly from the relevant industry. Its core activities fall under the MPRF's processes 3 and 4, where requirements comparison mappings, gap analysis and their validation are performed respectively.

The objective of the working group is to show the feasibility of achieving mutual recognition between well-known international cyber/cloud security standards (e.g., CSA CCM, ISO), as well as national (e.g., BSI C5, ANSSI SecNumCloud) and sectorial ones.

The results of the standards comparison works are used to update the EU-SEC Repository and made in this way available to the OCF WG and stakeholders group for validation and exploitation in favour of the standardisation community and finally cloud organisations within the EU.

Table 2: CCM WG Roles and Responsibilities

Role	Responsibilities
Security/Auditing Requirements Comparison	- Performs security requirements comparison between standards (mapping and gap analysis) - Outputs mutual recognition results between security standards - Updates EU-SEC security requirements repository and contributes to its maintenance - Reports back to CSA and communicates its output results to OCF

The PLA working group is responsible for providing to cloud service providers and consumers, a data protection and privacy guidance in adherence to EU's General Data Protection Regulation (GDPR). In addition, and similarly to the CCM WG, the PLA WG is responsible for performing comparison analysis between the requirements of data privacy standards. The outcome of these works is expected to contribute to the better understanding of the differences between the compared standards, hence increasing transparency, trust and a cost-effective adoption of these standards among cloud organisations.

The PLA WG performs its activities in the context of the MPRF and outputs its results to the EU-SEC repository, thus making them available to the OCF WG and stakeholders group for validation and exploitation in favour of the standardisation community and finally cloud organisations within the EU.

Table 3: PLA WG Roles and Responsibilities

Role	Responsibilities
Privacy Requirements Comparison	- Performs privacy requirements comparison between standards (mapping and gap analysis) - Outputs mutual recognition results between privacy standards - Updates EU-SEC security requirements repository and contributes to its maintenance - Reports back to CSA top management and communicates its output results to OCF

Cloud Certification Stakeholders Group

This group is comprised of standard owners organisations, accreditation bodies and EU regulators/agencies. The objective of the group is:

- To provide guidance on requirements that should be considered in the context of the MPRF, CABC, and the PLA CoC.
- Where appropriate and useful, provide an endorsement of the output of the work of the CSA Working groups in order to stimulate best practices in assurance in the EU.

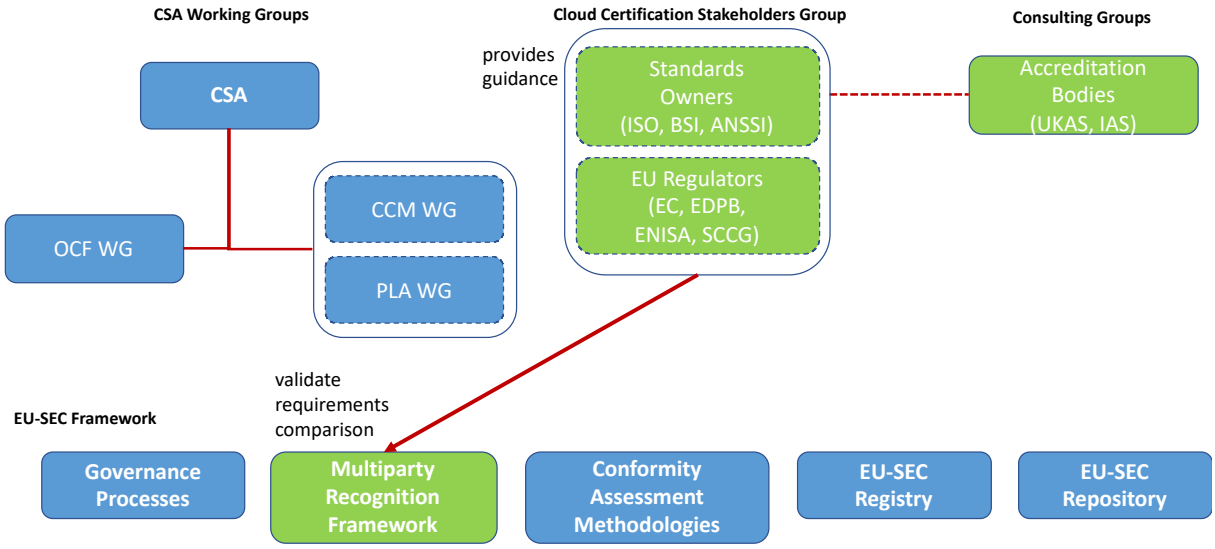

Figure 8: Overview of Cloud Certification Regulators relationships with EU-SEC framework components and bodies

