Methods and tools for GDPR Compliance through

Privacy and Data Protection 4 Engineering

Specification and design of risk management tools for data protection and privacy

Project: PDP4E
Project Number: 787034
Deliverable: D3.1
Title: Specification and Design of risk management tools for data protection and privacy
Version: v1.0
Date: 15/07/2019
Confidentiality: Public
Author: David Sánchez (TRIALOG),
Victor Muntés-Mulero (BEAWRE),

Funded by

Table of Contents

Document History

Version	Status	Date
V0.01	Table of content structure	25/04/2019
V0.1	First version of the use cases to reflect expectations from a methodological point of view. Main user needs were elicited.	17/05/2019
V0.2	First version of the requirements. Use cases were then modified to reflect functional needs.	19/06/2019
V0.3	Overall refinements to the document. Ready for review.	02/07/2019
V1.0	Version reflecting changes suggested by reviewers.	12/07/2019

Approval		
	Name	**Date**
Prepared	David Sanchez (TRIALOG)	12/07/2019
Reviewed	Gabriel Pedroza (CEA)	09/07/2019
Reviewed	Juan Carlos (UPM)	12/07/2019
Authorised	Antonio Kung	15/07/2019

Circulation	
Recipient	**Date of submission**
Project partners	12/07/2019
European Commission	15/07/year

List of Figures

Abbreviations and Definitions

Abbreviation	Definition
CSPO	Chief Security and Privacy Officer
DFD	Data Flow Diagram
DPIA	Data Protection Impact Assessment

DPO	Data Protection Officer
GDPR	General Data Protection Regulation
PDP4E	Privacy and Data Protection 4 Engineering
PDPbD	Privacy and Data Protection by Design
PIA	Privacy Impact Assessment
ROAM	Resolved, Owned, Accepted, Mitigated
UC	Use Case
WP29	Article 29 Working Party
WP	Work Package

Executive Summary

Objective of the document

The objective of the task 3.2, and this document, is to set the scope of the risk management tool to be developed within the PDP4E project. In particular, this document describes the specification of a tool that shall support actors from diverse background in the co-preparation of a plan to reduce data subjects' risks derived from a data processing system.

Structure of the document

This document starts with a high-level description of the background tools to be considered during the development of the PDP4E risk management tool. Then, Section 2describes the set of users involved in a risk management process and their different responsibilities and needs. Next, Section 3 includes the requirements elicitation for the PDP4E risk management tool, which is completed in Section 4 with the description of the use cases.

Relation with other deliverables

This document is strongly related with deliverables D2.2 "Technical analysis and synthesis of user requirements" [1] and D2.4 "Overall system requirements v1" [2], which have been used as a basis for the elicitation of the requirements in Section 13.

This deliverable has been prepared in parallel to D3.4 "Risk Management Method for data protection and privacy" [3], which describes the methodological aspects of the risk management process, so that both user needs and expectations from a risk-based regulation are reflected in the requirements of the tool.

The development of the PDP4E Risk Management tool will be guided by this document. As the development progresses, and evaluation from external stakeholders is received (see future validation reports D7.6 and D7.7), the specification may be slightly updated as part of deliverables D3.2 and D3.3. In both D3.2 and D3.3, we will cover the progress on the different requirements and use cases.

1 Background on Risk Management

In this section, we describe the state of the practice of the tools used for Risk Management resulting from research projects that have relation with risk management and plans to integrate them in PDP4E.

1.1 MUSA Risk Management

The MUSA Risk Assessment tool proposes a new agile risk analysis framework to facilitate the creation of tools for agile risk management. In particular, the objective of the risk assessment tool was to address the following four challenges [4]:

- Traditional risk analysis practices for software development do not easily translate to Agile.
- Analysis of risks should be continuous.
- Development teams (i.e. scrum teams) do not have enough expertise on risk analysis.
- Tools to manage risk in Agile do not foster collaboration.

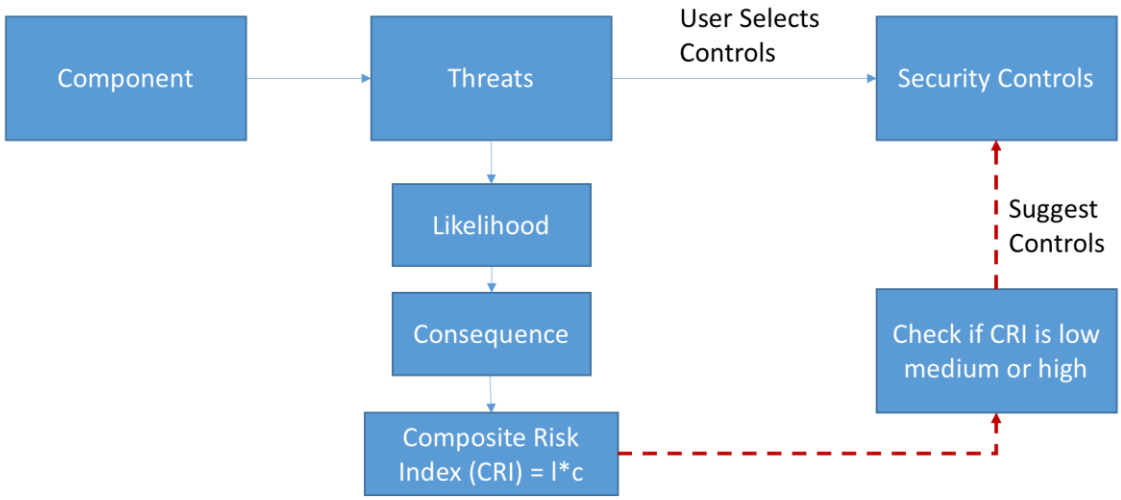


Figure 1 – Outline of Risk Assessment module flow with MUSA framework (Design Time)

MUSA tool uses a pull system in the style of Kanban[1], where the status of each asset with respect to a predefined risk analysis methodology is expressed through the different columns in the Kanban board. This makes the tool agnostic to any specific risk analysis methodology. Nonetheless, we describe here the methodology used by the MUSA Risk Assessment tool.

[1] Kanban boards are formed by cards and columns. Each column represents a stage of the development phase (*Definition*, *Design*, *Development*, *Testing*, *Deployment*), whereas cards represent the different development efforts. Kanban boards are commonly used by agile development teams to track progress of the next team release. The MUSA Risk Management tool reuses such artefact due to its familiarity and popularity between engineering teams, but it shall be depicted as a separated tool.

In order to assess the risks in the different components of a multi-cloud application, the MUSA Risk Assessment module uses a risk model based on the OWASP threat risk modelling[2]. Users choose among the threats that were potentially affecting a particular component of the multi-cloud application, as shown in Figure 1. These threats are chosen from a threat catalogue. Once the threats are selected, they are automatically classified in the security-oriented STRIDE categories (Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege).

Users are required to provide the likelihood and impact of each threat using a set of categorisations-based influencers taken from OWASP approach. The sub-values influencing likelihood are grouped by the type of factors and represented by the value in a scale of 0-9 where 0 represents a very unlikely scenario and 9 represents a very high likelihood of the factor to occur. Similarly, consequences are also assessed by a scale of 0-9 where 0 represent a negligible impact and 9 a significant business impact. When it comes to risks as in the GDPR, consequence shall be measured in terms of negative impact on the data subjects instead of impact on the business.

