This report was funded by the European Union's Internal Security Fund — Police

Public Resillience using Technology to Counter Terrorism

D1.2 – Risk Management and Quality Assurance

WP number and title	WP1 – Management and Coordination of the Action
Lead Beneficiary	DITSS
Contributor(s)	-
Deliverable type	Report
Planned delivery date	31/01/2019
Last Update	29/01/2019
Dissemination level	PU

Disclaimer

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The PRoTECT Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
2	KENTRO MELETON ASFALEIAS	KEMEA	RTO	GR
3	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	RTO	NL
4	INSPECTORATUL GENERAL AL POLITIEI ROMANE	IGPR	GOV	RO
5	FORUM EUROPEEN POUR LA SECURITE URBAINE	EFUS	NPO	F
6	LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS	L3CE	RTO	LT
7	GEMEENTE EINDHOVEN	Eindhoven	GOV	NL
8	AYUNTAMIENTO DE MALAGA	Malaga	GOV	SP
9	DIMOS LARISEON	DL	GOV	GR
10	VILNIAUS MIESTO SAVIVALDYBES ADMINISTRACIJA	VMSA	GOV	LT
11	MUNICIPIUL BRASOV	MUNBV	GOV	RO
12	STICHTING KATHOLIEKE UNIVERSITEIT BRABANT	JADS	RTO	NL
13	MINISTERIO DEL INTERIOR	MIR	GOV	SP

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
0.1	15/11/2018	Draft	George Kioumourtzis (DITSS)	Definition of Table of Contents (TOC)
0.2	15 /12/2018	Draft	George Kioumourtzis (DITSS)	Editing Sections 1-X
0.3	12/01/2019	Draft	Patrick Padding (DITSS)	Review and comments
0.4	20/01/2019	Draft	George Kioumourtzis (DITSS), Peter van de Crommert (DITSS)	Final review and Quality assurance
1.0	29/01/2019	Final	Patrick Padding (DITSS)	Final approval and submission

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
PRoTECT	Public Resilience using Technology to Counter Terrorism
LEA	Law Enforcement Authority
PMC	Project Management Committee
QC	Quality Control
URL	Uniform Resource Locator
CA	Consortium Agreement
DoA	Description of Action
GA	Grant Agreement
KOM	Kick-off Meeting
KPI	Key Performance Indicator
PC	Project Coordinator
ToC	Table of Contents
WP	Work Package
WPL	Work Package Leader

Table of Contents

List of Figures

List of Tables

Executive Summary

Deliverable D1.2 “Risk Management and Quality Assurance” is in essence a monitoring loop running throughout the lifetime of the PRoTECT project evaluating the quality of work and deliverables and assessing internal and external risks. This deliverable sets the guidelines for the aforementioned monitoring loop.

Since Quality Assurance and Risk Management are parts of the overall project management process a brief overview of the PRoTECT management context is initially provided in this document. The overall Project Management structure of PRoTECT is presented and detailed descriptions of the Quality and Risk Management roles are provided.

PRoTECT quality assurance strategy can be summarized in the following commitment: “The PRoTECT Consortium recognises that dedication to quality is vital to the PRoTECT Project mission and essential for delivering consistent results”. Core quality assurance objectives are quality work and deliverables and keeping project in track (in line with DoA). Moreover, PRoTECT Consortium commits that all project activities will be carried out in compliance with established ethical principles and the applicable law.

In his effort to achieve quality assurance objectives, the PRoTECT Quality Manager will have a number of quality assurance tools and processes, namely:

- Quality assurance tools
- Supporting Documents, like the CA, DoA, GA and relevant project deliverables).
- Templates.
- Quality Dashboard consisting of a KPIs, a Deliverables and Milestones, an APs, and a PMs Worksheet.
- Detailed Task Work plans (DTWs).
- Document Management System (DMS).
- Quality assurance processes
- Quality evaluation process.
- Deliverables review procedure.

The PRoTECT Consortium is aware that a variety of risks may impact project schedule and project objectives, and may even lead to contractual issues. For this reason, a Project Risk Management Plan is included in this deliverable focusing in risk assessment, monitoring and mitigation actions. A Risk Register available to all PRoTECT will be used to carry out the aforementioned actions.

Finally, it is important to note that any rules and regulations presented within this Project Risk Management and Quality Assurance are supplementary to the Consortium Agreement as well as the Grant Agreement. Many items regulated there are NOT repeated here, but should be taken into account.

1 Introduction

This deliverable focuses in the Risk Management and Quality Assurance of the project. It is both a plan and a manual to carry out the above activities. This deliverable consists of the following chapters:

Chapter 2 – PRoTECT Project Management Overview – provides a summary of PRoTECT's management structure and responsibilities.

Chapter 3 – Quality Management- provides quality planning and assurance procedures along with document handling and deliverable review guidelines.