More specifically, the group plays a fundamental role in the context of the MPRF as it provides guidance for evaluating and validating the requirements comparison results provided by the CCM WG during the analysis performed during process 3 of the framework after the process 4 "Comparison Results Validation", the group will provide feedback on the multiparty recognition results, that is, if the mappings, the gap analysis methodology and output results meet its quality standards. In case quality is substandard, recommendations from the group will be provided to the OCF and finally the CCM WG to review the indicated works and implement the necessary improvements in order to improve quality and reach a consensus between the group and the OCF.

In the context of CABC, the group will review, validate and eventually endorse the output of the OCF working, including:

- Catalogues of security and privacy metrics used for continuous assessments.

- Best practices for the application of metrics to platform-specific attributes, SLOs and SQOs.
- Assessment and monitoring guidance for auditors.

Additionally, the group will review PLA requirements and evaluation criteria.

The OCF and the stakeholders group will leverage the quality review and any recommendations to improve the efficiency and effectiveness of cloud security and privacy certification on a EU-wide scale.

Table 4: Stakeholders Group Roles and Responsibilities

Role	Responsibilities
Mutual Recognition Quality of Results	- Evaluate and validate the multiparty recognition output results provided by the CCM WG - Provide guidance to the OCF for multiparty recognition between standards - Ensure EU-SEC repository quality of results

Standards Owners

Represent the bodies or organisations who are the owners of the standards that are selected and compared for mutual recognition under the EU-SEC Framework activities.

Their contribution will ensure that the framework is comprised of standards with an equivalent level of quality and maturity. The MPRF, through the various standards' requirements comparison, enables standard owners to keep track of multiple standards' differences and their evolution, and provides the opportunity to review their own on a regular basis and update them accordingly, if required.

The framework favours collaboration between standard owners and encourages the establishment of mutual agreements between these parties, to recognise full or partial equivalences between their standard's requirements and their governance.

Table 5: Standards Owners Roles and Responsibilities

Role	Responsibilities
Advise Stakeholders Group	- Participate in Stakeholders group and provide consultation and feedback on own standard's requirements - Participate at own standard's mutual recognition activities - Provide guidance on mutual recognition with other standards' owners or regulators

EC, ENISA and European Data Protection Board (EDPB)

This group's role will be advisory to CSA and its working groups with regards to the requirements of the EU and the upcoming European certification framework, in the context of the Cybersecurity Act[5], as well as GDPR.

The group will be tasked to provide recommendations and guidance on the direction to be taken by EU-SEC framework so to be able to align with the requirement of the European Cybersecurity Act and its implementing acts and eventually endorse and accept the results as contribution to the Cloud Computing European Cybersecurity Certification Framework that will be defined by ENISA and approved by the European Commission.

Table 6: EU regulators roles and responsibilities

Role	Responsibilities
Advise Stakeholders Group	- Provide guidance and recommendations on how to evolve the current multiparty recognition framework (MPRF) to be an accepted component of the Cloud Computing European Cybersecurity Certification Framework - Assess and eventually approve the MPRF as a component of the Cloud Computing European Cybersecurity Certification Framework - If/once the initial results of the MPRF are approved, provide guidance on its evolution over time (e.g. updating security requirements) - Review the role of continuous auditing-based certification, notably for high-risk applications in the context of the Cybersecurity Act. - Provide guidance and recommendation on how to include continuous auditing as an accepted component of the Cloud Computing European Cybersecurity Certification Framework - Assess and eventually approve continuous auditing as a component of the Cloud Computing European Cybersecurity Certification Framework - If/once the initial results of the continuous auditing are approved, provide guidance on its evolution over time (e.g. updating security requirements) - Provide guidance and eventually approve the EU-SEC Registry as a component of the Cloud Computing European Cybersecurity Certification Framework - Provide guidance and eventually approve the PLA CoC as a mechanism for GDPR compliance.

