PDP4E

Methods and tools for GDPR Compliance through

Privacy and Data Protection 4 Engineering

Specification and design of assurance tool for data protection and privacy

Project: PDP4E
Project Number: 787034
Deliverable: D6.1
Title: Specification and design of assurance tool for data protection and privacy
Version: v1.3
Date: 10/07/2019
Confidentiality: Public
Author(s): Alejandra Ruiz (TECNALIA),
Jabier Martinez (TECNALIA),
Javier Puelles (TECNALIA),
Izaskun Santamaria (TECNALIA),
Samuel Martin (UPM),

Funded by

Table of Contents

DOCUMENT HISTORY 3
LIST OF FIGURES 3
LIST OF TABLES 3
ABBREVIATIONS AND DEFINITIONS 4
EXECUTIVE SUMMARY 5
1 INTRODUCTION 6
1.1 OBJECTIVE OF THE DOCUMENT 6
1.2 STRUCTURE OF THE DOCUMENT 6
1.3 RELATION WITH OTHER DELIVERABLES 6
2 BACKGROUND ON ASSURANCE TOOLS 7
3 USER NEEDS 9
4 REQUIREMENTS ELICITATION 11
5 DESIGN 22
5.1 USE CASES 22
5.1.1 Reference Framework Management 22
5.1.2 Assurance Project Management 23
5.1.3 Assurance Case Management 27
5.1.4 Evidence Management 32
5.1.5 Assurance Reporting 34
6 ARCHITECTURE 36
7 REFERENCES 38

Document History

Version	Status	Date
V0.1	Initial Table of Contents	16/01/2019
V0.2	Draft of sections use cases	24/04/2019
V0.5	Draft of the requirements elicitation	10/06/2019
V1.0	Completed all sections	17/06/2019
V1.1	Comments from 1st review addressed	27/06/2019
V1.2	Comments from 2nd review addressed	10/07/2019

Approval		
	Name	**Date**
Prepared	Alejandra Ruiz (TECNALIA)	10/07/2019
Reviewed	Nicolás E. Díaz Ferreyra (UDE) Patrick Tessier (CEA)	21/06/2019 09/07/2019
Authorised	Antonio Kung (TRIALOG)	15/07/2019

Circulation	
Recipient	**Date of submission**
Project partners	11/07/2019
European Commission	15/07/2019

List of Figures

Figure 1 - Assurance Management environment 9
Figure 2 GPDR Actors from the assurance viewpoint 10
Figure 3 Use cases on compliance management 22
Figure 4 Use cases on Assurance Project Management 24
Figure 5 Use cases on Assurance Case Management 28
Figure 6 Use cases on Evidence Management 32
Figure 7 Use cases on Assurance Reporting 34
Figure 8 Functional decomposition of Assurance tool 36

List of Tables

Table 1 Use case "Capture information from standards". 22
Table 2 Use case "Define equivalence mappings". 23
Table 3 Use case "Manage an assurance project". 24
Table 4 Use case "Create assurance project". 25

Table 5 Use case "Drop assurance project"..... 25
Table 6 Use Case "Define Assurance Project Baseline"..... 26
Table 7 Use Case "Navigate Assurance repository”. 26
Table 8 Use case "Manage agreements on compliance means". 27
Table 9 Use case "Define Compliance means". 27
Table 10 Use Case "Monitor argumentation status". 28
Table 11 Use Case "Define and navigate an assurance case structure". 29
Table 12 Use case “Develop Claims and Links to Evidence”. 30
Table 13 Use case "Define an argument pattern"..... 30
Table 14 Use case “Apply an argument pattern”. 31
Table 15 Use case “Semi-automatic generation of product arguments”. 31
Table 16 Use case “Automatic generation of process arguments”..... 32
Table 17 Use case "Characterise Artefact"..... 33
Table 18 Use case “Link Artefact with External Tool”. 33
Table 19 Use case “Specify Artefact Lifecycle”..... 33
Table 20 Use case “Evaluate Artefact”. 34
Table 21 Use case "Monitor status of assurance project". 35
Table 22 Use case "Report on assurance assessment". 35

Abbreviations and Definitions

Abbreviation	Definition
DPIA	Data protection impact assessment
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IOT	Internet of Things
OEM	Original Equipment Manufacturers
PDP	Privacy and Data Protection
PDP4E	Privacy and Data Protection 4 Engineering
PDPbD	Privacy and Data Protection by Design
PET	Privacy-enhancing Technologies
TFEU	Treaty on the Functioning of the European Union
WP29	Data Protection Working Party

Executive Summary

The deliverable D6.1 (Specification and design of assurance tool for data protection and privacy) is the output of the Task 6.2, which falls within the scope of the Assurance discipline which supports the demonstration of compliance with GDPR and the observance of the principle of accountability through systematic capture of evidences, their association to requirements and artefacts, traceability to the GDPR, and argumentation of compliance derived from those evidences.

This document is going to be used during the execution of Task 6.1, Task 6.3 and Task 6.4 of WP6. The PDP4E deliverables D6.1 (Specification and design of assurance tool for data protection and privacy) plans to be a living document. Two more versions and planned to be based on this document. This document is one of the outputs of Task 6.2 (Design and specification of the PDP4E assurance tools for compliance and accountability.

1 Introduction

1.1 Objective of the document

The objective of this document is to include a comprehensive architecture of the assurance tool according to the users' needs firstly identified in deliverable D2.2 [7] and the requirements and architecture specified in WP2. This document provides a detailed design of the tool for data protection and privacy assurance. This is a first version of the specification of such a tool which will iteratively improve up in two more occasions.

1.2 Structure of the document

This document is structured as follow, first a brief introduction of the document, Section 2 provides a high-level description of assurance tools on the market, Section 3 describes the users' needs identified for an assurance tool in the context of the GDPR and privacy regulation. Next, Section 4 includes the requirements elicitation for PDP4E assurance tool, and finally Section 5 describes the design in form of use cases.

1.3 Relation with other deliverables

This document is strongly related with deliverables D2.2 "Technical analysis and synthesis of user requirements" which has served as an input for the user needs described in section 3.

Deliverable D2.3 "Overall system requirements" is beings created in collaboration with authors of this document, and as such the information included in D2.3 is coherent with the requirements included in section 4.

2 Background on assurance tools

As we mentioned in deliverable D7.2 [1], there is a lack of tools targeting responsible product design regarding the GDPR and other regulations and standards at any time of their development. Moreover, tools often lack of features for the systematic capture and recording of evidences, their association to requirements and artefacts and their traceability to the GDPR.

We propose the use of OpenCert [2] to support the assurance activities and adapt it for addressing the particular requirements of the GDPR. Privacy assurance can be defined as the process of the systematic gathering, quantifying, and using of information in view of judging the effectiveness of the actions done to comply with the privacy standards. OpenCert is an integrated and holistic solution for assurance and certification management of Cyber-Physical Systems (CPS) spanning the largest safety and security-critical industrial markets, such as aerospace, space, railway, manufacturing, energy and health. The ultimate aim is to lower certification costs in face of rapidly changing product features and market needs.

The current features of OpenCert include the management of information from standards and regulations, the management of assurance projects, architecture-driven assurance, assurance case management, and compliance management. For architecture-driven assurance, OpenCert is linked with the Papyrus [3] and CHESS [4] Eclipse projects, and with the EPF project [5] for compliance management.

The main functional blocks from OpenCert that will be used and modified in the context pf PDP4E project are:

- **Reference Framework Management**: Functionality related to the management of standards information as well as any other information derived from them, such as interpretations about intents, mapping between standards, etc. This functional group maintains a knowledge database about “standards & understandings”. The database is independent of the assurance projects. OpenCert project hosted in eclipse do not include any model of any standard. The modelling of the GDPR should be done specifically in this project and the metamodel used for standard modelling should be analysed and modify if necessary.
- **Assurance Project Lifecycle Management:** This functionality factorizes aspects such as the creation of assurance projects. This module manages a “project repository”, which can be accessed by the other modules.
- **Assurance Case Management:** This group manages argumentation information in a modular fashion. It also includes mechanisms to support compositional safety assurance, and assurance patterns management. It supports the idea of the assurance case as the OMG defined “An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. An Assurance Case is a document that facilitates information exchange between various system stakeholder such as suppliers and acquirers, and between the operator and regulator, where the knowledge related to the safety and security of the system is communicated in a clear and defendable way” [9]. It will be used to include privacy and security argumentation. An argumentation pattern library should be created to provide the best practices on privacy argumentation. The connection on arguments depending on the risk management information used in WP3 should be studied.
- **Evidence Management:** This module manages the full life-cycle of evidences and evidence chains. This includes evidence traceability management. This module is used to

store all evidenced used for GDPR accountability purposes. New ways for connecting with outcomes from other work packages tools should be analysed.