Chapter 4 – Risk Management Plan- presents the main elements of risk management, how risk assessment will be carry out in the project along with responsibilities for risk monitoring and mitigation.

Finally, in **Chapter 5 – Conclusions –** we conclude this document.

2 PRoTECT Project Management Overview

2.1 Project Structure

European projects such as PRoTECT are complex organizations in which entities with different culture, approaches, and interests join forces and expertise to achieve common goals. In order to be successful, a functional organizational structure must be put in place, which ensures efficient, result-driven management.

The overall management of the PRoTECT project is based on the following points:

- The Organisational Structure, which defines the management structure in terms of project governance and boards;
- Means for governance and control:
  - The **Consortium Agreement**, which defines the rules of collaboration among partners within the Project (roles, responsibilities and mutual obligations for the project life).
  - The project **Description of Work (DoW)**, which, among the others, describes the project objectives and expected results, the work plan in terms of work packages, tasks, deliverables, milestones, and the effort/cost distribution per WP/task and per partner;
  - The **Project Reference Manual** (D1.1 - Project Management Handbook), which defines in detail the structures, the procedures, and the actors of the project. D1.1 also includes the guidelines for internal communication;
  - The **Project Risk Management and Quality Assurance** which defines the procedures and standards for risk management and quality assurance of project work and deliverables;

The PRoTECT project management structure is depicted in Figure 1 below.

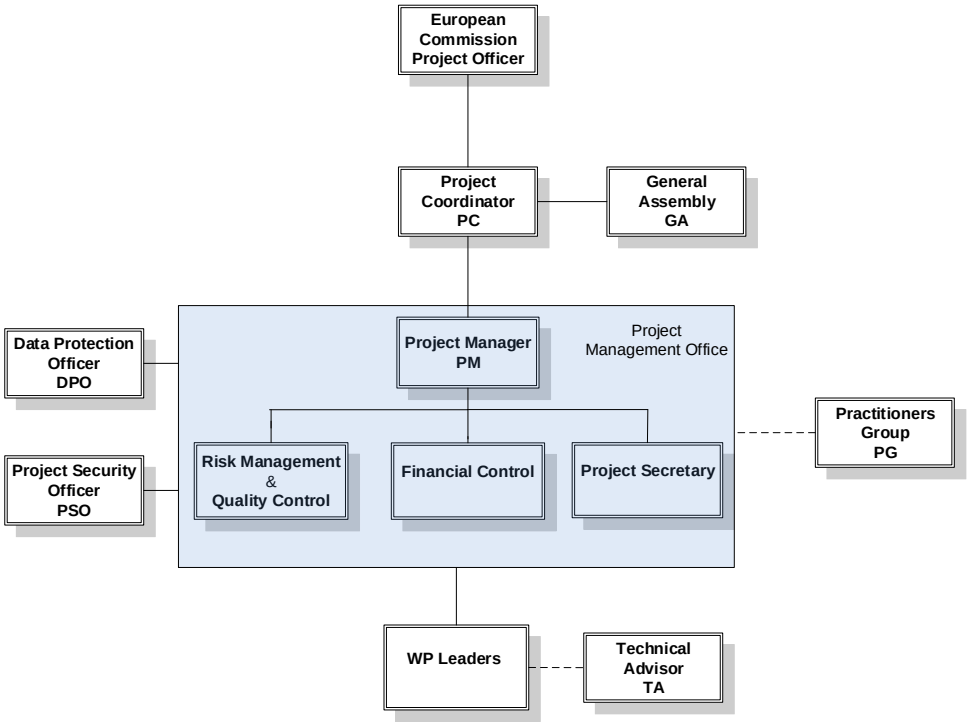

Figure 1: PRoTECT organizational and management structure

2.2 Risk and Quality Manager

The role of the Quality Manager is to keep PRoTECT focused on its objectives of producing high quality outputs and adopting standard-based approaches. In the line of the project Quality Management, the Quality Manager will be asked periodically to review technical progress in order to ensure that the project remains innovative, driven by requirements of end users, open to collaborations and to market needs and forward looking. Fulfilment of those requirements will ensure that PRoTECT is producing an outcome of high technical quality.

The **Quality Manager** is responsible for the quality of all project deliverables; details on internal review and approval procedures of the PRoTECT deliverables are given later on. However, quality shall not only be addressed for the deliverables but also for the project process itself. Thus, management process and developments of the project will be submitted to periodical reviewing by the Quality Manager with respect to:

- Staying focused on project objectives of focusing on end-user requirements, high quality outputs, and standard-based approaches.
- Adequacy of the project management plan and how the work performed complies with it including dissemination of results.
- How well the project processes are synchronized and inter-linked.
- Identification and evaluation of activities and results that would adversely affect the achievement of the project objectives.
- Process improvement in the project by identifying deviations and changes.