After risk assessment, risks requiring treatment (high and medium risk level) are identified. NIST provides a mapping that links security controls with risks [5]. Based on this mapping, and the extension done by the MUSA research and innovation project, the required controls are obtained for the risks selected by users. These controls are then suggested to the end-user, but the user is free to extend the choice to all the available security controls if desired.

Users are finally requested to approve acceptance of the level of risk mitigation status. Within the MUSA Risk Assessment tool, we leverage ROAM model risk mitigation classification. ROAM is a common agile management risk mitigation classification and stand for:

- Resolved - the risk has been answered and avoided or eliminated.
- Owned – the risk has been allocated to someone who has responsibility for doing something about it.
- Accepted - the risk has been accepted and it has been agreed that nothing will be done about it.
- Mitigated - action has been taken so the risk has been mitigated, either reducing the likelihood or reducing the impact.

With this framework, the tool created by the MUSA project facilitates translating traditional risk analysis practices for software development to agile software development contexts, allowing for continuous risk analysis and permitting the main stakeholders to collaborate.

1.2 CNIL Privacy Impact Assessment tool

In order to facilitate adoption of the GDPR in data processing organizations, CNIL[3], the French supervisory authority, released a user-friendly tool for conducting Privacy Impact Assessments

[2] Accessible via https://www.owasp.org/index.php/Application_Threat_Modeling. An updated version of the OWASP methodology can be found in https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Threat_Modeling_Cheat_Sheet.md

[3] Commission Nationale de l'Informatique et des Libertés. https://www.cnil.fr

(PIA). This tool puts in practice the PIA methodology that CNIL has been developing since 2015, in parallel to the conception of the GDPR. Following this methodology will ease compliance with not only the GDPR, but also satisfy requirements set by the WP29 Guidelines on Data Protection Impact Assessment [6] adopted in October 2017.

The PIA software tool offers several features facilitating the DPIA process:

- A didactic interface to carry out PIAs, asking relevant questions for assessing compliance with the regulation.
- A knowledge base with information extracted from the GDPR, different DPIA guides and the Security guide published by CNIL.
    - A list of pre-defined privacy and data protection controls are available when defining the planned measures.
    - Risk assessment is built around three common categories of risks: illegitimate access to data, unwanted modifications of information and removal of information.
- Visualization tools designed to ensure understanding of the risks involved with the data processing.

The tool is mainly addressed to data controllers who are slightly familiar with the PIA process. During PDP4E, we plan to show how a Risk Management tool can be built around the CNIL PIA tool for conducting impact assessments in an environment that is not savvy neither in risk management nor on GDPR-compliance.

1.3 LINDDUN

LINDDUN[4] is a privacy threat analysis methodology that integrates 7 main privacy threat categories [7]: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance. The PDP4E Risk Management tool will take LINDDUN as the starting point for risk analysis, as well as STRIDE to cover for those risks related to security that may affect privacy also.

LINDDUN methodology steps are divided in problem space steps (step 1-3), which aim at describing privacy threats, and in solution space steps (step 4-6) necessary for the elicitation of mitigation measures and solutions corresponding to the threats identified. This methodology will be further aligned with those stated by ISO 31000 Risk Management [8], CORAS[5] and ISO/IEC 29134 [9].

[4] LINDDUN privacy threats modelling methodology, Available at: https://linddun.org/linddun.php# Last accessed on 17 April 2019.

[5] http://coras.sourceforge.net/ , being a core part of the methodology used by the MUSA Risk Assessment tool.

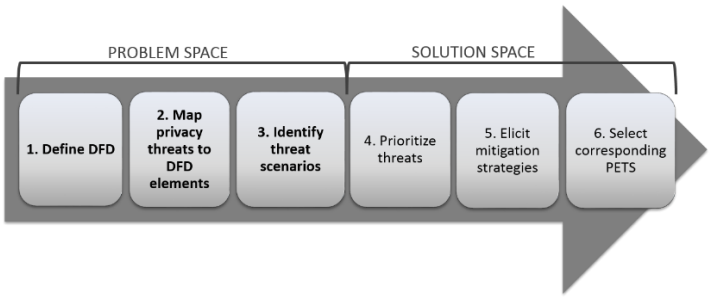


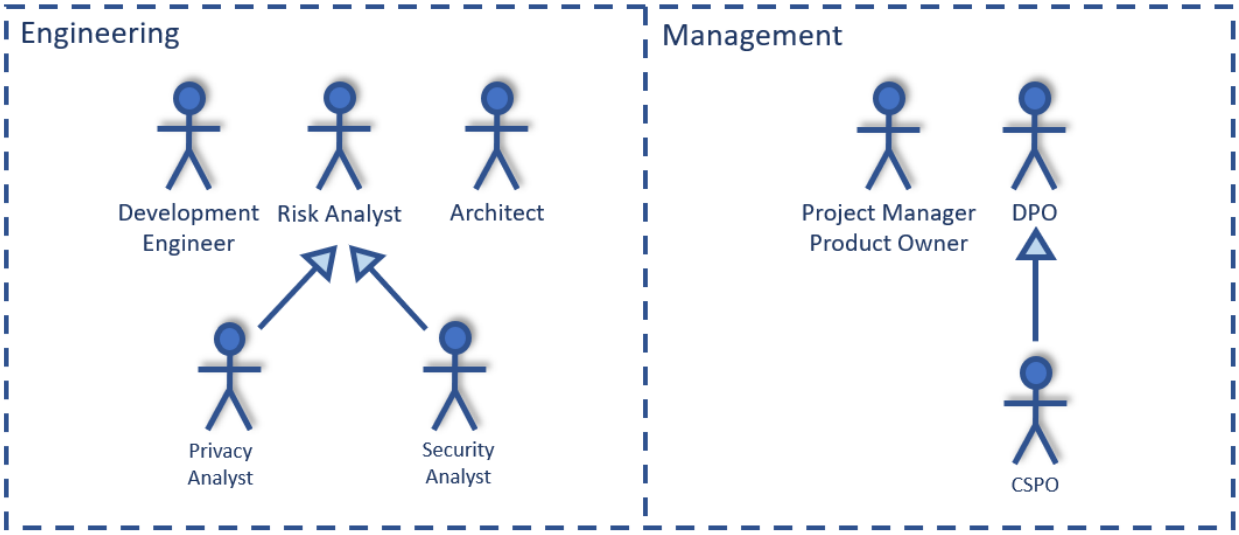
Figure 2 – The LINDDUN methodology steps

In particular, LINDDUN presents several aspects to consider when designing the methodology and tools to support the objectives of PDP4E:

- Risk analysis should be initiated at early stages of the design process, in parallel or replacing requirements definition, depending on the internal culture of the organization using PDP4E tools, i.e. if the organization follows a goal-oriented approach or a risk-oriented approach for designing the application.
- The threat categories elicited by LINDDUN shall be considered by the Risk Management tool in parallel to the security-centric STRIDE categorization used by other engineering-oriented risk management tools (such as in MUSA).
- PDP4E risk analysis tool needs to consume models created previously by other tools in PDP4E. Namely, it needs to consume at least:
    - *Data stores information* and *Data Flow Diagrams* (DFD), both defined in WP5 as part of the data and functional layers of the design of the system.
- The risks analysis tool will generate a set of mitigation actions or controls. There may be different types of controls, but in particular we will focus on those that affect engineers and impact the design process. For instance, the implementation of a particular PET may be one of these controls.