- **Assurance Reporting:** This functionality is related with the reporting and compliance levers measurement. New reports should be designed and created on GDPR related topics and for the PDP4E pilot's domain.

3 User needs

As we mentioned in deliverable D7.2 [1], different roles and processes are involved in preparing an assurance project, as shown in Figure 1. Therefore, solutions on the assurance management area need to be prepared for being used by an audience with very diverse backgrounds and motivations. Therefore, we have identified the following main customer groups based on how likely it is that they are interested in a tool of such characteristics:

- Product management boards within data controllers, processors and third parties
- Assessor and Authorities
- Tool providers

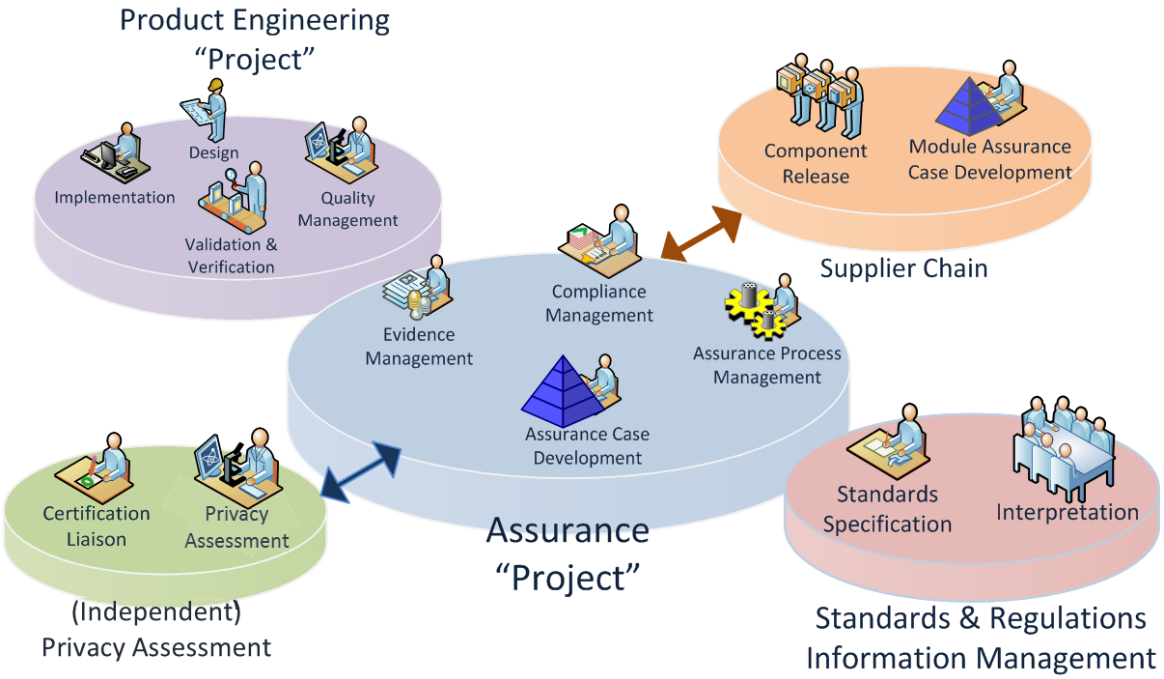

Figure 1 - Assurance Management environment

In deliverable D2.1 [6] the main actors involved in the development lifecycle were identified from the perspective of the PDP4E project. In this section we are not eliciting them again, but we will specialize them for the purposes of this particular work package.

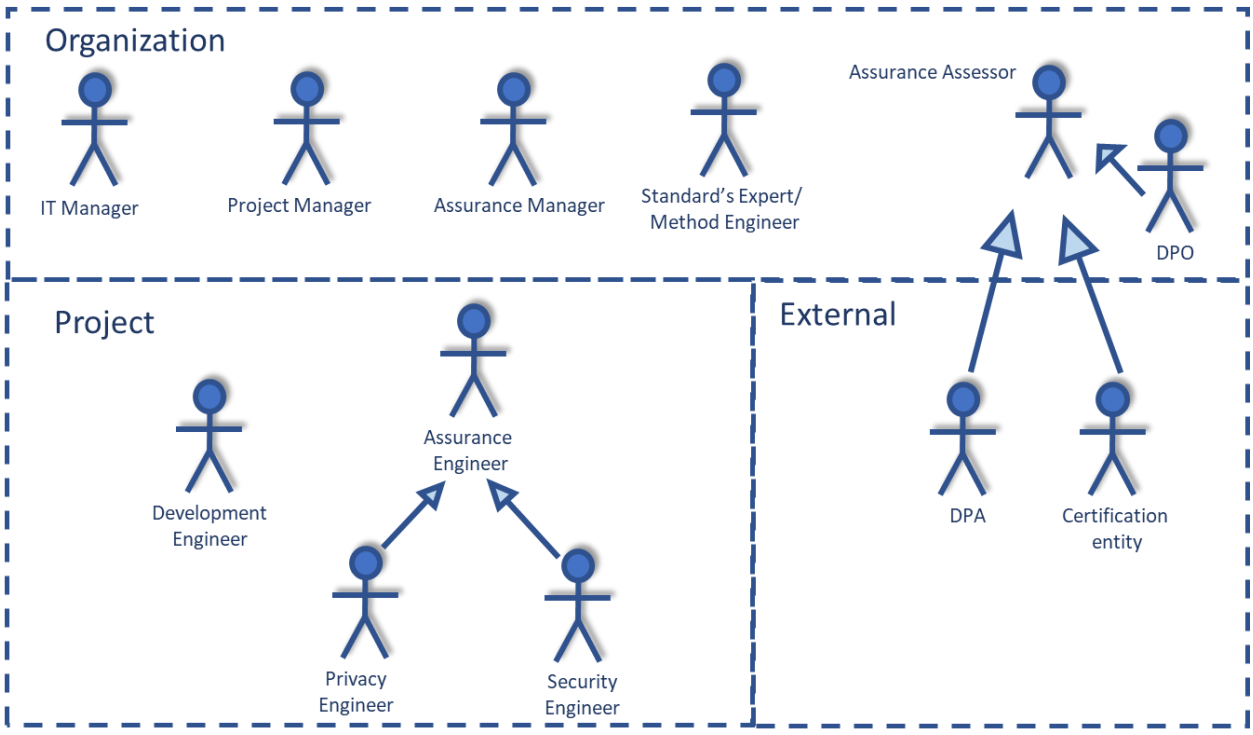

Figure 2 GPDR Actors from the assurance viewpoint

- **Management**. It includes managers from the most important hierarchically like the Project Manager or the Assurance Manager. This last one is a specific actor artificially created to represent a manager who is in charge of managing all the processes and activities involved in assurance platform usage. This also includes an IT Manager who is in charge of managing and setting the assurance tool platform, as an IT infrastructure. A special actor here is Standards Expert or Method engineer. This role should be performed by someone with a strong expertise in the regulations' applications and the company's processes.
- **Engineers**. Any actor involved in the execution of development, Validation & Verification and safety-security analysis activities. We separate privacy and security engineers, since some activities may need to distinguish according to the targeted concern (privacy and security).
- **Assessors**. Two kind of assessors need to be distinguished: internal to the company and external or independent assessor. Assessors internal to the company such as a DPO could have access to the whole set of projects from the company and know the company code of conducts so they could enforce to use some available evidences to justify compliance. External assessors such as DPA or a certification entity would only see the public information of regularly one project.

4 Requirements elicitation

Formalization of the requirements.