5 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act, accessed on 5/8/19.

Accreditation Bodies

This group, acting as a consultation entity, represent the bodies or organisations that are accrediting the auditing bodies and auditing methodologies and will participate in the context of multiparty recognition and continuous audit based certification.

One of the core comparison activities of the MPRF is that of the auditing requirements comparison between the various certification schemes. Accreditation bodies will investigate and possibly ensure that different auditing requirements from different standards can be normalised and integrated in the context of certification schemes' mutual recognition.

Continuous audit based certification requires auditors to perform a more extended analysis of the auditee's information system, including an assessment of the monitoring tools that are used for continuous auditing. Accreditation bodies will be consulted to define the extended level qualification that will be required from auditors to cover these new tasks.

Table 7: Accreditation bodies roles and responsibilities

Role	Responsibilities
Advise Stakeholders Group	- Provide consultation on mutual recognition of auditing criteria/requirements between two compared standards - Propose means of integration of multiple auditing standards under a common certification scheme or method based on mutual recognition - Review extended requirements applicable to auditors that undertake audit activities in the context of CABC.

4.2 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.

- **Standard Owner / Authority**
  The Scheme Owner / Authority has no additional roles and responsibilities as mentioned in D2.1 (section 4.2) and D2.2 (section 6.1).

- **Cloud Service Provider**

The Cloud Service Provider has no additional roles and responsibilities as mentioned in D2.1 (section 4.2) and D2.2 (section 6.1).

- **Authorised Auditors**
  The Cloud Service Provider has no additional roles and responsibilities as mentioned in D2.1 (section 4.2) and D2.2 (section 6.1).

4.1.1. 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 (section 4.2) like organisation and operation of all defined governance processes as well as coordinating working groups and D2.2 (section 6.1) like qualifying external auditors to perform audits as well as establishing rules for recognition of external auditors.

5. GOVERNANCE PROCESSES

In order to achieve an effective and efficient operation of the framework, the EU-SEC Framework governance will be comprised of five governance processes that are defined in this section.

5.1. POLICY AND ROLE MANAGEMENT

Policies reflect management's statement of what should be done to effectively control the framework and its operation. Management's policies shall be communicated explicitly in writing or implied through management's actions and decisions. Procedures consist of actions that implement a policy. Policies can be created in the form of guidelines, rules, regulations, etc. Roles indicate the responsible person for the defined aspects in the policies. Both procedures and roles 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 framework. The policy and role management process is comprised of seven activities, starting from setting the goals finishing with 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 group 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 8: 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.
Timeliness	Responsible personnel perform 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 comprise eight activities as outlined in the table below:

Table 9: 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

Policy and Role Management Process	
	- Request from Change Management - Request from Complaint Management - Request from Resource Management
Activities	1. Set the goals and directives of the EU-SEC framework 2. Establish the organisational structure and reporting line 3. Define the responsibility and accountability of roles and groups 4. Establish policies and procedures to support deployment of EU-SEC's directives 5. Approve the policies and procedures by the EU-SEC Governance Body 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 10. 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	CSA	C	A	A R	A	A R	A	A
	Stakeholders group	R	C I	I	C I	I	A R	R
	OCF WG	R	R	C	R	C/I	R	R
	CCM/PLA WGs	C I	I	C I	I	I	I	C 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 the EU-SEC Framework is governed.

Table 11. The Policy and Role Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #1	
List of the activities: *1# The OCF WG in conjunction with the* Stakeholders group *shall set the goal of the business and the directives of the EU-SEC framework. With clear objectives, the instructions and guidance establish the requirements and measures with which to guide and measure the success of the activities.* *2# The goals and directives must be documented in writing, approved by CSA and regularly assessed to reflect the current environment.*	
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 12. 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 Framework must enable the operation of the entities and organisational structures that operate and execute the governance.*