2 User needs

In terms of users, Privacy and Data Protection by Design (PDPbD) involves many different stakeholders, including legal experts, requirements engineers, software architects, developers and system operators. Currently, legal departments and engineers work in silos. The legal approach is based in performing a Data Protection Impact Assessment (DPIA), while the software Engineers approach, deals with threat modelling to identify privacy requirements and risks. In general, the aim of our tool is focused on getting engineers engaged in risk analysis. So we foresee at least the following roles involved in the usage of our tool:



Data Protection Officer (DPO). Overall responsible for privacy and data control. Whenever an organization does not need to appoint a DPO, other actors in the organization may share DPO's responsibilities. In particular, the Chief Security and Privacy Officer (CSPO) might be involved in the same tasks as the DPO when it comes to risk management processes.

Within the risk control process, the DPO will be responsible for: reviewing and validating contents of the risk plan and/or DPIA, controlling treatment implementation, reporting non-compliance risks (e.g. to the company's board), and consulting supervisory authorities or other external stakeholders (e.g. data subjects) when necessary.

Given the growing complexity and fast evolution of cyberattacks, DPO may feel the pressure to constantly update risk plans according to the most recent practices.

Project Manager (or Product Owner). The project manager usually conducts the risk management process for a particular product or project of her responsibility.

The project manager should be involved in several phases of the risk analysis process, including: the identification of risk sources (e.g. hacker), the definition of assets, the assessment of risks, appointing owners to the definition of threats and their respective mitigation actions, control of their implementation and finally supporting the DPO in preparing documentation related to a DPIA.

In order to fulfil their tasks, Project Managers need to coordinate contributions from several actors. It is particularly important that the risk management tool provides an easy-to-check

dashboard with the current status of the risk plan (both at preparation and implementation stage).

Architect. The architect is a key actor in the execution of the risk control process, as she holds most of the technical knowledge on the system to be implemented, likelihood of the identified threats and the technical maturity / feasibility of privacy controls.

The architect will support the definition of assets (and in particular, the definition of the architecture, data flow diagrams, etc), the identification of threats, the assessment of risks, the definition of controls or treatments and the assessment of the residual risk after the application of these controls.

Risk Analyst. The risk analyst role represents someone appointed to control the overall risk assessment process, bringing specific expertise in risk management. While the role may exist in any type of organization, small companies may not have staff with particular expertise in risk management and this role may be played by an architect or an external consultancy firm. In large enterprises, this role may represent a much wider subsets of roles including staff in the Quality Assurance department, a Chief Security and Privacy Officer (CSPO) or a security / privacy expert in general.

Risk analyst will be specially involved in identifying risk sources and threats, performing the risk assessment, defining controls and calculating residual risks after their application.

Development Engineer. Developers will be involved in the correct implementation of treatments and their continuous control. They may also be involved in the risk assessment process and the definition of controls. Their role in the risk control process may significantly change depending on the type of organization, but they will be mostly involved to be aware of the data protection strategy and the consequences of incorrect, or partial, implementations.

3 Requirements elicitation

R-F-WP3-001	Threat identification
Description	Users of the risk management tool shall be able to define a set of threats to the data subjects' rights and freedoms. Such threats shall be described in terms of an event or a malicious actor making an unwanted, unsolicited usage of data processing assets.
Relation to other requirements	
Actor	Project Manager, Risk Analyst
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	One of the main objectives of a risk management process is to identify the assets you want to protect and those unwanted events that threaten those assets. Data protection under the GDPR follows a risk-based approach, where the data subjects' rights and freedoms are the assets to protect.

R-F-WP3-002	Collaborative Risk Management
Description	The risk management tool shall provide transparent information to engineering stakeholders such as development teams and architects. The tool shall also allow engineering stakeholders to perform some of the steps traditionally performed by project managers and/or risk analysts.
Relation to other requirements	
Actor	Development team, Architect
Priority	Must have
Type	Functional
Non-functional category	Usability
Rationale	Risk Management is typically conducted by Project Managers and Risk Analysts, with little feedback from the engineers involved in the design and implementation of the data processing system. This might result on longer times to adapt risk plans to the technical details of the data processing systems, as well as engineering stakeholders feeling alienated from the protection of data subjects' privacy.

R-F-WP3-003	Risk Assessment
Description	The risk management tool shall allow users to measure the importance of identified threats. Such assessment shall be conducted by considering the likelihood of the unwanted usage and its consequence on data subjects' rights and freedoms. Likelihood and consequence shall be measured on a numerical scale. The risk management tool shall allow users to provide a written explanation of the provided score. The user may engage engineering stakeholders by asking feedback about the likelihood of the unwanted event given their knowledge on the technical specification of the system.
Relation to other requirements	R-F-WP3-001, R-F-WP3-002
Actor	Project Manager, Risk Analyst
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	Risk management standards [8] [9] and the GDPR ask organizations to act with respect to the magnitude of a threat. This is a fundamental requirement to establish a first priority to a risk, based on its likelihood and consequence. Notice that there are multiple mechanisms to support risk analysts in assessing risks. Deliverable D2.2 introduced some of them in section 3.2 and briefly introduced as part of the background tools of the project (see Section 1.1, OWASP Scoring Methodology). The methodology set on PDP4E will further elaborate on how to perform such assessment.

R-F-WP3-004	Risk Evaluation
Description	The risk management tool shall enforce users to actuate on all identified risks. To do so, the tool shall label risks to reflect whether • This risk is still undergoing a deep analysis. • Risk has been analysed and a plan for reducing its impact and consequence has been devised. Implementation of the plan might have not finished. • Risk has been analysed but there is no plan for reducing its impact as it is deemed as acceptable.

	• Risk was analysed in the past, but changes in the environment and/or data processing system makes it irrelevant at the moment.
Relation to other requirements	R-F-WP3-003
Actor	
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	Those four categories follow the ROAM evaluation scheme (Resolve, Owned, Accepted, Mitigated) largely used in large-scale project management risks[6].

R-F-WP3-005	**Define Controls**
Description	The risk management tool shall allow users to define a strategy to mitigate the risks identified at a previous stage. Such strategies may be defined in terms of reducing the likelihood of the unwanted event, and/or reducing the impact of its consequences. These mitigation strategies might come in the form of (1) formal functional or non-functional requirements to be considered by the engineering stakeholders; (2) implementation of privacy-enhancing techniques on the different data processing activities; and/or (3) changes in the specification of the data processing activities. Given its technical nature, it is advised that the user seeks the feedback from the engineering stakeholders.
Relation to other requirements	R-F-WP3-002, R-F-WP3-004
Actor	Project Manager, Risk Analyst
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	The risk plan shall not be finished with the identification of the risks, but the preparation of a plan to reduce the impact of the identified risks.