[Original ID - The ID used in your requirements management system. A single project cannot have two requirements with the same original ID]	[Short description of the requirement] ID: [R]-[T]-[WP]- [xxx] [R-requirement] [T-Type] [WP – Work package] [xxx – sequential number]
Description	[Detailed definition of the requirement]
Relation to other requirements	[ID of the other requirements which this requirement has a relation]
Actor	[A person in a certain role or different system interacting with the system of interest: Assurance Manager, Product Engineer, Assurance Assessor (Independent/Internal), System Administrator, Configuration Manager]
Priority	[MoSCoW priority] (Must have, Should have, Could have, and Won't have but would like) [8]
Type	[Functional (F)or Non-functional) (NF)] (Non-functional requirements describe the quality of functional requirements)
Non-functional category	[Cost/Price, Design Constraint, Memory Storage, Performance, Physical Power Consumption, Reliability, Safety, Security, Standard Compliance, Usability]
Rationale	[Rationale, the *why* behind this requirement]

R-F-WP6-001	**Modelling of standards**
Description	The Assurance tool shall be able to model a set of industrial standards (including the parts, objectives, practices, goals/requirements, applicability and security levels from the standards). The tool shall be able to model: - Activity applicability and requirement applicability in the context of a standard modelling, - Description of requirement coverage, - Capture specific safety normative constraints/objectives - Description of privacy assurance processes - Description of privacy analysis techniques - Description of privacy requirements - Capability of modelling processes, activities, requirements and roles - Capability of modelling the order in which activities should be performed
Relation to other requirements	
Actor	Standards' Expert, Method engineer

Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	Standards are composed of hundreds of pages and usually contain thousands of requirements. To be compliant with the standards, manufacturers/suppliers must fulfil the requirements. By digitalizing the information/requirements contained in the standards in a common format (which can be retrieved, elaborated, and stored), compliance management becomes easier since the fulfilment becomes traceable. Stakeholder need: Facilitate the visualization and management of standards-related information/requirements

R-F-WP6-002	**Integrate standards models**
Description	The Assurance tool shall enable to integrate existing models with reference information (referenceFramework)
Relation to other requirements	R-F-WP6-001, R-F-WP6-003
Actor	Standards' Expert, Method engineer
Priority	Should have
Type	Functional
Non-functional category	N/A
Rationale	Different regulations and recommendations should be taken into account: GDPR, the company’s best practices, codes of conduct, implementation standards

R-F-WP6-003	**Tailoring of Standards models to specific projects**
Description	The tool shall enable the tailoring of GDPR to specific project/company needs (e.g., by establishing the parts of the Standard that apply to a given assurance project). The tool should be adapted to different domains and company types
Relation to other requirements	R-F-WP6-001, R-F-WP6-002
Actor	Assurance Manager
Priority	Must
Type	Functional
Non-functional category	N/A
Rationale	In order to get the certificate from certification bodies, a two-stage certification process is typically adopted. First, manufacturers/suppliers have to illustrate how, within their specific project, they plan to comply with the requirements included in the standards. This is a very demanding task as applicants usually have to negotiate their interpretation.

	Stakeholder need: To facilitate the specification of how to comply with a standard in a specific project.

R-F-WP6-004	**Compliance Monitoring**
Description	The tool shall support monitoring of compliance status to be filtered by any custom criteria at any time of the development process
Relation to other requirements	R-F-WP6-001
Actor	Project manager, Assurance Assessor
Priority	Must
Type	Functional
Non-functional category	N/A
Rationale	Standards may consist of hundreds of pages and applicants typically have to show compliance with thousands of requirements contained in them. Additionally, project assurance is usually a collaborative task and information should be at disposal for interested parties. Stakeholder need: To control compliance status.

R-F-WP6-005	**Compliance Status to Externals**
Description	The Assurance tool shall enable the export in a human-readable format the compliance status report in order to allow external users (e.g. DPO) to get a (read-only) view of it.
Relation to other requirements	R-F-WP6-004
Actor	Assurance Manager, Assurance Assessor
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	In order for a system to get the approval for operation, a compliance status report should be generated. Due to the complexity of the standards-related practice, having the possibility of filtering by any custom criteria will facilitate the work of the assessor or any other interested user. Stakeholder need: To reduce cost and time in the certification process.

R-F-WP6-006	**Compliance metrics**
Description	The tool shall be able to calculate/estimate compliance metrics of a specific standard
Relation to other requirements	R-F-WP6-004
Actor	Project Manager
Priority	Could have
Type	Functional

Non-functional category	N.A.
Rationale	In order to have a better knowledge of the compliance effort, some metrics should be created and show to the responsible.

R-NF-WP6-007	**Adapt language**
Description	Possibility to adapt the language to the different domains (energy or automotive)
Relation to other requirements	
Actor	N.A:
Priority	Could have
Type	Non-functional
Non-functional category	Usability
Rationale	In some cases, the language could differ depending on the domain working. There should be a way to adapt the tool to the different domains.

R-F-WP6-008	**Assurance case edition**
Description	The system shall be able to create arguments for an assurance case in a scalable way. Particularly, the tool should be able to: - Support different types of safety arguments - Describe of privacy claims, assumptions, context and evidence - Characterize assurance argument modules - Support modular assurance case concepts - Characterize assurance case module interfaces - Characterize s assurance case assumptions - Characterize assurance case contexts - Characterize other relevant aspects of assurance case modules interfaces - Describe the concepts related to privacy-threats directed arguments
Relation to other requirements	
Actor	Assurance Engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	Scalable editing of an assurance case. Stakeholder need: Working efficiently and effectively.

R-F-WP6-009	**Drag and drop argumentation patterns**
Description	The system shall be able to instantiate for the current assurance case an argument pattern (concerning privacy) selected from a list of patterns.

Relation to other requirements	R-F-WP6-008
Actor	Assurance Engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	Easy drag and drop selection from the list of stored patterns. Stakeholder need: Working efficiently and effectively.

R-F-WP6-010	**Provide guidelines for argumentation patterns**
Description	The system should be able to provide guidelines to use and instantiate argument patterns (concerning privacy and security) presented in the current assurance case.
Relation to other requirements	R-F-WP6-009
Actor	Assurance Engineer
Priority	Should have
Type	Functional
Non-functional category	N.A.
Rationale	Providing guidelines for argumentation patterns ensures they are used correctly, and the understanding is shared by all stakeholders. Stakeholder need: Working efficiently and effectively.

R-F-WP6-011	**Organize patterns**
Description	Possibility to categorize, organize, hierarchised the argument patterns
Relation to other requirements	R-F-WP6-009
Actor	Assurance Manager, Assurance Engineer
Priority	Should have
Type	Functional
Non-functional category	N.A.
Rationale	As a guide, the pattern organization could help the user to identify the most adequate pattern in each situation.

R-F-WP6-012	**Semi-automatic generation of product arguments**
Description	The system should reduce efforts of creating product-based assurance case arguments manually. This could be done by enabling semi-automatic generation of product-based arguments-fragments. For each control an argument pattern should be associated and used when the control is used

Relation to other requirements	R-F-WP6-008, R-F-WP6-009
Actor	Assurance Engineer
Priority	Should have
Type	Functional
Non-functional category	N.A.
Rationale	Reducing efforts of manual creation of product arguments. Stakeholder need: Working efficiently and effectively.

R-F-WP6-013	**Semi-automatic generation of process arguments**
Description	The system should be able to semi-automatic generate fragments of an assurance case for process arguments based on the process followed to develop a component/system. Automatically generation of argument fragments based on a standard model instantiation (Activities and requirements are claims, artefacts are evidences and evidences should support the associated constraint requirements of the referenced artefact
Relation to other requirements	R-F-WP6-008, R-F-WP6-009, R-F-WP6-003
Actor	Assurance Engineer
Priority	Should have
Type	Functional
Non-functional category	N.A.
Rationale	Reducing efforts of manual creation of process arguments. Stakeholder need: Working efficiently and effectively

R-F-WP6-014	**Link Evidences**
Description	The tool shall enable to link artefacts (URI) as evidence
Relation to other requirements	
Actor	Assurance Engineer, Assurance Assessor (DPO)
Priority	Must
Type	Functional
Non-functional category	
Rationale	Evidence artefact used to support a claim should be accessible when reviewing an assurance case

R-F-WP6-015	**Useful Feedback Upon Violations**
Description	The tool shall enable assurance managers/DPO to have more information on the possible causes of violations of requirements not just only the YES/NO type answer. This information (read-only) shall be provided in the compliance status report.