Activity #2	
2# The EU-SEC governance body must define reporting lines including responsibilities and accountabilities as the basis for the decision making process. . The reporting lines ensure the information flow within the organisation, that is essential for important decision making and governance of the EU-SEC Framework.	
Inputs (upstream)	**Outputs (downstream)**
1# Documented and approved EU-SEC framework business goals and directives. 2# Request / requirements from Multiparty Recognition Framework 3# Request / requirements from Continuous Auditing Scheme 4# Request / requirements from Privacy Code of Conduct 5# Request from Change Management 6# Request from Complaint Management 7# Request from Resource Management	1# EU-SEC organisational structure 2# EU-SEC framework 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 13. The Policy and Role Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
1# CSA must define the responsibility and accountability of roles, groups and business. The responsibilities shall align with the business goals and directives defined. • *Working areas or groups* • *Functionalities and duties* • *Collaboration and communication*	
Inputs (upstream)	**Outputs (downstream)**
1# Document and approve EU-SEC framework's business goals and directives. 2# EU-SEC organisational structure 3# EU-SEC organisation reporting line	1# EU-SEC organisational structure with defined responsibility and accountability for each role, group, and business unit.

Activity #3	
4# Request / requirements from Multiparty Recognition Framework 5# Request / requirements from Continuous Auditing Scheme 6# Request / requirements from Privacy Code of Conduct 7# Request from Change Management 8# Request from Complaint Management 9# Request from Resource Management	

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

Activity #4
List of the activities: *1# The OCF WG together with CSA will continually identify the required policies and procedures needed for the EU-SEC to function. As a recommendation, policies should initially first cover:* • *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* *2# A policy and procedure template must be established covering the following 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,*

Activity #4	
• *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 established in a written form shall consider. the following aspects:* • *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 framework's business goals and directives. 2# EU-SEC organisational structure 3# EU-SEC organisation reporting line 4# Policies and procedures best practices 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	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 15. The Policy and Role Management Process Activity #5 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #5	
List of the activities: *1# CSA receives the policies and procedures, and gives a final approval. In case of rejection, reasons shall be provided to guide further improvement. After rework the policies and procedures, shall again be reviewed. The process (feedback loop) continues until final approval is obtained.*	
Inputs (upstream)	**Outputs (downstream)**
1# Documented and approved EU-SEC framework's 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	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 16. The Policy and Role Management Process Activity #6 Card to Detailed Sub-Activities, Inputs and Outputs.

<table>
<tr><th colspan="2">Activity #6</th></tr>
<tr><td colspan="2">List of the activities:
1# The publication channel is decided, and communication plans are established.
• Publication channel: a document management system, where the EU-SEC policies and procedures are stored and can be accessed by the audience.
• Communication plan: how the target audience is made aware (Email, workshop, or awareness training, etc) of new policies and procedures ,.

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.</td></tr>
<tr><th>Inputs (upstream)</th><th>Outputs (downstream)</th></tr>
<tr><td>1# Approved EU-SEC policies and procedures in written form</td><td>1# Established publication channel for EU-SEC policies and procedures
2# Executed communication with target audience on the EU-SEC policies and procedures</td></tr>
</table>

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

Table 17. 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 the EU-SEC framework and continue to meet market demands.* *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 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 complaint management system in a more general manner along with the relevant Governance Enablers.

The following Governance Enablers were identified as key for 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 complaint-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 18: 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 without preventing problem resolution. 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 governance body.
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 must fulfil the following functional requirements that were derived from the aforementioned general complaint management principles and requirements.

Table 19: 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 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 governance body. 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 monitoring and review activities, e.g. by providing number or proportions of: • complaints received within a period of time, • complaints resolved at a certain point in time, • 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. 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 "objectivity" and "customer-focused approach" principles shall be met by establishing and monitoring collective and individual goals for the EU-SEC Complaint management group and its members. The goals and associated incentives and rewards shall be proposed and established by CSA. 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 same process defined at the Multiparty Recognition Framework. 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 20. 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

CSA has the main responsibilities for the complaints management process. The responsibilities are presented in the RACI matrix per assigned activity below.

Table 21. The Complaint Management Process activities mapped to roles and responsibilities.