[6] Readers may check the PI Planning artefacts used by the Scaled Agile Framework for a better understanding of the ROAM evaluation scheme. https://www.scaledagileframework.com/pi-planning/

	Quality of the defined controls should be key to the proper evaluation of risks (R-F-WP3-003).

R-F-WP3-006	**Report Generation**
Description	The risk management tool shall be capable of generating a report that summarizes the risk plan in a human readable format. This report shall contain a description of the identified risks, including • a description of the unwanted event; • a description of the external or internal actors that could materialize such unwanted event; • the likelihood of such event; and • the potential impact on the data subjects.
Relation to other requirements	R-F-WP3-001, R-F-WP3-003, R-F-WP3-005
Actor	Project Manager
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	In annex 2 of [6], the WP29 sets a baseline criterion for acceptable data protection impact assessments. The items highlighted by this requirement are those related to risk management.

R-F-WP3-007	**Integration with Data Protection Impact Assessment**
Description	The risk management tool shall facilitate including the results of the risk analysis into a data protection impact assessment. To achieve this objective, the tool shall • provide an API where third party tools can fetch the necessary information from the risk management plan; and / or • export the data in a computer readable format. At least all information contained in the report (R-F-WP3-006) shall be available to third party tools.
Relation to other requirements	R-F-WP3-006
Actor	Project Manager
Priority	Must have
Type	Functional

Non-functional category	N/A
Rationale	Albeit risk analysis is a fundamental part of DPIAs, not all data processing projects are obliged to conduct such data protection impact assessments. Whereas risk management processes shall identify risks to the data subjects, DPIA should also provide information related to compliance with articles that are not directly related to risks. Even though, in such cases where a DPIA is not mandatory, it is still advised to perform a risk analysis as part of the *data protection by design approach* and, hence, we believe it is important to separate both concepts. With this requirement, we are deliberately making a difference between risk management processes and conducting a DPIA. As part of PDP4E, we plan to make an integration with the CNIL tool (see Section 1.2) to fill these DPIA needs and demonstrate how risk plans can be integrated.

R-F-WP3-008	**Report Validation**
Description	The risk management tool shall allow DPOs (or equivalent) to validate the appropriateness of the risk plan. In case of unsuccessful validation, the DPO shall be capable of providing feedback to the risk management team and other engineering stakeholders.
Relation to other requirements	R-F-WP3-006, R-F-WP3-007
Actor	DPO
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	

R-F-WP3-009	**Load description of the data processing system**
Description	The risk management tool shall allow loading a technical description of the data processing system. This description should include: • A high-level overview of the different data sources, processes, and datastores to be considered. • Flow of information between the different elements of the description. • A high-level description of the architecture.
Relation to other requirements	

Actor	Project Manager, Architect
Priority	Should have
Type	F
Non-functional category	N/A
Rationale	Necessary for applying STRIDE and LINDDUN methodology.

R-F-WP3-010	**Define Vulnerabilities**
Description	The risk management tool shall allow users to enhance the description of the data processing system (R-F-WP3-009) by linking its different elements to vulnerabilities that may be exploited by a malicious actor.
Relation to other requirements	R-F-WP3-009
Actor	Risk Analyst
Priority	Could have
Type	Functional
Non-functional category	N/A
Rationale	In some scenarios, it is easier to define threats by first performing a deep analysis of the different elements in an architecture and its vulnerabilities. Then, unwanted incidents are a matter of describing how malicious actors may make use of such vulnerabilities.

R-F-WP3-011	**Threats are associated to vulnerabilities and elements of the system description**
Description	The risk management tool shall allow users to enhance the description of the data processing system (R-F-WP3-009) by (1) linking its different elements to the unwanted events they facilitate and (2) establishing a relation between the different vulnerabilities of the system and the threats.
Relation to other requirements	R-F-WP3-010
Actor	Risk Analyst
Priority	Could have
Type	Functional

Non-functional category	N/A
Rationale	Similarly to R-F-WP3-010, we allow the user to make explicit the link between the threats and different elements of the system. In this case, this might help in defining strategies to reduce the risk to the data subject (the user has a clear idea of which part of the system, or which vulnerabilities, needs to be addressed). We make a distinction between linking threats to vulnerabilities and/or elements of the system as, in some cases, the definition of threat has an implicit description of the vulnerability.

R-F-WP3-012	**Knowledge Base**
Description	The risk management tool shall facilitate the definition of vulnerabilities, threats and privacy controls by providing access to external privacy and data protection bodies of knowledge. The tool shall provide the means to allow users to interchange the default body of knowledge with one provided by a third party.
Relation to other requirements	R-F-WP3-001, R-F-WP3-005, R-F-WP3-010, R-F-WP3-011
Actor	Risk Analyst
Priority	Should have
Type	Functional
Non-functional category	N/A
Rationale	Having a default body of knowledge to check is particularly important when non-risk experts are involved in the process (R-F-WP3-001).

R-NF-WP3-001	**Unique ID**
Description	The elements included in the body of knowledge (R-F-WP3-012) shall be entitled with a Unique ID that allows the user to keep track of (1) provenance of the knowledge and (2) check if there has been any update or correction on the body of knowledge.
Relation to other requirements	R-F-WP3-012
Actor	
Priority	Could have
Type	Non-Functional

Non-functional category	Usability
Rationale	Cybersecurity is an evolving environment that demands practitioners to be updated on the latest vulnerabilities and threats.

R-NF-WP3-002	**Link to external documentation**
Description	The different elements of the body of knowledge shall reference documents where this information was extracted and/or more details can be found.
Relation to other requirements	R-F-WP3-012
Actor	
Priority	Could have
Type	Non-FunctionalF
Non-functional category	Usability
Rationale	

R-F-WP3-013	**Task Ownership**
Description	Risk Analysts may take ownership of identified vulnerabilities and threats. Owners shall monitor, or take care of carrying out, the analysis until its completion or transfer to another actor. In non-agile environments, Project Managers may assign ownership to individual actors.
Relation to other requirements	R-F-WP3-001
Actor	Project Manager, Risk Analyst
Priority	Could have
Type	Functional
Non-functional category	N/A
Rationale	

R-F-WP3-014	**Dashboard**
Description	At any point, users can check the progress of the risk management process. This includes: • A view that depicts detected vulnerabilities, threats and controls;

	• A warning indicating if there are vulnerabilities without associated threats (indicator that further analysis is required); • A warning indicating if there are elements in the system description without any vulnerability nor threat associated; • A risk map providing visual information on the detected threats, its likelihood and consequence to the data subjects.
Relation to other requirements	R-F-WP3-001
Actor	
Priority	Must have
Type	Functional
Non-functional category	N/A
Rationale	

R-F-WP3-015	**Assigning data processors to system elements**
Description	The risk management tool shall allow the user to assign processor to the different system elements (R-F-WP3-009). Such assignment indicates that the processor is involved in (1) executing the processing activity, (2) storing data, (3) providing infrastructure. If the project has not chosen a vendor yet, the user shall be able to create placeholders.
Relation to other requirements	
Actor	
Priority	Could have
Type	Functional
Non-functional category	N/A
Rationale	