At the same time, having in mind that risk may have an impact on the project schedule and objectives, and finally may lead to contractual issues, the role of **Risk Manager** has been foreseen. The Risk Manager will be asked periodically to review project progress as well as the risk items table to ensure that PRoTECT remains in line with its technical objectives. Finally, he will be also in charge of keeping up-to-date the "Project Risk Management Plan", which is defined in Section 4 of this report.

The role of **Risk and Quality Manager** for the PRoTECT project has been assigned to **Dr**. ***Georgios Kioumourtzis*** (DITSS).

3 Quality Management

Quality management is an aspect of project management that normally differentiates three different aspects:

- **Quality Planning**: This is basically the identification of quality goals, and identification of the metrics that will be used to control the quality.
- **Quality Control**: This determines how and when quality checks and controls will take place to collect data related to the quality metrics identified, and who will perform these checks.
- **Quality Assurance**: This basically determines who/how/when will monitor if the quality goals that have been set are being met or not and to seek for continuous improvement.

3.1 Quality Planning and Control

Quality planning in this project is reflected in this document as it specifies quality policies on the topics that have been identified as most important for this project, namely Communication, Reporting, Documents, Deliverables, and Dissemination. In this document, for each of the aforementioned topics quality goals are set and the process to control and assure that those goals are met are defined.

As there is always, a need to find the appropriate balance between cost and benefit, in this project the quality goals (and therefore the metrics associated to them) have been identified taking into account among other things risks and expected benefits.

The Project Coordination Group (PCG) will be responsible to put in place and run the quality control mechanisms needed for the project.

The goals and associated metrics along with quality control mechanisms that have been chosen are as follows:

3.1.1 Communication (COMM)

- **Goal1**: Having efficient and well-managed project meetings.
  - Metric(s):
  - COMM-G1-M1: all formal meetings should have an agenda prepared and distributed with sufficient time in advance so that all invited people know what the goal of the meeting is, what the expected output of the meeting is (e.g. decision, plan, information exchange), what is expected from them and so that they can be able to prepare the meeting appropriately.
  - COMM-G1-M2: all formal meetings should have the minutes prepared and submitted within 48 labour hours, using the approved template for minutes, and uploaded to the collaboration tool.
  - **Quality control mechanism**: 6 monthly audits run by the Quality Manager and the Project Coordinator.

- **Goal2**: Establishing and maintaining good communications with other related projects
  - Metric(s):
  - COMM-G2-M1: Number of related projects contacted.
  - COMM-G2-M2: Frequency of the coordination meetings between PRoTECT and other related projects.
  - **Quality control mechanism**: Verification of the existence of minutes or formal documents that reflect the contacts that have taken place.

- **Goal3**: Setting up and maintaining efficient and easy-to-use collaboration tools
  - Metric(s):
  - COMM-G3-M1: To have private collaboration tools set up and ready to be used before M3 (as defined in DoA).
  - COMM-G3-M2: Number of complaints from team members with regard to the appropriateness of the collaboration tools.
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

3.1.2 Reporting (REP)

- **Goal1**: Meeting EC related reporting requirements on time and with no issues.
  - Metric(s):
  - REP-G1-M1: Number of issues that have been identified related to reporting to the EC
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

- **Goal2: Meeting internal reporting policy (see Deliverable D1.1 "Project Reference Manual and Tools ", Section 4.2) on time and with no issues.**
  - Metric(s):
  - REP-G2-M1: Number of issues that have been identified related to internal reporting
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

3.1.3 Documents (DOC)

- **Goal1**: To follow agreed upon standards for formats and tools to be used in document editing and exchange as described in section 3.3.
  - Metric(s):
  - DOC-G1-M1: 6 monthly audits of a sample of the documents generated by the project to check if they have followed the Quality Management Plan.
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

3.1.4 Deliverables (DEL)

- **Goal1**: to assure that the deliverables produced in the project are of high quality and that they have followed the deliverables preparation policy as described in section 3.4.
  - Metric(s):
  - DEL-G1-M1: 6 monthly audits of a sample of the deliverables generated by the project to check if they have followed the Quality Management Plan.
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

3.1.5 Dissemination (DISS)

- **Goal1**: To have the project's website up and running before M3 and updated on a regular basis.
  - Metric(s):
  - DISS-G1-M1: To have the public website up and running before M3 (as described in the DoA)
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

- DISS-G1-M2: Audits every 3 months to check that the public website is updated with the relevant information.
- **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

- Goal2: To organise at least three workshops (as defined in the DoA) and if possible, more in which to successfully engage end-users of different profiles (LEA, municipal authorities, etc.)
  - Metric(s):
  - DISS-G2-M1: workshop minutes and conclusions reports
  - **Quality control mechanism**: Emails or notes in meeting minutes reflecting those complaints.