Roles	**Complaint Management Process Activities**						
	#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**
CSA	A R	A R	A R	A R	A	A	A R
Stakeholders Group	-	-	-	-	-	-	-
OCF WG	I	C	C	-	R	R	-
CCM/PLA WGs	-	-	C	I	I	I	-
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 22: 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 CSA 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 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 acknowledgement 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 23: The Complaint Management Process Activity #2 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #2	
List of the activities: 1# *CSA 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 24: The Complaint Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: 1# *CSA investigates the complaint and provides a decision or action (solution) to solve the complaint. Support is obtained from the OCF WG as deemed applicable for the nature of the complaint. The level of investigation should be commensurate 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 25: The Complaint Management Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4	
List of the activities: 1# *CSA 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 26: 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, CSA 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 CSA informs the OCF WG and initiates the identification of alternative solutions. Activities 3 to 5 are repeated as deemed appropriate in the circumstances. CSA 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. CSA 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 27: 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, CSA or the OCF WG accordingly 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 28: 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, CSA 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 29: 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 fallback 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 Governance body.

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 30. 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 31. The Change Management Process Activities' Mapped to Roles and Responsibilities.

Change Management Process		**Activities**							
		#1	**#2**	**#3**	**#4**	**#5**	**#6**	**#7**	**#8**
Roles	CSA	A	-	A R	A	I	A R	I	-
	Stakeholders Group	R	C	-	-	I	-	I	C
	OCF WG	R	A R	-	R	A R	-	A R	A R
	CCM/PLA WG	I	C	-	R	R	-	R	C
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 32. The Change Management Process Activity #1 Card to Detailed Sub-Activities, Inputs and Outputs.

<table>
<tr><th colspan="2">Activity #1</th></tr>
<tr><td colspan="2">List of the activities:
1# The Change Requestor (e.g., member of the OCF Working Group or the Stakeholders Group) 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 OCF WG 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.</td></tr>
<tr><th>Inputs (upstream)</th><th>Outputs (downstream)</th></tr>
<tr><td>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</td><td>1# RfC in status “submitted” in the change management ticketing system</td></tr>
</table>

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 33. 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 OCF WG 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 OCF WG 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 OCF WG 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;* • *The possibility of fallback 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;*

Activity #2	
• *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 34. The Change Management Process Activity #3 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #3	
List of the activities: *1# CSA* 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 inappropriate, CSA 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 governance body obtains the authorisation in accordance with the change categorisation.* • *Minor change: CSA** • *Regular change: CSA* + Working Groups responsible for the components affected by the change* • *Major change: CSA* + Working Groups responsible for the components affected by the change + OCF WG* *4# If the authorisation is refused, the rationale for the decision is recorded with the RfC and CSA 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 that 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 35. 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, CSA assembles an effective Change Implementation Team that includes appropriate members from the OCF and CCM/PLA working groups 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 stakeholders' responsibilities, OCF WG 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.* 3# *CSA 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 OCF WG 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 36. 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*

Activity #5	
are remediated and formally accepted; the decision is documented by the Change Implementation Team. *6# The Change Implementation Team specifies fallback and recovery procedures.* *7# The Change Implementation Team initiates actions to update relevant documents.* *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)**
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 37. The Change Management Process Activity #6 Card to Detailed Sub-Activities, Inputs and Outputs.

<table>
<tr><th colspan="2">Activity #6</th></tr>
<tr><td colspan="2">List of the activities:

1# After the Change Implementation Team promoted the deliverables for production or release, CSA obtains the approval in accordance with the change categorisation.
• Minor change: CSA*
• Regular change: CSA* + Working Groups responsible for the components affected by the change
• Major change: CSA* + Working Groups responsible for the components affected by the change + OCF WG
• 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 OCF WG 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 to 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 which participated in the Change Implementation Team that executed activity #5 must not be involved in the approval.</td></tr>
<tr><th>Inputs (upstream)</th><th>Outputs (downstream)</th></tr>
<tr><td>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)</td><td>1# RfC in status “approved” in the change management ticketing system</td></tr>
</table>

5.3.2.7. ACTIVITY #7: IMPLEMENT CHANGE

Abstract: The change is implemented.

Table 38. The Change Management Process Activity #7 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #7	
List of the activities: *1# The OCF WG 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 39. 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 OCF WG 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 OCF WG 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 OCF WG creates an action plan for identified issues to prevent their re-occurrence in future changes. The action plan is provided to the OCF WG 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.