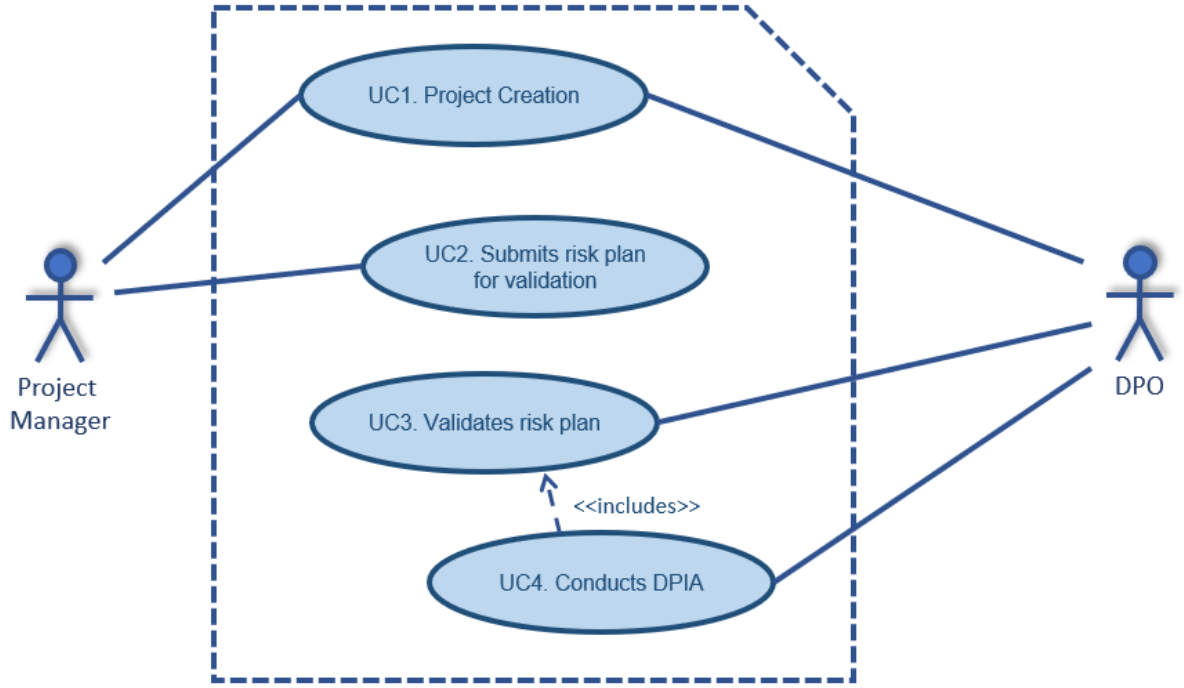
R-F-WP3-016	**Group by processor**
Description	The report generated by the risk management tool (R-F-WP3-006) may include an appendix with all vulnerabilities, threats and privacy controls that are indirectly associated with each processor.
Relation to other requirements	R-F-WP3-015
Actor	

Priority	Could have
Type	Functional
Non-functional category	N/A
Rationale	This information might be useful when selecting vendors as processors.

4 Design

4.1 Use cases

4.1.1 Risk Project Management



Use Case	UC1. Project Creation
Functionality Description	Creation of a new project in the risk management tool.
Actors	Project Manager, DPO
Assumptions / Preconditions	The project should not exist
Post-conditions	The project should be stored in the projects database
Steps	1. Press option to create a new project. 2. Provide name of the project and staff associated to the project with roles they will play in the project. 3. Choose whether definition of vulnerabilities is part of the methodology or not in this project. 4. Save the project
Variations	-
Exceptions	2.a The user aborts the creation of the project. The project is not saved.

Requirements	
Related use cases	

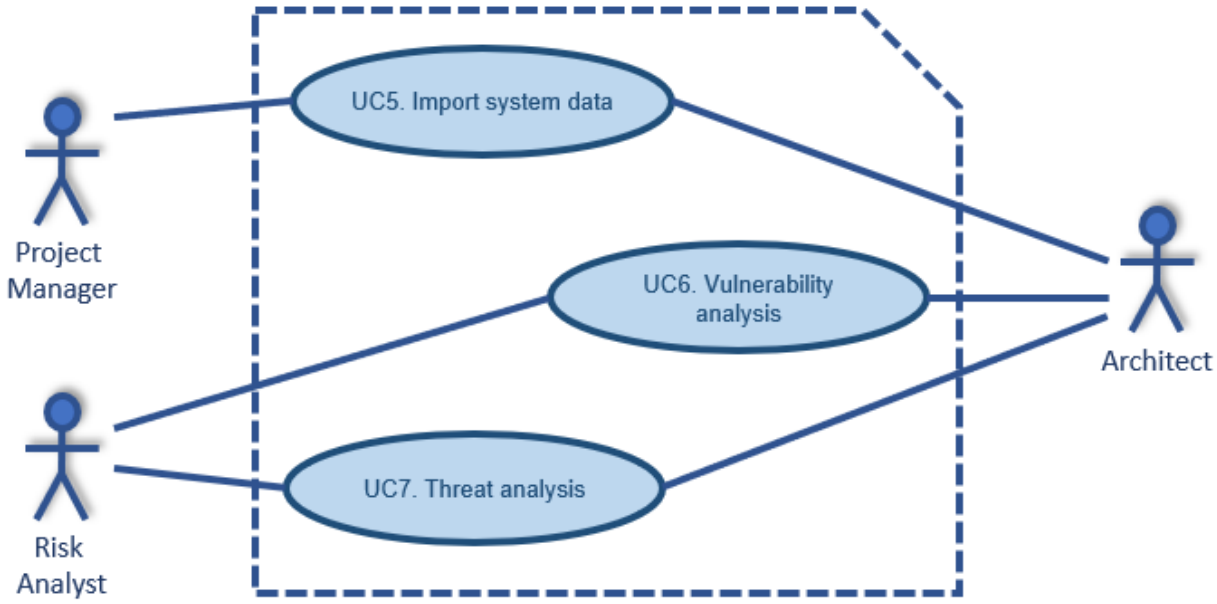
Use Case	**UC2. Submits risk plan for review**
Functionality Description	Project is submitted to a reviewer for checking compliance with relevant regulations and/or organization policies.
Actors	Project Manager
Assumptions / Preconditions	A project has been created and a draft of the risk plan is ready.
Post-conditions	A report containing the current risk plan is generated and submitted to a reviewer.
Steps	1. Press option to send document for review. 2. The tool sends the risk plan to the reviewer.
Variations	1a. The user can choose the reviewer. 2a. Risk plan is submitted to a third-party tool that keeps track of the risk plan status.
Exceptions	
Requirements	R-F-WP3-006, R-F-WP3-008
Related use cases	UC3. Validates risk plan

Use Case	**UC3. Validates risk plan**
Functionality Description	A partial or complete risk plan is ready for review its contents with respect to compliance with relevant regulations and/or organization policies.
Actors	DPO
Assumptions / Preconditions	A draft of the risk plan is ready for review, and Project Manager has requested a review of the plan.
Post-conditions	Risk plan is accepted.
Steps	1. Receive risk plan for review. 2. Review list of risks and identified mitigation controls 3. Check if residual risk is acceptable 4. Prepare a report with the result of the validation
Variations	