Relation to other requirements	R-F-WP6-008
Actor	Assurance Manager, Assurance Assessor
Priority	Should
Type	Functional
Non-functional category	N.A.
Rationale	The localization of problematic parts of the processes where violations have occurred can provide support in taking corrective measures. However, a binary decision on whether the process is compliant or not (YES/ NO Type answer) is not sufficient. Whenever there is a violation of the requirements, an explanation of the (possible) causes must be reported to the users. Such reports must be in a format that non-technical people can understand. Besides, violation explanation can provide pointers to quickly rectify potential non-compliance issues.

R-F-WP6-016	**Compliance map generation from argument evidences**
Description	The system should be able to detect when a claim about a requirement from a standard (compliance claim) is supported by an evidence and generate the compliance indicator in a transparent way.
Relation to other requirements	R-F-WP6-014
Actor	Assurance Manager, DPO
Priority	Should have
Type	Functional
Non-functional category	N.A.
Rationale	To demonstrate compliance, manufacturers/suppliers must show that they have fulfilled the requirements. This can be illustrated via compliance maps (matrix)[1] or argumentation. Stakeholder need: To show compliance of development process with lifecycles depicted in standards

R-F-WP6-017	**Capability to capture conflicts occurring during system development and the trade-off process**
Description	The system shall provide the capability for modelling an assurance case which captures the conflicts that occur during system development and the trade-off process to justify why the taken design decisions are the most optimal ones.
Relation to other requirements	R-F-WP6-008
Actor	Assurance Engineer, Assurance manager, Assurance Assessor
Priority	Must
Type	Functional

[1] Design Requirements Compliance Matrix https://hanford.gov/tocpmm/files.cfm/TFC-ENG-DESIGN-C-42.pdf

Non-functional category	N.A.
Rationale	Capture conflicts occurring during system development and the trade-off process. Stakeholder need: Working efficiently and effectively.

R-F-WP6-018	**Evidence characteristics specification**
Description	The Tool shall allow an assurance engineer to specify the characteristics of assurance evidence. The user is able to view all the inventory of every piece of evidence, like evidence characterization, but also information like name, time stamp of creation, etc
Relation to other requirements	
Actor	Project Manager, assurance engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	The characteristics of the artefacts used as assurance evidence must be recorded for system developed assurance and certification purposes.

R-F-WP6-019	**Evidence traceability**
Description	The Tool shall allow an assurance engineer to specify relationships between evidence artefacts.
Relation to other requirements	R-F-WP6-018
Actor	Assurance engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	Relationships between evidence artefacts might have to be recorded for several purposes, e.g. impact analysis and certification.

R-F-WP6-020	**Evidence evaluation**
Description	The Tool shall allow an assurance manager/ engineer to specify information about the results from evaluating an evidence artefact.
Relation to other requirements	R-F-WP6-018
Actor	Project Manager, Assurance Engineer
Priority	Must
Type	Functional
Non-functional category	N.A.

Rationale	It can be necessary to evaluate the properties and quality of evidence artefacts (e.g. completeness and consistency).

R-F-WP6-021	**Evidence lifecycle information storage**
Description	The Tool shall allow an assurance engineer to specify the events that have occurred during the lifecycle of an evidence artefact.
Relation to other requirements	R-F-WP6-018, R-F-WP6-020
Actor	Assurance Engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	It can be necessary to keep track of all the events occurred during an evidence artefact's lifecycle.

R-F-WP6-022	**Interactive evidence-change impact analysis**
Description	The Tool could allow an assurance manager to indicate which evidence artefacts are actually impacted by the changes to a given evidence artefact.
Relation to other requirements	"R-F-WP6-018, R-F-WP6-019, "
Actor	Assurance Manager
Priority	Could have
Type	Functional
Non-functional category	N.A.
Rationale	A user should not only know what evidence artefacts are impacted by changes in another artefact, but also select what evidence artefact are actually impacted.

R-F-WP6-023	**Evidence resource specification**
Description	The Tool shall allow an assurance engineer to indicate the location of the resource that an evidence artefact represents in the system.
Relation to other requirements	R-F-WP6-018, R-F-WP6-014
Actor	Assurance engineer
Priority	Must
Type	Functional
Non-functional category	N.A.
Rationale	Evidence artefacts are usually stored physically and originally in some external resource.

R-F-WP6-024	Evidence report generation
Description	The Tool could be able to automatically generate reports, checklists, and evidence for certification purposes.
Relation to other requirements	R-F-WP6-018, R-F-WP6-004, R-F-WP6-005
Actor	Project Manager, Assurance assessor (DPO)
Priority	Could have
Type	Functional
Non-functional category	N.A.
Rationale	The project manager or the DPO could have a ready to read report with the status of project in relation with the standard compliance

R-F-WP6-025	Evidence validation
Description	The tool could connect to external tools by an extension point to provide automatic validations of evidences
Relation to other requirements	
Actor	
Priority	Could have
Type	Non-Functional
Non-functional category	Usability
Rationale	It is interesting for the user perspective and for the tool vendors as stakeholders to connect the assurance tool with other tools

R-F-WP6-026	Manage project
Description	The tool shall enable the user to navigate and edit the project assets and even delete the project if it is no longer necessary
Relation to other requirements	R-F-WP6-003
Actor	Assurance Manager
Priority	Must
Type	Functional
Non-functional category	N/A
Rationale	Stakeholder need: To facilitate the specification of how to comply with a standard in a specific project.

R-F-WP6-027	Navigate through the project repository
Description	The tool shall enable the user to navigate through the company’s project repository to browse what has been done in previous and/or current projects

Relation to other requirements	R-F-WP6-026
Actor	Assurance Manager, DPO
Priority	Must
Type	Functional
Non-functional category	N/A
Rationale	Stakeholder need: To facilitate the specification of how to comply with a standard in a specific project.

5 Design

5.1 Use cases

5.1.1 Reference Framework Management

The uses cases for the Reference Framework Management functional block include functionality about how information of standards is captured and managed and monitored in the context of an assurance project. The tool should provide to the Assurance Manager the mechanisms to model all the information that is contained in a standard including the life-cycle defined on it, requirements and recommendations.

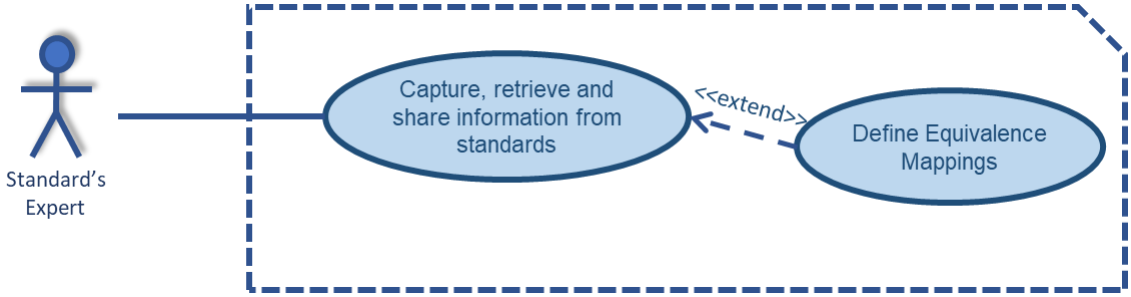

Figure 3 Use cases on compliance management

Use Case	**Capture information from standards**
Functionality Description	The system should be able to retrieve, digitalize and store a set of norms, recommendations, standards, or quality models.
Actors	Assurance Manager
Assumptions/ Preconditions	A metamodel shall allow the structuration of standard information. The actor has deep knowledge about the standards. The standard's information shall be always available in the platform (except if it is explicitly dropped).
Post-conditions	None so far
Steps	1. The user creates a new standard model and specifies the characteristics that define the standard 2. The user structures/categorizes the standard by parts, objectives, activities, practices, goals and requirements 3. The user describes the parts, objectives, activities, practices, goals and requirements contained in the standard.
Variations	# The user extends the standard interpretation by defining a project baseline. # From the baseline, the system is able to generate argument fragments for the assurance case in relation with process-based argumentation.
Exceptions	None so far
Non-functional	
Requirements	R-F-WP6-001, R-NF-WP6-007
Related use cases	

Table 1 Use case "Capture information from standards".