3.2 Quality Assurance

In order to assure that quality goals are met and that a continuous improvement philosophy is followed the Project Coordination Group will meet and include in their meetings a session to review quality control outputs and to assess whether quality goals are being met or not and whether mitigation or contingency plans need to be put in place to tackle some quality aspects.

The PRoTECT Quality Manager – Dr. Georgios Kioumourtzis (DITSS) will be responsible for preparing and chairing the session related to Quality Assurance.

3.3 Documents

Most documents are written with contributions from several beneficiaries. In order to minimize the effort for handling such documents, it is important for all participants to follow agreed standards for formats and tools to be used in document editing and exchange. Every document must include an Executive Summary, a Table of Contents, and a Conclusion section.

3.3.1 Document header

For documents intended for formal use, a document header page will be used which specifies the following:

- Document Title
- Document Version
- Date of last update
- Lead Author/Main contributor
- Dissemination level (See Section 3.3.5.4)
- Relevant Work Package (optional)
- Relevant Task (optional)
- Relevant Deliverable (optional)
- Relevant Milestone (optional)
- Document Control

3.3.2 Document standards

All the documents to be made public or with external visibility (e.g. papers, presentations) as well as the final versions of all deliverables of the project must be released in Portable Document Format (PDF). The exchange of documents to and from the European Commission will be done using PDF format, unless MS Office (MS Office 2013 format) is required.

3.3.3 Nomenclature

File names should be as descriptive as possible, without being too long. Spaces must not be used in filenames. Where needed, instead of space, an underscore character should be used ("_"). All filenames must begin with "PROTECT_".

3.3.4 Document versions

Each document will have a main number and a sub-number separated by a dot. When a document is issued for the first time, it should be defined as a draft with the main number set to zero (v0.x). Usually the approval process requires that a document be circulated for comments among the interested beneficiaries. Upon receiving comments by the specified deadline, the author will make the proper modifications, therefore changing the version sub-number, without affecting the main number. Each document might have several contributing authors, but a Main Author must be clearly defined for each document. The online collaboration tool does not support document versioning and therefore the version numbers will be updated manually by the Main Author.

3.3.5 Document guidelines

Fonts and Language

Prefer to use 11pt size fonts, and either Calibri or Arial. The Language of the document should be set to "English (UK)" for the whole document.

3.3.5.1 Logo

The logo of the PRoTECT project is shown on the title page of each document. It is available for download from the file repository and is also included in all document templates.

3.3.5.2 Templates

The following six (6) templates and basic models for production of official project documentation will be available:

- Deliverables
- Deliverable Review Form
- Progress report
- Meeting agenda and minutes
- Presentations
- Financial progress report

The templates will be available for download from the online file repository, which can be accessed through the private area of the project website.

3.3.5.3 Acronyms

When using an acronym, the words should be written out in full when the acronym appears for the first time in the document. Alternatively, if many acronyms are used, a list of acronyms and their explanation should be provided at the beginning of the document. Although some acronyms are very common in certain fields, they should still be explained because readers with different backgrounds might not be familiar with those acronyms.

3.3.5.4 Document dissemination levels

Dissemination levels are indicated by one of the following codes:

PU = Public

PP = Restricted to other programme participants (including the Commission Services).

EU_REST = Restricted to a group specified by the consortium (including the Commission Services).

CO = Confidential, only for members of the consortium (including the Commission Services).

3.3.5.5 Document classified levels

There are four **levels of classification**[1]:

- TRÈS SECRET UE/EU TOP-SECRET **(TS-UE)**

TRÈS SECRET UE/EU TOP-SECRET is NOT used for the security scrutiny of research proposals.

- SECRET UE/EU SECRET **(SEC-UE)**

Use this classification for information which could seriously harm essential EU or national interests.

- CONFIDENTIEL UE/EU CONFIDENTIAL **(CON-UE)**

Use this for information which could harm essential EU or national interests.

- RESTREINT UE/EU RESTRICTED **(RES-UE)**

Use this for information which could be disadvantageous to those interests.

3.3.5.6 How to classify information?

IMPORTANT NOTE: None of the project deliverables have been classified as EU_RESTRICTED. However, in the following subsections we provide the guidelines provided by the European Commission[2] to classification of information.

The classification of information produced by research projects will normally depend on two parameters:

- the subject-matter of the research
- the type of the research/results and whether it is being done in simulated environments (e.g. serious gaming, etc.) or in real world experimentation

Terrorism research

What?

'Terrorism' refers to criminal offences committed with one (or more) of the following goals:

- seriously intimidating a population
- unduly compelling a government or international organisation to perform or abstain from performing any act
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or international organisation.4

How to deal with threat assessments?

[1] See. Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p.53.)