Exceptions	2a. User does not accept the description and/or level of details in the identified risks or mitigation controls. 2b. User identifies a risk that was not included in the risk plan. 2c. User suggest removal of some of the contents of the risk plan.
Requirements	R-F-WP3-006, R-F-WP3-007, R-F-WP3-008
Related use cases	UC4. Conducts DPIA

Use Case	**UC4. Conducts DPIA**
Functionality Description	The results of the risk plan are embedded into the contents of a Data Protection Impact Assessment.
Actors	DPO
Assumptions / Preconditions	Risk plan is available for review, or has been previously accepted.
Post-conditions	A Data Protection Impact Assessment is populated with the contents of the risk plan.
Steps	1. Receive risk plan for review. 2. Choose the Data Protection Impact Assessment that is associated to the risk plan. 3. Extract the relevant contents from the risk plan. 4. Collect and fill in the remaining information necessary to conduct a DPIA. 5. Review contents of the DPIA.
Variations	2a. Create a Data Protection Impact Assessment. Steps 3 and 4 are exchangeable. Step 5 extends UC3. Validates risk plan.
Exceptions	
Requirements	R-F-WP3-007
Related use cases	UC3. Validates risk plan

4.1.2 Import system data and threat identification



Use Case	UC5. Import system data
Functionality Description	The tool will be able to import a description of the system in the form of an architecture of the system and the data flow diagrams (DFD) describing data processes
Actors	Project Manager, Architect
Assumptions / Preconditions	A project has been created, architecture definition and DFDs are defined in a format that can be imported by the tool
Post-conditions	Architecture and DFDs are stored in the database and associated to the project
Steps	1. Files to import selected from file system (or using a drag and drop option) 2. Content of the files stored in the database
Variations	
Exceptions	1.a The user aborts the importing of files. Files are not imported to the project.
Requirements	R-F-WP3-009
Related use cases	

Use Case	UC6. Vulnerability Analysis

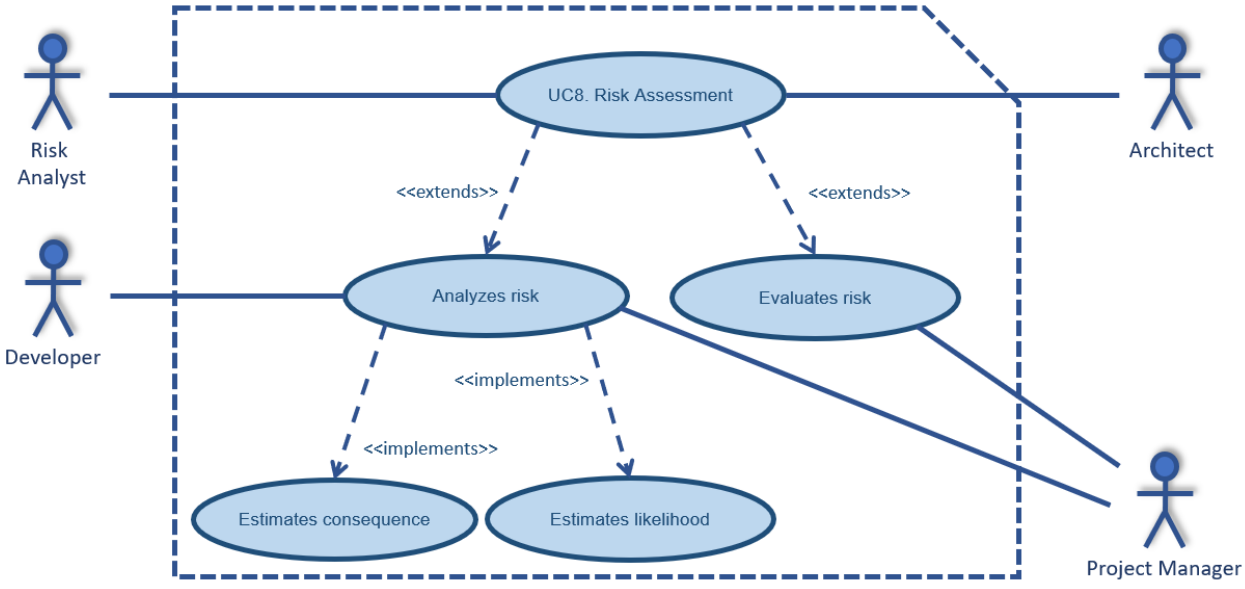
Functionality Description	Detecting vulnerabilities based on the warehouses, data flows, processes and terminators or entities in the DFD. Vulnerabilities can be associated to one or a set of these elements.
Actors	Risk Analyst, Architect
Assumptions / Preconditions	A set of DFDs have been imported to the project, a set of risk sources is available in a pre-populated library
Post-conditions	A set of vulnerabilities are associated to DFD elements or to sets of these elements
Steps	1. Open a particular DFD for editing 2. Click on the element(s) of the DFD for which user wants to associate a vulnerability 3. Obtain a recommendation of vulnerabilities for that element 4. Choose or describe vulnerabilities 5. Associate one or more risk sources obtained from a library to vulnerabilities 6. Save DFD with detected vulnerabilities
Variations	If a pre-populated library of vulnerabilities is not available, eliminate step 3. Alternatively, defined vulnerabilities may be edited or removed during the analysis process.
Exceptions	
Requirements	R-FWP3-010, R-F-WP3-011, R-F-WP3-012, R-NF-WP3-001, R-NF-WP3-002
Related use cases	

Use Case	**UC7. Threat Analysis**
Functionality Description	Detecting threats[7] based on the warehouses, data flows, processes and terminators or entities in the DFD. Threats can be associated to one or a set of these elements or to vulnerabilities if they are associated to the DFD.
Actors	Risk Analyst, Architect
Assumptions / Preconditions	A set of DFDs have been imported to the project, a set of risk sources is available in a pre-populated library
Post-conditions	A set of threats are associated to DFD elements or to sets of these elements, or through vulnerabilities detected in a previous step
Steps	1. Open a particular DFD for editing 2. Click on the element(s) of the DFD for which user wants to associate a threat

[7] In some contexts, and in the background literature considered by PDP4E, threats are sometimes also depicted as '*unwanted incident*'. Nonetheless, definition of unwanted incident is not consistent across the different standards and sectors.