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 resource management.

Table 40: Principles and related Requirements for Resource Management

PRINCIPLE	REQUIREMENT
Quantifiable	The resources in use and their planning shall be quantifiable to support the understanding of the organisation's current state and its future needs.
Forecast	The resource consumption status and resources in need must be evaluated. Resource forecast shall be made on regular basis from different levels: IT resource, human resource, financial resource and in order to ensure their adoption in a timely manner.

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 41: 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 framework 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 42: The resource management process activities' mapped to roles and responsibilities

Resource Management Process		**Activities**			
		#1	**#2**	**#3**	**#4**
Roles	CSA	C	C	C	C
	Stakeholders Group	-	R	-	-
	OCF WG	R A	R A	R A	R A
	CCM/PLA WGs	-	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 43: 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 the OCF WG*	
Inputs (upstream)	**Outputs (downstream)**

Activity #1	
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 44: 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 45: 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# The OCF WG to provide regular reports for efficient resources management*	
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 46: 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# OCF WG to provide regular reports for resources management* *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 the OCF WG*	
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 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 47: 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 to ensure valid and useable results.
Comparable	The monitoring results are comparable to the goals, 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 comprise five activities as outlined in the table below:

Table 48: 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 the OCF WG and Stakeholders Group - 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 49: The monitoring and measurements process activities mapped to roles and responsibilities.

Monitoring and Measurements Process		**Activities**				
		#1	**#2**	**#3**	**#4**	**#5**
Roles	CSA	C	-	-	I	-
	Stakeholders Group	R	I	I	I	R
	OCF WG	R A	R A	R A	R A	R A
	CCM/PLA WGs	C	-	-	I	-
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 50: 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 within the OCF WG and* Stakeholders Group. *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 OCF WG and Stakeholders Group 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 51: 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 52: 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 53: The Monitoring and Measurement Process Activity #4 Card to Detailed Sub-Activities, Inputs and Outputs.

Activity #4	
List of the activities: *1# The OCF WG reports deviation report to the EU-SEC Governance body WGs and Regulators'* Group. 2# *The OCF WG reports effectiveness report to the EU-SEC Governance body WGs and Regulators'* Group.	
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 54: 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. FINDINGS

The EU-SEC framework is composed of 3 main components:

1. the Multiparty Recognition Framework,
2. Continuous Auditing Certification Scheme and
3. Privacy Code of Conduct

This document presented the EU-SEC framework's governance body structure, as well as the governance model with five main governance processes have been defined to support the effective and efficient operation, and continuous improvement of the EU-SEC framework. These processes are:

- Policy and role management
- Complaint management
- Change management
- Resource management
- Monitoring and measurements

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 will be realised and implemented after the EU-SEC Project has finished.
- The EU-SEC Governance Body model, which provides a good foundation for the further implementation of the EU-SEC framework.
- The EU-SEC Framework's governance model with five governance processes, which demonstrate the EU-SEC framework's governance structure and governance activities. This provides the baseline for the future implementation of the governance model around the EU-SEC Framework's components.

The EU-SEC framework has been finally successfully completed, based on the know-how, lessons learnt and experience gained throughout the project duration. Along with the aforementioned achievements, we would like to outline the important role this work can play towards the preparations and development of the EU certification framework, under the umbrella of the EU Cybersecurity Act.

ANNEX A

This annex is created with a purpose to record the changes applied during the transition from the deliverable D2.4 to the final EU-SEC framework presented at D2.5.

New content is introduced to:

Section 1 Introduction	Extension of the scope and objectives based on the feedback from pilots, workshops and reviews. Review of the approach.
Section 2 EU-SEC Framework overview	Review of the chapter, adding detailed feedback from pilots and reviews.
Section 3 Introduction to EU-SEC framework's governance	Review and update of the chapter.
Section 4 Governance Body Organisation	Update of the governance body organisation based on the feedback from pilots, workshops and consortium feedback.
Section 5 Governance Processes	Update on the matrices with new governance organisation and roles and responsibilities.
Section 6 Findings	Review and update of the findings.