Use Case	**Define Equivalence Mappings**
Functionality Description	Mapping of model elements from different Ref. Frameworks. A Ref. Framework model can represent either a Standards/Rules/Regulations model or a Company-Specific Process Definition model. Mapping can occur at these levels: 1. Between a process definition and a standard, either while it is being developed, of afterwards, to analyse or demonstrate compliance. 2. Between two processes or two standards, to analyse equivalence or to derive a new one from an existing one.
Actors	Standards Expert
Assumptions/ Precondition	The main experts from a company must define a procedure to create interpretations of mappings
Post-conditions	None
Steps	1. Browse the Source and Target Ref. Framework models 2. Create map links between model elements of the source and target Ref. Frameworks. 3. Edit the map information, including coverage, conditions, justifications, etc.
Variations	None
Non-functional	None
Requirements	R-F-WP6-002, R-NF-WP6-007
Related use cases	Capture Information from standards Define Assurance Project Baseline

Table 2 Use case "Define equivalence mappings".

5.1.2 Assurance Project Management

This functionality block makes possible the management of the assurance project, which implies the modelling of the baseline work compliance.

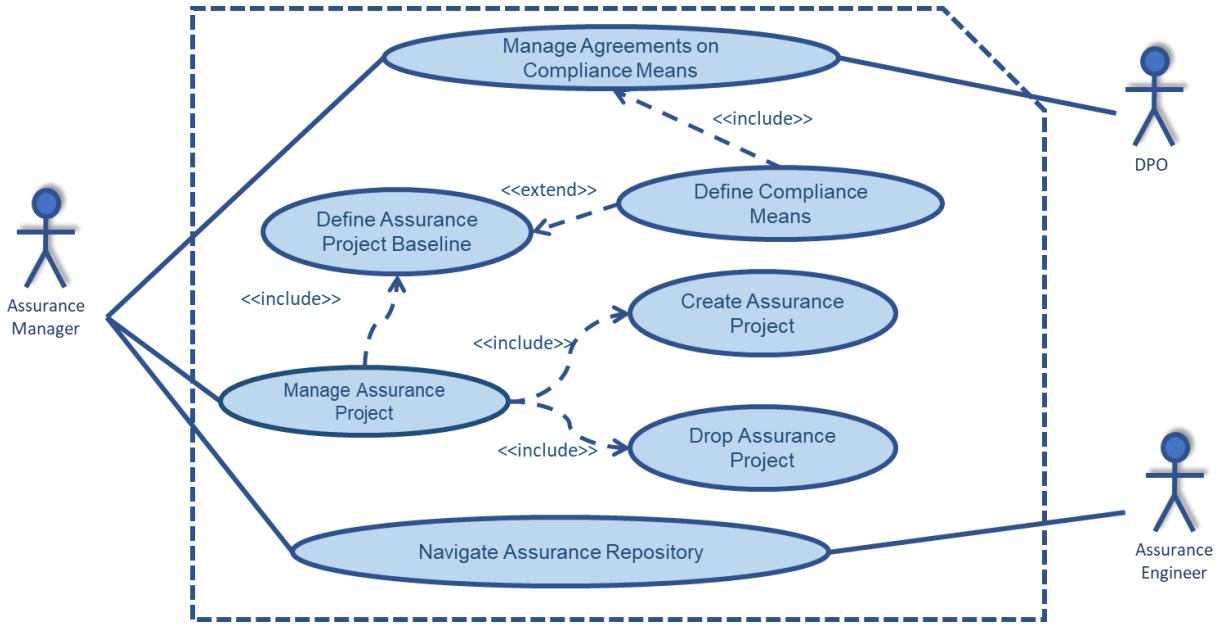

Figure 4 Use cases on Assurance Project Management

Use Case	**Manage an Assurance Project**
Functionality Description	The system should be able to create, modify and drop assurance information from a specific project through the project lifecycle.
Actors	Assurance Manager, Assurance Assessor
Assumptions/ Preconditions	A model containing information from the standard shall be available in the platform.
Post-conditions	The user shall continue with the specification with the rest of the modules. The user is able to assign profiles to the different users of the assurance project.
Steps	1. The user creates a new assurance project 2. The user specifies the baseline in association with a standard which will be followed in the project 3. The user specifies the compliance maps/links though the project lifecycle.
Variations	# The user imports previous assurance project information.
Exceptions	None so far
Non-functional	
Requirements	R-F-WP6-003
Related use cases	Create Assurance Project Drop Assurance Project Define Assurance Project Baseline

Table 3 Use case "Manage an assurance project".

Use Case	**Create Assurance Project**
Functionality Description	The system should allow users to create a kind of “container” for the whole information related to a given safety assurance project.
Actors	Assurance Manager

Assumptions/ Preconditions	General Information about the project must be available: general timing, responsible person in the system, client, product and type of product under assurance, etc.
Post-conditions	None
Steps	1. Create a new project defining any dependency with other projects 2. Specify general project information (general timing, responsible person in the system, client, product and type of product under assurance, etc.)
Variations	
Exceptions	None
Non-functional	None
Requirements	R-F-WP6-003, R-F-WP6-026
Related use cases	Drop Assurance Project Manage Assurance Project

Table 4 Use case "Create assurance project".

Use Case	**Drop Assurance Project**
Functionality Description	The system should allow the user to delete the whole information related to a given assurance project.
Actors	Assurance Manager
Assumptions/ Preconditions	The assurance project has already been created and the information is no longer valid.
Post-conditions	None
Steps	1. Select an existing assurance project 2. Delete all the models, diagrams and information stored under the assurance project structure
Variations	
Exceptions	None
Non-functional	The tool should be available to let the user do more actions in less than 1 minute
Requirements	R-F-WP6-003, R-F-WP6-026
Related use cases	Manage an Assurance Project Create Assurance Project

Table 5 Use case "Drop assurance project".

Use Case	**Define Assurance Project Baseline**
Functionality Description	The system should allow users to define a technical information baseline about a given project, including, standards scope, compliance means, and justifications on any project decisions of company process tailoring.
Actors	Assurance Manager
Assumptions / Preconditions	Technical information about the project must be available: project plans, dependability/safety/certification plans, standards scope, and means of compliance (agreed with authorities. The assurance project has already been created.
Post-conditions	None
Steps	1. Define project structure (into sub-projects if needed).

	2. Define the scope of standards for this project (phases, activities, etc.) and/or sub-projects if needed. 3. Define the compliance means (evidence to be presented for compliance) 4. Specify any justification on compliance means
Variations	#Import an assurance project: the system lets the user import the information for this use case, from an external file created with the process editor.
Exceptions	None
Non-functional	None
Requirements	R-F-WP6-004
Related use cases	Manage an Assurance Project Manage Agreements on compliance means Define Compliance Means

Table 6 Use Case "Define Assurance Project Baseline".

Use Case	**Navigate Assurance repository**
Functionality Description	The system should allow users to navigate along the assurance project repository.
Actors	Assurance Manager
Assumptions / Preconditions	The assurance project repository previously exists.
Post-conditions	None
Steps	1. Open the Assurance Project. 2. Navigate through the different assurance project elements.
Variations	None
Exceptions	None
Non-functional	
Requirements	R-F-WP6-027
Related use cases	Manage Assurance Project

Table 7 Use Case "Navigate Assurance repository".

Use Case	**Manage Agreements on compliance means**
Functionality Description	The tool should allow both Assurance Manager and DPO to explicitly identify and indicate the set of evidences that shall be provided for a compliance for the assurance project. Such a set of evidences must correspond to those identified in the project baseline (standards scope for this project).
Actors	Assurance Manager and DPO
Assumptions / Preconditions	At the beginning of the assurance project before starting the artifact collection
Post-conditions	
Steps	1. In the project baseline select the artefacts that will be required. 2. Indicate the justification for not selecting specific artefacts and the selection of the others 3. If needed, add new artefacts together with the justification for that specific project.
Variations	

Exceptions	
Non-functional	
Requirements	R-F-WP6-003
Related use cases	Capture information from standards Define Compliance Means Report on Assurance Assessment

Table 8 Use case "Manage agreements on compliance means".