	3. Obtain a recommendation of threats for that element 4. Choose or describe threats 5. Assign threats to owners 6. Associate one or more risk sources obtained from a library to threats 7. Save DFD with detected threats
Variations	If a pre-populated library of threats is not available, eliminate step 3. Alternatively, defined threats may be edited or removed during the analysis process. Alternatively, if vulnerabilities are defined: 1. Open a particular DFD for editing 2. Click on the vulnerabilities associated to the DFD elements for which user wants to associate a threat 3. Obtain a recommendation of threats for that vulnerability and element 4. Choose or describe threats Save DFD with detected threats
Exceptions	
Requirements	R-F-WP3-001, R-F-WP3-011, R-F-WP3-012, R-NF-WP3-001, R-NF-WP3-002
Related use cases	

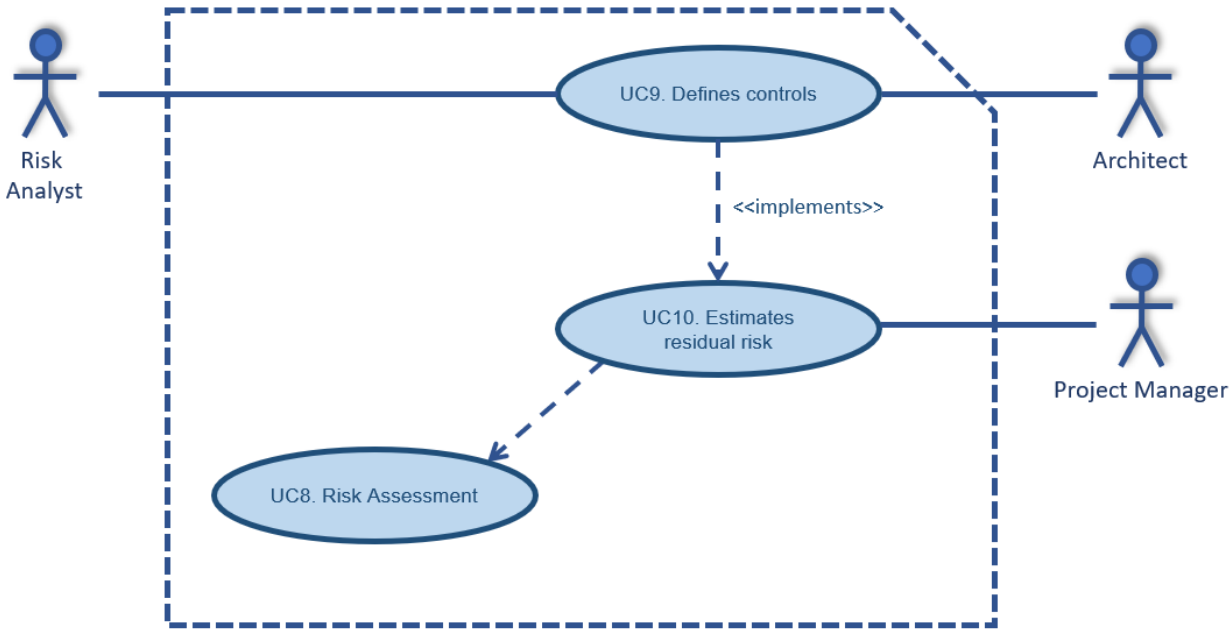
4.1.3 Risk Assessment and Evaluation



Use Case	UC8. Risk Assessment
Functionality Description	Analyze risks defining a likelihood and a consequence and evaluate the risk using ROAM (Resolved, Owned, Accepted or Mitigated)
Actors	Risk Analyst, Architect, Developer, Project Manager

Assumptions / Preconditions	A set of threats have been detected in the DFDs corresponding to the project
Post-conditions	Likelihood and consequence of a threat is evaluated and stored as the risk analysis of the threat and an evaluation of the risk is stored also in the database
Steps	1. Open a list of threats of a DFD 2. Select a methodology to analyse Risk (e.g. OWASP, CNIL) 3. Define likelihood and consequence related to each threat 4. Evaluate each risk by marking it as Accepted or leave it as Owned (value by default)
Variations	If the risk is not a risk anymore: 4.a Mark risk as Resolved
Exceptions	
Requirements	R-F-WP3-002, R-F-WP3-003, R-F-WP3-004
Related use cases	

4.1.4 Risk mitigation and residual risk

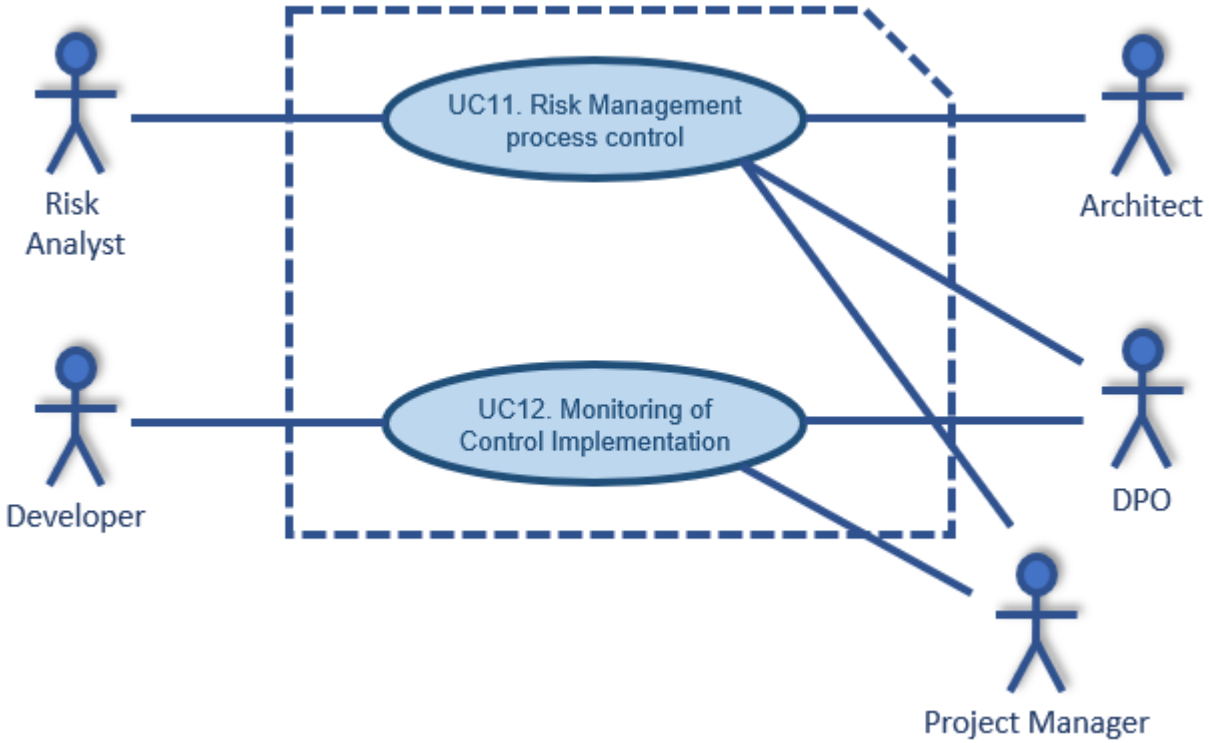


Use Case	UC9. Defines controls
Functionality Description	Define mitigation actions in the form of controls for each risk and reassess residual risk
Actors	Risk Analyst, Architect, Project Manager

Assumptions / Preconditions	At least one threat has unacceptable levels of likelihood and/or consequences to the data subjects.
Post-conditions	There is at least one control defined for each threat satisfying the precondition of UC9.
Steps	1. Open a list of risks 2. Select a set of mitigation controls 3. Decide if further controls are needed to mitigate the risk
Variations	2a. No mitigation controls are known.
Exceptions	
Requirements	R-F-WP3-005
Related use cases	By reassessing the threat likelihood and consequence (UC10), one can decide if risks are still at unacceptable levels.