[2] GUIDE FOR HANDLING CLASSIFIED INFORMATION IN THE CONTEXT OF FRAMEWORK PROGRAMME RESEARCH PROJECTS

Threat assessments of terrorist organisations should be classified RESTREINT UE/EU RESTRICTED.

How to deal with vulnerability assessments?

Detailed evaluations of the current capacity of law enforcement staff to predict, detect, understand and respond to terrorist strategies, attacks and activity should be classified RESTREINT UE/EU RESTRICTED. General assessments of the vulnerability of urban locations to terrorist attack should also be classified RESTREINT UE/EU RESTRICTED. (See also Explosives and CBRN.)

How to deal with specifications?

Information on four main types of law-enforcement measures to counter terrorism should generally be classified RESTREINT UE/EU RESTRICTED:

- prediction: anticipating the decisions, behaviour, strategies, attacks and other activities of terrorist groups (including any techniques for predicting terrorist actions, such as decision-making and behavioural models)
- detection: identifying terrorist operatives and their activities or plans (e.g. through operational activities such as intelligence-gathering) and technical information on detection devices (such as sensors, pattern recognition, algorithms and operating systems)
- understanding: obtaining detailed information on processes such as radicalisation (e.g. through case studies of radicalised individuals and conceptual models detailing the radicalisation process, including information such as psychological indicators)
- response: action based on the three previous categories (e.g. operational and strategic information).

How to deal with capability assessments?

This covers:

- law enforcement agencies' capabilities to predict, detect and respond to terrorist activities in light of the potential advances detailed in specific projects
- the capabilities of individual state-of-the-art prediction and detection techniques and systems
- the capabilities of intervention programmes, particularly with regard to radicalisation
- the technological and operational ability of law enforcement personnel to respond to terrorist activities.

Detailed information on the performance of integrated systems to predict, detect, understand and respond to terrorism, in simulated environments, should be classified RESTREINT UE/EU RESTRICTED, as should information on the operating and technological capabilities of law enforcement personnel.

Information on the performance of integrated systems to predict, detect, understand and respond to terrorism, in real-life environments, should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with incidents/scenarios?

Detailed information on previous terrorist attacks and detailed scenarios of potential attack strategies should be classified RESTREINT UE/EU RESTRICTED.

Organised crime research

What?

'Organised crime' means a structured association of more than two persons acting together to commit serious offences to obtain, directly or indirectly, financial or other material benefits.5

How to deal with threat assessments?

Assessments of the threat(s) of organised crime should be classified RESTREINT UE/EU RESTRICTED.

How to deal with vulnerability assessments?

Detailed information on gaps in existing systems, tools and methodologies for predicting and detecting organised criminal activities should be classified RESTREINT UE/EU RESTRICTED.

How to deal with specifications?

The following specifications of measures to predict, detect and respond to organised crime should be classified RESTREINT UE/EU RESTRICTED:

- the identification and prioritisation of indicators
- detailed information on factors which influence the development of organised crime
- detailed specifications of technical countermeasures (e.g. the design, prototypes, characteristics, operation and requirements of key functional tools and systems and information on the software and algorithms employed)
- detailed information on the operational processes or strategies used by law enforcement personnel to respond to organised criminal acts.

How to deal with capability assessments?

Assessments of the capabilities of law enforcement personnel to predict and detect organised criminal activities including:

- detailed information or test reports on the capabilities of beyond the state-of-the-art detection subsystems (such as intelligent surveillance systems)
- demonstrations of systems and evaluations of detection devices, in both simulated and real-life environments
- assessments of the performance of prediction methods and models

should be classified RESTREINT UE/EU RESTRICTED.

Technical, operational and strategic capabilities of law enforcement personnel to respond to organised crime should also be classified RESTREINT UE/EU RESTRICTED

How to deal with incidents/scenarios

Detailed information on previous incidents or representative scenarios of organised crime should be classified RESTREINT UE/EU RESTRICTED.

3.3.5.7 Nature

For deliverables, the nature is indicated using one of the following codes:

R = Report,

P = Prototype,

D = Demonstrator,

O = Other

3.4 Deliverables

Each deliverable has a Deliverable Leader who will coordinate the production of the document, interacting as necessary with the beneficiaries involved. Before starting on the production of a deliverable, the Deliverable Leader will define the document structure and the contributions expected from each beneficiary. This is realised in a document named the DDP (Deliverable Development Plan) and will propose the calendar for the meetings (teleconferences) that may be necessary.

Upon receiving the inputs from different contributors for the deliverable, the Deliverable Leader will merge them into a single document. This first draft will then be circulated and asked for comments. Each beneficiary will check its consistency with the plans and give their feedback and approval. This iterative procedure will continue until all involved beneficiaries give approval. The Deliverable Leader will then prepare the final draft of the deliverable (**version 1.0**).