Use Case	**Define Compliance Means**
Functionality Description	The compliance mapping is the mechanism the system has to indicate that an asset (an activity of the process, a requirement, an analysis…) has been executed as mean for compliance with part of what it is requested in a standard or regulation.
Actors	Assurance Manager
Assumptions / Preconditions	None
Post-conditions	None
Steps	1. The user selects the artefacts in the project baseline. Create map links between model elements of the source and target. 2. The user maps the artefacts with the specific artefacts 3. Edit the map information, including coverage, conditions, justifications, etc.
Variations	None
Exceptions	None
Non-functional	
Requirements	R-F-WP6-007
Related use cases	Manage Agreements on compliance means Capture information from standards Monitor Status of Assurance project Report on Assurance Assessment

Table 9 Use case "Define Compliance means".

5.1.3 Assurance Case Management

This functional block manages argumentation information in a modular fashion. It also includes mechanisms to support assurance patterns management.

Assurance cases are a structured form of an argument that specifies convincing justification that a system is adequately dependable for a given application in a given environment. Assurance cases are modelled as connections between claims and their evidence.

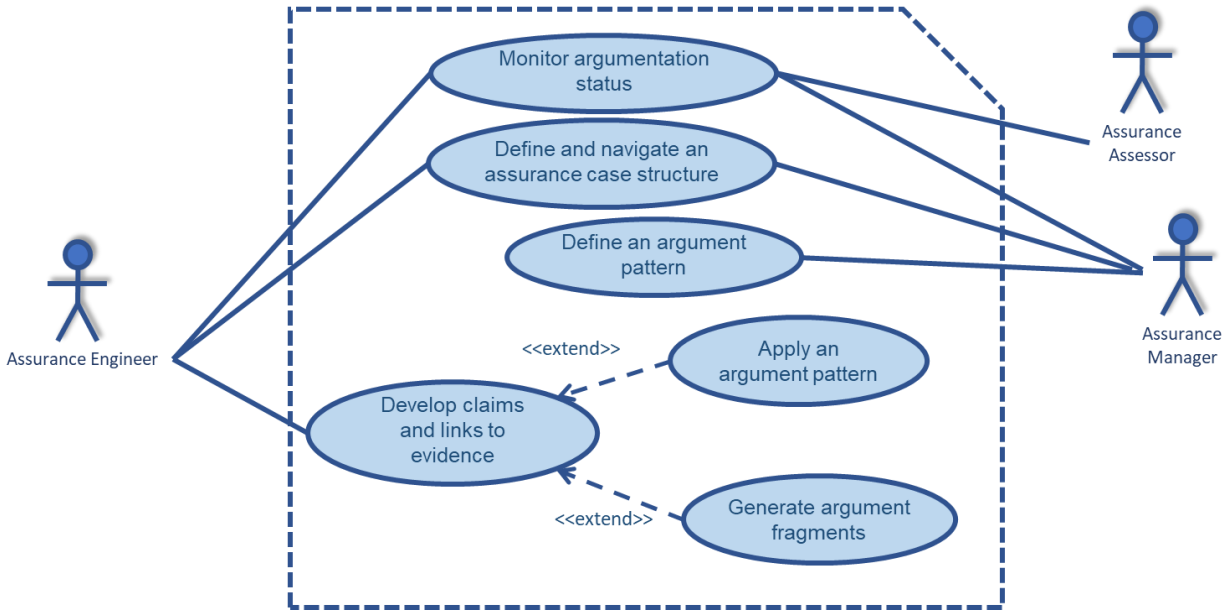

Figure 5 Use cases on Assurance Case Management

Use Case	**Monitor Argumentation Status**
Description	At any time in the development the actor can browse the assurance case diagram and query assurance case progress and particular aspects such as undeveloped goals
Actors	Assurance Engineer, Assurance Manager, Assurance Assessor
Assumptions	
Pre-conditions	The assurance case has already been created and at least the argumentation skeleton has been defined
Post-conditions	
Steps	1. The user will select the assurance case diagram to monitor from the assurance projects “repository”. 2. The user browses the argumentation contained in the selected diagram
Variations	
Non-functional	N.A.
Requirements	R-F-WP6-004, R-F-WP6-008, R-F-WP6-015, R-F-WP6-017
Related use cases	Define and navigate an assurance case structure

Table 10 Use Case "Monitor argumentation status".

Use Case	**Define and navigate an assurance case structure**
Description	The actor aims to use the assurance case skeleton as the basis for assurance accountability justification. This use case corresponds to the scenario to define an integrated and structured assurance case where the actor can navigate through the structure.
Actors	Assurance Manager, Assurance Engineer

Assumptions	We have different levels of argumentation abstraction.
Pre-conditions	None
Post-conditions	The assurance structure for a given project has been detailed.
Steps	1. The user should create an argumentation diagram 2. In an argumentation diagram the user will: a. Define the appropriate granularity by using argument patterns and modules to encapsulate arguments b. Inside each argument module include appropriate arguments taking into account: hazard mitigation, requirements, integration, etc.
Variations	
Non-functional	None
Requirements	R-F-WP6-008
Related use cases	

Table 11 Use Case "Define and navigate an assurance case structure".

Use Case	**Develop claims and links to evidence**
Description	The system should help users to identify and define the most appropriate arguments and evidence to support their goals.
Actors	Assurance Engineer
Assumptions	The actor uses guidelines and support to apply the best practices to develop the statements of argument structures.
Pre-conditions	The current argumentation module has been created. The pieces of evidence addressed by the current project have been established.
Post-conditions	The current Argumentation Module is completely defined.
Steps	For every argument module: 1. Specify manually the claims set 2. Provide stated and valid assumptions applied to the claims 3. Map to the available pieces of evidence that support the claims 4. Specify contextual information to define or constraint the scope over which the arguments are assumed to be valid 5. When required, map claims (away goals) to the external claims (public goals) that support to (in other argument modules)
Variations	# Reuse and argument module (Import additional pieces of argumentation set) from an external file # Select the option of generate argument fragments based on external inputs either on the process or on the product risks # Select an argument pattern to substantiate or address particular claims
Non-functional	None
Requirements	R-F-WP6-008, R-F-WP6-014

Related use cases	

Table 12 Use case "Develop Claims and Links to Evidence".

Use Case	**Define an argument pattern**
Description	The tool should be able to support the Assurance manager to encapsulate the best practices on argumentation in argument patterns and categorizes based on predefined criteria
Actors	Assurance Manager
Assumptions	
Pre-conditions	
Post-conditions	The pattern is accessible to be used in the library of patterns Provide guidelines to use and instantiate argument pattern
Steps	1. The user creates an argument diagram 2. Creates a set of claims, context and evidences 3. Identify Pattern parameters to be defined when the pattern is instanced 4. Classifies the pattern
Variations	None
Non-functional	The pattern should be stored in a place accessible for the assurance engineers.
Requirements	R-F-WP6-009, R-F-WP6-010, R-F-WP6-011
Related use cases	Develop claims and links to evidence Apply an argument pattern

Table 13 Use case "Define an argument pattern".

Use Case	**Apply an argument pattern**
Description	This use case corresponds to the capability to instantiate an argument pattern selected from the list of stored patterns.
Actors	Assurance Engineer
Assumptions	Assurance patterns have been specified and stored
Pre-conditions	The assurance argumentation is under edition.
Post-conditions	Changes are registered
Steps	1. Library of patterns is available to be used in a specific assurance case model 2. Drag and drop argument pattern into the desired diagram of assurance case 3. Pattern parameters must be defined by the user
Variations	None
Non-functional	None
Requirements	R-F-WP6-009, R-F-WP6-010, R-F-WP6-011
Related use cases	Develop claims and links to evidence Define an argument pattern

Table 14 Use case "Apply an argument pattern".

Use Case	**Semi-automatic generation of product arguments**
Functionality Description	The tool shall enable semi-automatic generation of product-based argument-fragments based on the controls selected to mitigate identified risks. Details on the generation of the argument fragments are given in deliverable D6.4[10].
Actors	Assurance Engineer
Assumptions	
Post-conditions	None
Steps	1. The user selects the "Generate argumentation fragments" functionality 2. The user selects either new or existing assurance project as the destination for the argument-fragments 3. The tool validates the system model and extracts the information needed for the argument-fragment generation for each component 4. The tool generates the corresponding argument-fragments and notifies the user of their location.
Variations	None
Non-functional	None
Requirements	R-F-WP6-012
Related use cases	Develop claims and links to evidence

Table 15 Use case "Semi-automatic generation of product arguments".