Use Case	**UC10. Estimates Residual Risk**
Functionality Description	Likelihood and consequence are recalculated taking into consideration the identified mitigation controls.
Actors	Risk Analyst, Architect, Project Manager
Assumptions / Preconditions	Risks have been assessed and a mitigation control has been selected for this risk.
Post-conditions	Controls have been defined and their mitigation effect has been estimated to reassess risks. New likelihood, consequence and risk evaluation status is stored in the database.
Steps	1. Recalculate likelihood and consequence of each risk using methodology to analyse Risk (OWASP, CNIL) selected in the initial risk analysis process 2. Re-evaluate each risk by marking it as Mitigated
Variations	If the risk is not a risk anymore: 2a Mark risk as Resolved If the risk is not mitigated but it can be accepted or we will continue defining controls later on: 2a Mark risk as Accepted or Owned, respectively
Exceptions	
Requirements	R-F-WP3-003
Related use cases	

4.1.5 Monitoring and Visualization of Risk Plan



Use Case	UC11. Risk Management process control
Functionality Description	Agile mechanism to control risk management status based on the use of a Kanban-like board to check the status for all assets and risks.
Actors	DPO, Project Manager, Risk Analyst, Architect
Assumptions / Preconditions	A project has been created
Post-conditions	Users have a global vision on the execution status of the risk management process and know the status and the owner of each subtask and have changed the status if necessary.
Steps	1. User selects an option to see the risk management process through a Kanban-like board 2. A Kanban-like board appears showing the evolution of the assets through the different steps of the risk analysis methodology User can access the functions related to the other use cases from the board by clicking on an element in the board
Variations	3.a Users can change the status of an element in the board by dragging and dropping it 3.b Users can add new elements to the board by connecting them to an element in DFD and creating a new element in the column of the board related to Vulnerability Analysis or Threat Analysis

	If all the elements in the risks in the board have been re-assessed after defining controls: 4.a Pop-up message to ask the user if the risk plan is ready to be validated Alternatively: 4.b A user can select a subset of risks that have been already re-assessed and send the subset of validation
Exceptions	
Requirements	R-F-WP3-002, R-F-WP3-013, R-F-WP3-014
Related use cases	

Use Case	**UC12. Monitoring of Control Implementation**
Functionality Description	Control indicators related to the proper implementation and effectiveness of controls
Actors	DPO, Project Manager, Developer
Assumptions / Preconditions	Necessary controls have been defined for corresponding risks and risk plan have been approved by the DPO
Post-conditions	Status of the implementation and effectiveness of controls is known and consequent actions can be taken
Steps	1. Visualize dashboard with incidents related to not-implemented controls
Variations	
Exceptions	
Requirements	
Related use cases	

4.2 Architecture

In Figure 3, we present a general view of the architecture of the Risk Management Tool developed in PDP4E and its connection to the other tools of the project. The figure is based in the actual functional decomposition for the Risk Management tool as it is described in deliverable D2.6 [10].

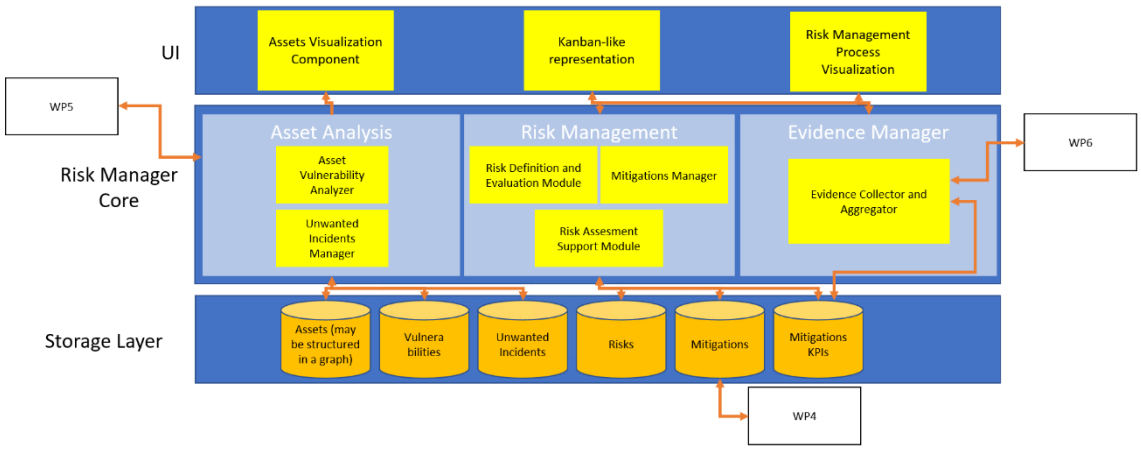


Figure 3 – General Architecture of the risk management tool

The components of our architecture are divided in 3 layers: Storage layer, Risk Manager Core layer and the UI layer:

- Storage layer: this layer represents all the components in the system that are in charge of storing relevant data for the risk management process. We would like to highlight:
  - Assets: assets may be any element, or flow of data between them, in a system which may be subject to be analyzed from a risk perspective. This includes isolated components in a complex system. We expect to collaborate with WP5 in the definition of a format to express such assets and flow of data between them.
  - Threats (or unwanted incidents): threats are also associated to assets as defined in the first data store. The LINDDUN catalog will help us create an initial set of threats to be considered by risk analysts.
  - Mitigations: this data store keeps the controls or mitigation actions defined by each of the risks that require mitigation. This is also the source to feed the Requirements tool developed in WP4.
- Risk Manager Core layer: this layer keeps all the brains of the risk management tool. The software modules in this layer are:
  - Risk Management: it provides all the software components for risk analysis (including assessment and evaluation), definition of mitigation controls and all the tool to support risk assessment. D3.4 focuses on describing the method that supports this functionality.
  - Evidence Manager: this module could consume information from the compliance tool developed in WP6 to monitor status of implementation and the efficiency of the chosen mitigations.
- UI layer: this layer contains all the components related to the interface of the tool.
  - Kanban-like representation: elements will be mapped in a Kanban so that users will know the status of execution of the risk management process.

There may be other components to connect the risk analysis tool to other external tools such as the CNIL tool, through the generation of reports in specific formats.

5 References

[1] PDP4E Consortium, "D2.2 Technical analysis and synthesis of user requirements (rev. 2)," 2019.

[2] PDP4E Consortium, "D2.4 Overall system requirements," 2019.

[3] PDP4E Consortium, "Risk Management Method for data protection and privacy," 2019.

[4] V. Muntés-Mulero, O. Ripolles, S. Gupta, J. Doiminiak, E. Willeke, P. Matthews and B. Somosköi, "Agile Risk Management for Multi-Cloud Software Development," *IET Research Journals, IET Software Journal,* December 2018.

[5] NIST, "NIST Special Publication 800-53 (Rev. 4)," 2013.

[6] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)," 2017.

[7] K. Wuyts, "Privacy Threats in Software Architectures," 2015.

[8] ISO, "ISO 31000 - Risk management," 2018.

[9] ISO/IEC, "ISO/IEC 29134:2017 - Information technology -- Security techniques -- Guidelines for privacy impact assessment," 2017.

[10] PDP4E Consortium, "D2.6 Overall architecture and methodological framework," 2019.