The final draft will then be sent to the Work Package Leader, to the Project Coordinator, and to the Quality Manager. The deliverable will then undergo a Quality review process detailed in Section 3.4.2 below. Once the Work Package Leader, Project Coordinator and Quality Manager have agreed on the Deliverable, the Project Coordinator will submit the requested number of copies to the European Commission.

3.4.1 Deliverable Development Plan (DDP)

The DDP is issued by the Deliverable Leader in order to clarify the main objectives of the Deliverable and to assign specific tasks to the different contributors. Its purpose is to provide a detailed plan on how the Deliverable will be completed successfully and on time. The DDP must sketch the structure of the future Deliverable, and therefore must contain a clear indication of:

1. Person responsible for the deliverable

2. Persons in charge of each section/task

3. A timetable for the deliverable development, setting deadlines for:

   a. Submission of contributions
   b. Production of first draft (version 0.1)
   c. Internal review (beneficiaries' comments)
   d. Productions of further draft versions (versions 0.x)
   e. Production of first complete version (version 1.0)
   f. Delivery to the Project Coordinator and Work Package Leader

At least six (6) weeks before the deliverable's deadline the Deliverable Leader will distribute the DDP. The Deliverable Leader can request the guidance of the Quality Manager for producing the DDP. Once the DDP is complete, it is sent to the Project Coordinator, the Quality Manager, and to all beneficiaries who are assigned with responsibilities in the DDP.

3.4.2 Deliverable Quality Process

The main technique that will be used for the document revision process is Peer Review. The Peer Review technique requires project team members to review each other's work. This technique is known to increase the level of quality of deliverables. It will also enable quality issues to be identified earlier in the project execution phase, and therefore increase the likelihood of quality issues being solved earlier.

In those cases, where all consortium members are involved in the deliverable creation process, a third person will be responsible for developing the review.

Peer Review policy description:

1. A list of peer reviewers for each deliverable will be created. Work Package Leaders, in coordination with the Quality Manager, will assign a reviewer for the deliverables within their work packages.

2. Reviewers will document the results of each peer using the Deliverable Review Form

3. Deliverable responsible partners will integrate the suggested quality improvements in the deliverable final versions.

Table 1 below shows the all deliverable and review partners. We have followed the rational that reviewing partners are those who will make use of that specific deliverable in an ongoing of future work within PRoTECT.

No.	Deliverable Name	Lead Part.	Reviewers
D1.1	Project Management Handbook (including report templates to be used by all WPs)	DITSS	TNO, JADS
D1.2	Risk Management and Quality Assurance	DITSS	KEMEA, JADS
D1.3	Mid-term progress report	DITSS	TNO, KEMEA
D2.1	Manual for vulnerability assessment	FESU	EINDHOVEN, DITSS
D2.2	Workshop results EINDHOVEN (Netherlands)	EINDHOVEN	MALAGA, EFUS
D2.3	Workshop results MALAGA (Spain)	MALAGA	LARISA, EFUS
D2.4	Workshop results LARISA (Greece)	DL	VILNIAUS, EFUS
D2.5	Workshop results VILNIAUS (Lithuania)	MUNBV	BRASOV, EFUS
D2.6	Workshop results BRASOV (Romania)	MUNBV	KEMEA, EFUS
D2.7	Aggregate Report	FESU	TNO, JADS
D3.1	Description of Best practices and Technologies/report	JADS	MALAGA, DITSS
D3.2	Technology Evaluation framework/report	TNO	DITSS, JADS
D3.3	Open calls/website	KEMEA	TNO, JADS
D3.4	Technology roadmap/report	JADS	KEMEA, EFUS
D4.1	Test scenarios	KEMEA	TNO, DITSS
D4.2	Exercise results	KEMEA	TNO, JADS
D4.3	Demonstration results	KEMEA	TNO, JADS
D4.4	Manual: A concise guide to contact table-top exercises for the protection of soft targets.	KEMEA	EFUS, DITSS
D5.1	Communications Plan & Dissemination Roadmap	DITSS	JADS, EFUS
D5.2	PRoTECT web site	DITSS	TNO, JADS
D5.3	Dissemination materials	KEMEA	DITSS, EFUS
D5.4	Securipedia content	TNO	DITSS, JADS
D5.5	1st Workshop results	DL	BRASOV, EFUS
D5.6	2nd Workshop results	MUNBV	EINDHOVEN, EFUS
D5.7	3rd Workshop results	EINDHOVEN	DITSS, EFUS

Table 1: Deliverable Owners and Reviewers

Once each deliverable has a clear owner for content preparation as well as the reviewers identified, the review process timeline will be as follows:

1. At least six weeks before the deliverable's deadline the owner of that deliverable will distribute a draft of the document with the proposed sections, requested contributions from other partners.