Use Case	**Automatic generation of process arguments**
Functionality Description	The tool shall enable automatic generation of process-based argument-fragments based on the process implicit in the GDPR compliance. Details on the generation of the argument fragments are given in deliverable D6.4[10].
Actors	Safety Engineer, Security Engineer
Assumptions	A process model has been specified.
Post-conditions	None
Steps	1. The user selects the "Generate argumentation fragments" functionality. 2. The user selects either new or existing assurance project as the destination for the argument-fragments. 3. The information needed for the argument-fragment generation is extracted from the process model. 4. The corresponding argument-fragments are generated; the location is notified to the user.
Variations	None
Non-functional	None
Requirements	R-F-WP6-013, R-F-WP6-016
Related use cases	Develop claims and links to evidence Semi-automatic generation of product arguments

Table 16 Use case "Automatic generation of process arguments"

5.1.4 Evidence Management

This functional block manages basic aspects related to the specification of information related to those artefacts that can be (or are) used as assurance evidence in an assurance project. Such artefacts can have specific properties (e.g. the result of a test case) and be stored in external data sources as data bases and by using external tools or be generated by tools developed in the other work packages.

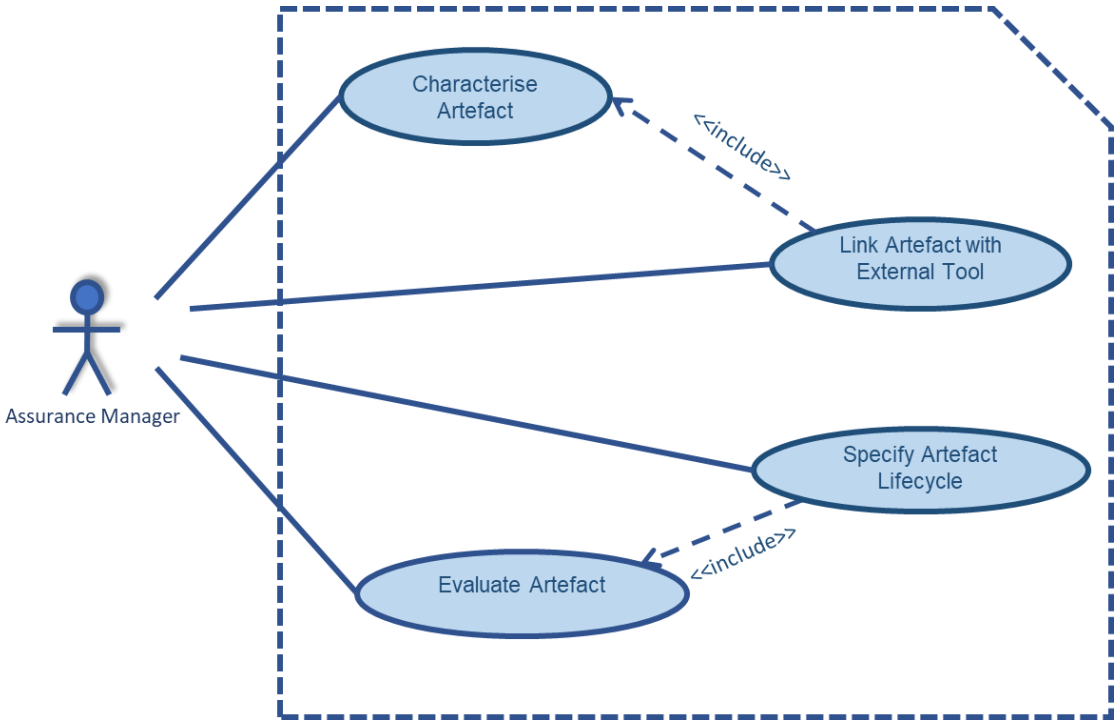

Figure 6 Use cases on Evidence Management

Use Case	**Characterise Artefact**
Functionality Description	The tool shall allow an Assurance Engineer to specify the characteristics of assurance evidence.
Actors	Assurance Engineer
Assumptions	An Artefact Definition has been created
Post-conditions	The characteristics of the Artefact are shown.
Steps	1. The Assurance Engineer creates an Artefact for an Artefact Definition. 2. The Assurance Engineer specifies the information of the Artefact.
Variations	# The Assurance Engineer adds Artefact Properties # The Assurance Engineer adds sub-artefacts to the Artefact # The Assurance Engineer indicates the precedent version of the Artefact # The Assurance Engineer executes 'Link Artefact with External Tool'
Non-functional	None
Requirements	R-F-WP6-018
Related use cases	

Table 17 Use case "Characterise Artefact"

Use Case	**Link Artefact with External Tool**
Functionality Description	The system shall: (1) be able to import evidence information; (2) allow an Assurance Engineer to indicate the location of the resource that an evidence artefact represents in the system.
Actors	Assurance Engineer
Assumptions	An Artefact has been created
Post-conditions	The link with the external tool is stored in the tool
Steps	1. The Assurance Engineer selects an Artefact 2. The Assurance Engineer adds a Resource to the Artefact 3. The Assurance Engineer specifies the information about an External Tool in the Resource
Variations	# The tool retrieves data from the external tool
Non-functional	The tool will connect to the external tool in less than 2 seconds
Requirements	R-F-WP6-023
Related use cases	Characterise Artefact

Table 18 Use case "Link Artefact with External Tool".

Use Case	**Specify Artefact Lifecycle**
Functionality Description	The tool shall allow an Assurance Engineer to specify the events that have occurred during the lifecycle of an evidence artefact.
Actors	Assurance Engineer
Assumptions	An Artefact has been created
Post-conditions	The Artefact Lifecycle is shown.
Steps	1. The Assurance Engineer selects an Artefact 2. The Assurance Engineer adds an Artefact Event to the Managed Artefact 3. The Assurance Engineer indicates the Event Kind of the Artefact Event
Variations	# When an Artefact is linked with an external tool, the lifecycle of the Artefact could be retrieved from the external tool (e.g., the modifications events of the Artefact could be determined from a SVN log). # The Assurance Engineer executes 'Evaluate Artefact'.
Non-functional	None
Requirements	R-F-WP6-021
Related use cases	Characterise Artefact

Table 19 Use case "Specify Artefact Lifecycle".

Use Case	**Evaluate Artefact**
Functionality Description	The tool shall allow an Assurance Engineer to specify information about the results from evaluating an evidence artefact.

Actors	Assurance Engineer
Assumptions	An Artefact has been created
Post-conditions	The evaluation information is shown
Steps	1. The Assurance Engineer selects an Artefact 2. The Assurance Engineer adds an Artefact Evaluation to the Artefact 3. The Assurance Engineer specifies the information of the Artefact Evaluation.
Variations	# The Assurance Engineer associates the Artefact Evaluation with an Artefact Event
Non-functional	None
Requirements	R-F-WP6-020
Related use cases	Specify Artefact Lifecycle

Table 20 Use case "Evaluate Artefact".

5.1.5 Assurance Reporting

The monitoring of the assurance project will be provided by this functionality block. For this prototype, the monitoring will be performed by showing the compliance result on a dashboard.

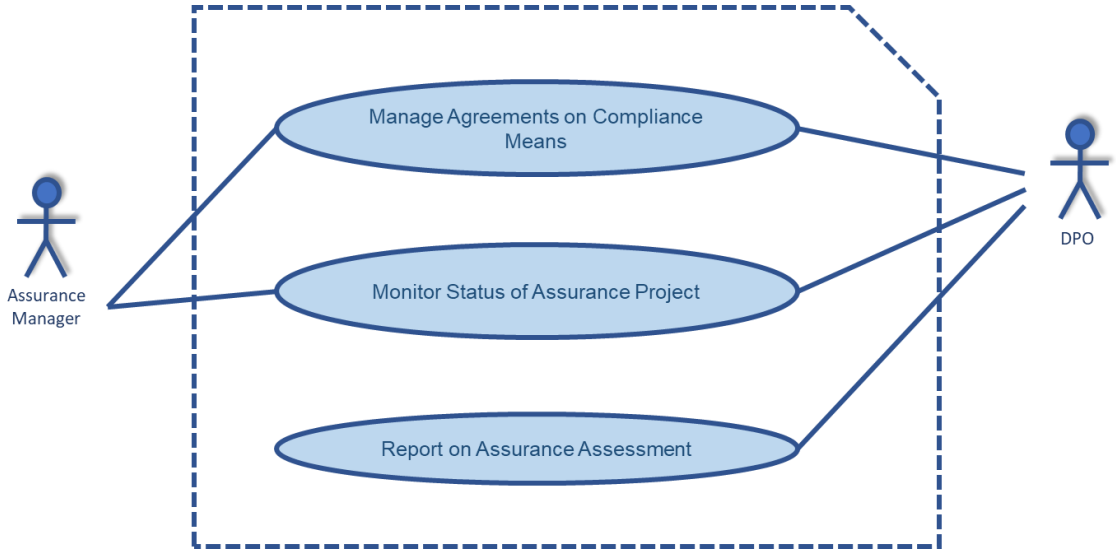

Figure 7 Use cases on Assurance Reporting

Use Case	**Monitor status of assurance project**
Functionality Description	The system should provide information about the progress of the assurance activities in relation with the corresponding plan
Actors	Assurance Manager, Assurance Assessor (DPO)
Assumptions / Preconditions	An assurance project and a project baseline have been specified
Post-conditions	
Steps	1. The user selects the assurance project 2. From a menu, the user asks for the project progress report

	3. A progress report is automatically generated from the different modules' information.
Variations	None so far
Exceptions	
Non-functional	
Requirements	R-F-WP6-004, R-F-WP6-005, R-F-WP6-006
Related use cases	Manage an Assurance Project

Table 21 Use case "Monitor status of assurance project".

Use Case	**Report on assurance assessment**
Functionality Description	The system should be able to provide information about the assurance activities and evidences provided for compliance accountability and the assessment about the project.
Actors	Assurance Manager, Assurance Assessor (DPO)
Assumptions / Preconditions	An assurance project and a project baseline have been specified together with the compliance means
Post-conditions	
Steps	1. The user selects the assurance project 2. From a menu, the user asks for the project progress report 3. A progress report is automatically generated from the different modules' information. 4. The DPO includes its comments and assess the evidences provides
Variations	None so far
Exceptions	
Non-functional	
Requirements	R-F-WP6-004, R-F-WP6-005, R-F-WP6-006
Related use cases	Manage an Assurance Project

Table 22 Use case "Report on assurance assessment".

6 Architecture

The following figure is based in the actual functional decomposition for the OpenCert tool as it is described in deliverable D2.6[11]. The figure shows the areas that will be in the scope of PDP4E and that will be required adaptation to support either functional needs in relation with the GDPR or improvements in relation with performance to increase the actual TRL.

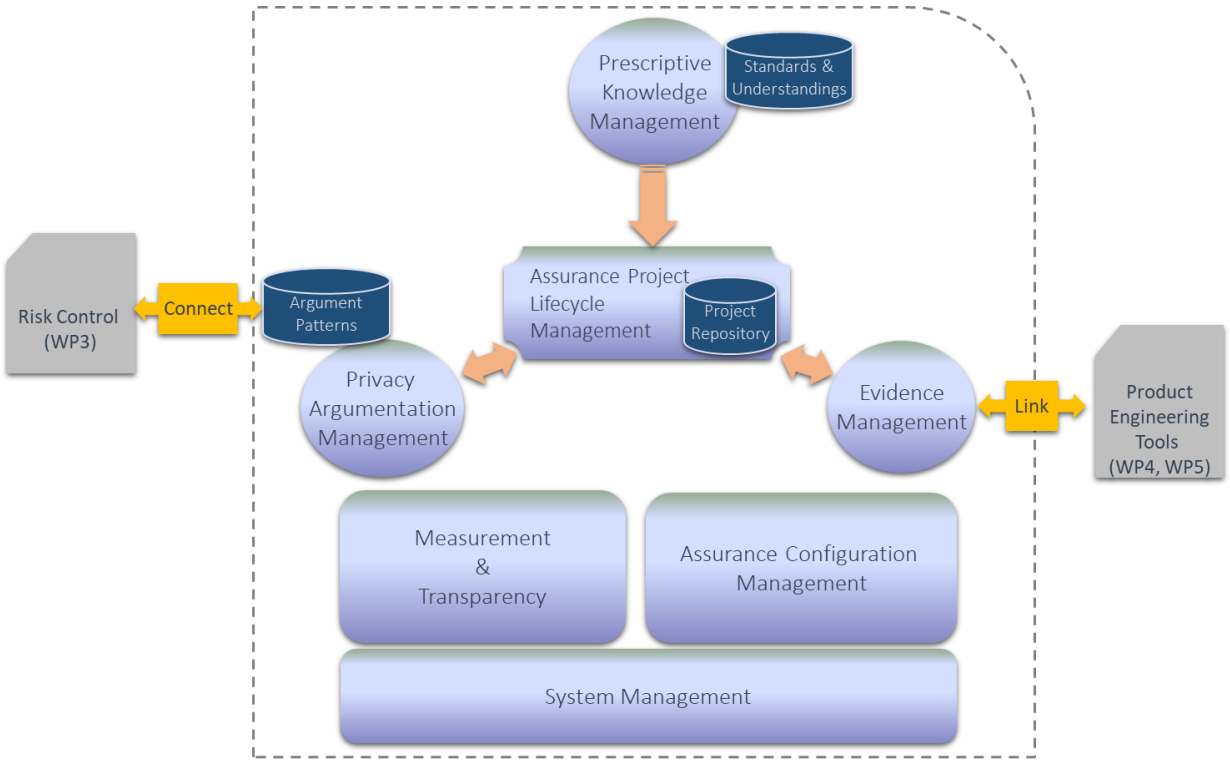

Figure 8 Functional decomposition of Assurance tool

Inside the dashed square in the figure we can see the scope of the assurance tool. Highlighted in yellow there are the connection with the results from other PDP4E technical work packages. In deliverable D6.4 [10] there is a detail explanation on the contents of the information which depends in other technical work packages results.

The assurance tool will ensure the following functionalities:

Prescriptive Knowledge Management: Functionality related to the management of standards information. This functional group maintain a knowledge database about “standards & understandings”. The functionality should be extended so as to be able to deal with GDPR concepts and other privacy related regulation.

Assurance Project Lifecycle Management: This functionality factorizes aspects such as the creation of assurance projects. This module manages a “project repository”, which can be accessed by the other modules. The technology used before will be updated to improve its performance

Privacy Argumentation Management: This group manages argumentation information mainly in safety and will be extended to take into account privacy and security argumentation.

Evidence Management: This module manages the full life-cycle of evidences and evidence chains. It will be extended to connect with other project tools.

Assurance Configuration Management: This is an infrastructure functional module. This functionality needs to be improved its performance.

System Management: It includes generic functionality for data access, reports, etc. This functionality needs to be improved its performance.

Measurement: This module contains functionality which should be extended to include privacy and security measurements.

7 References

[1] D7.2 Innovation and exploitation plan and report, PDP4E Project Deliverable
[2] OpenCert, 2019. Online, https://www.polarsys.org/opencert/ (Accessed June 11th, 2019)
[3] Papyrus, 2019. Online, https://eclipse.org/papyrus/ (Accessed June 11th, 2019)
[4] CHESS, 2019. Online, https://www.polarsys.org/projects/polarsys.chess (Accessed June 11th, 2019)
[5] Eclipse Process Framework Project, 2019. Online, https://eclipse.org/epf/ (Accessed June 11th, 2019)
[6] D2.1 Multi-stakeholder specification; PDP4E Project Deliverable, March 2019
[7] D2.2 Technical Gap Analysis and Synthesis of User Requirements; PDP4E Project Deliverable; March 2019
[8] Clegg, Dai; Barker, Richard (1994). Case Method Fast-Track: A RAD Approach. Addison-Wesley. ISBN 978-0-201-62432-8.
[9] OMG; SACM – Structured Assurance Case Metamodel v2.1, March 2019
[10] D6.4 Assurance methods for data protection and privacy, PDP4E Project Deliverable
[11] D2.6 Overall architecture and methodological framework v1, PDP4E Project Deliverable