2. All contributors (including the owner of the deliverable) will prepare the content and pass it to the deliverable owner, who will consolidate, review and harmonise if needed.

3. At least two weeks before the deliverable's deadline the owner of the deliverable will distribute the first draft of the deliverable to the peer reviewers.

4. At least a week before the deliverable's deadline peer reviewers will review and provide feedback to the deliverable owner. Feedback will be provided using the Deliverable Review Form.

5. At least one week before the deliverable's deadline the deliverable owner (with the assistance of other contributors as needed) will update the deliverable taking into account the reviewers' feedback AND the deliverable owner will distribute the final version of the document to the Quality Manager and to the Project Coordinator.

6. At least one day before the deliverable's deadline the Quality Manager and to the Project Coordinator will provide their comments/feedback.

7. The day before the deliverable's deadline the owner will make whatever final modifications might be needed (if any) considering the feedback provided by the Quality Manager and the Project Coordinator.

8. The day of the deliverable's deadline, the Project Coordinator will submit to the Project Officer the final version of the deliverable.

3.4.3 Incidents in the delivery process

Several incidents can occur during the delivery process:

- The author foresees a delay in the delivery (the risk should have been detected before and remedy actions should already have been taken):
  - As soon as the author detects the potential delay, he/she must immediately make known such incident to the Work Package Leader, Project Coordinator and Quality Manager.
  - In any case, the delay must be made known well in advance. As a general rule, a delay of N days must be made known at least 2xN days before the due date.
  - Recovery actions must be defined and agreed with the Work Package Leader and the Project Coordinator in order to reduce the impact of the delay as much as possible. The Quality Manager should be informed about the recovery action.

- The Project Coordinator does not accept a delay due to lack of quality or due to other reasons:
  - As a first action, the author must immediately agree with the PC and the WPL on a recovery plan. The reviewers may be consulted on this recovery plan.
  - The Work Package Leader or the Project Coordinator may call a meeting of the Project Coordination Group in order to explain the problem and take the corresponding actions.
  - The Project Coordinator will inform the Project Officer about the problem and the corrective measures.

In the end, all project deliverables will be subject to acceptance by the following parties, in the order indicated:

1. Scientific-Technical and/or Management Representative of the partner responsible for the Deliverable

2. Work Package Leader (WPL)

4. Project Coordinator (PC)

5. Project Management Team (PMT)

6. Project Reviewers

7. European Commission (EC)

3.4.4 Deliverable Quality Checklist

The reviewers will use the Deliverable Review Form (template provided) which includes a checklist of items. These are shown in the following Table 2.

Check Point	Yes/No	Observations
Does the deliverable include an initial overview or executive summary section that is self-explanatory and easy to understand by all readers with a maximum length of 2 pages? Does this initial section describe what the reader will find in the rest of the document?		
Does the deliverable include a final conclusions section which lists the most remarkable things included in the document?		
Does the deliverable mention explicitly when it includes content copy-pasted from other documents? (Note: when the copy-pasted content is lengthy it is highly recommended to include just a summary of it on the document and then a reference to the original document)		
Does the document cover the objectives and task description stated in the DoA taking also into consideration the overall project vision?		
Is the Executive Summary in publishable form?		
Are the structure and appearance (layout, images, etc.) compliant with the Quality Plan?		

Table 2: PRoTECT Deliverable Check Points

3.5 Supporting Documents

Besides this Project Quality Assurance Management, the Quality Manager will also have at his disposal and will be able to consult a series of other documents that will act as supplementary sources of information:

- The Consortium Agreement (CA) which legally defines all aspects of cooperation between the Partners of the PRoTECT Consortium.
- The Description of Action (DoA) Part A and Part B which provide a complete and detailed description of the contractually agreed action (project and work plan).
- The Grant Agreement (GA) which sets out the rights and obligations and the terms and conditions applicable to the grant awarded to the beneficiaries for implementing the action.
- Relevant project deliverables, e.g. D1.1 “Project Management Handbook” (M3), as well as any other project deliverable that might be useful to the Quality Manager, e.g. all deliverables of WP1 reports etc.

4 Risk Management Plan

4.1 Introduction

The purpose of this Section is to provide a management framework to ensure that levels of risk and uncertainty are properly managed for the PRoTECT project. As risk management is an ongoing process over the life of a project, the Risk Register must be considered a 'snap shot' of relevant risks at one point in time.

The PRoTECT Risk Management Plan is based on [1] and will achieve its objectives by defining the following:

- the process that will be/has been adopted by PRoTECT to identify, analyse and evaluate risks during the remainder of the project;
- how risk mitigation strategies will be developed and deployed to reduce the likelihood and/or impact of risks;
- how often risks will be reviewed, the process for review and who will be involved;
- roles and responsibilities for risk management;
- how reporting on risk status, and changes to risk status, will be undertaken within PRoTECT and to the Project Coordination Group ;
- a complete Risk Register containing all risks identified for the Project, their current grading and the identified risk mitigation strategies to reduce the likelihood and seriousness of each risk.

Where required, the process of risk identification, assessment and the development of countermeasures will involve consultation with the Project Coordination Group, other relevant stakeholders and Project team members.

4.2 Risk Identification

Risk identification involves determining which risks or threats are likely to affect the project. It involves the identification of risks or threats that may lead to project outputs being delayed or reduced, outlays being advanced or increased and/or output quality (fitness for purpose) being reduced or compromised.

Multiple ways for accomplishing this step are available, ranging from engaging the project team in a brainstorming session, to consulting experienced team members, and to requesting opinions of experts not associated with the project. Typical methods of identifying risk are expert interviews, reviewing historical information from similar projects, conducting a risk brainstorming meeting, and using more formal techniques such as the "Delphi method".

Risk identification in PRoTECT will be realised with the engagement of experienced team members via brainstorming sessions.

4.3 Risk Categorization

Project planning outputs—scope, cost, time, and quality baselines—are what is at risk. Having full knowledge of them is crucial in developing response plans to counter risks to which the outputs will be exposed. These risks can be organized into different categories. In PRoTECT risks will be classified according to their effect on the project—scope, quality, and schedule.

4.4 Risk Assessment

Once risks have been identified, it is important to determine both the probability that each of the risks will occur, and the impact to the project if they occur. In order to determine the severity of the risks identified, a probability and impact factor has to be assigned to each risk. This process allows the project manager to prioritize risks based on the effect they may have on a project.

For our risk assessment, we will use qualitative criteria that is a nonnumeric probability scale [2], as follows:

Likelihood

near certain - 5
highly likely - 4
Likely - 3
low likelihood -2
very unlikely - 1

Table 3: PRoTECT Risk Probability Scale

The next step is to assess the impact of each risk, again on a discrete scale, as follows:

Impact

very high impact - 5
high impact - 4
medium impact - 3
low impact -2
very low impact - 1

Table 4: PRoTECT Impact Scale

Although nonlinear formulas can be employed, linear formulas can be used [3] to measure the severity of a risk, such as:

Severity = Probability × Impact

Severity Scales

Scale	
1-3	**LOW**
4-7	**MEDIUM**
8-10	**SERIOUS**
>10	**HIGH**

Table 5: Severity Scale

Severity

	Impact				
Likelihood	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**
2	**2**	**4**	**6**	**8**	**10**
3	**3**	**6**	**9**	**12**	**15**
4	**4**	**8**	**12**	**16**	**20**
5	**5**	**10**	**15**	**20**	**25**

Table 6: PRoTECT Risk Assessment Scale

4.5 Risk Response

Once risks have been qualitatively defined, the project team must determine how to address the risks that have the greatest potential for affecting the project. This section of the risk management plan explains the response options and actions that are available to the project team in managing the risks.

Any suitable risk response action essentially falls into one of the four broad categories of response strategies: avoidance, transference, mitigation, and acceptance of risk [4]. Changing the project plan or condition to eliminate the selected risk event is risk avoidance. For instance, if faced with the risk of not having an available expert to perform a quality business process analysis, the risk can be avoided by hiring such an expert.

Risk transfer simply involves shifting consequences of a risk event to a third party, along with the ownership of the response. If, for example, projects within a firm have historically been exposed to a risk of slow quality testing from their internal capabilities, the risk can be transferred to a third party by hiring a professional firm to do the testing.

The intent of risk mitigation is to lower the probability or impact (or both) of an unfavourable risk event to an acceptable threshold. A fairly common risk for many projects is the potential decision delays caused by the busy schedules of the project.

This risk can be mitigated by a number of ways, such as reducing the number of major milestone decision points or the delegation of decision authority to one of the executive's direct reports.

The three response strategies—avoidance, transference, and mitigation—are deployed when risks they are responding to are among the highest-ranked risks.

In PRoTECT we have already in place both a quality process and risk process but not any additional budget for risk transfer to any external third party. The main strategies we will follow are avoidance and mitigation of risks. Obviously, these responses will be incorporated in the project plan.

4.6 Risk Monitoring

Most of a project managers attention with respect to risk management tends to focus on the activities associated with risk identification, risk assessment, and risk response planning. Where project managers

historically spend less time and focus are the activities associated with risk monitoring. It is not uncommon, that project managers continue to be surprised when a risk event they had identified earlier, but were not monitoring, suddenly turns into an issue. To protect against this, diligent risk monitoring must be a part of every project manager's activities and he or she must have tools in their Project Management Toolbox to effectively perform this function.

There are four primary elements involved with risk monitoring activities: (1) systematically track the status of risks previously identified; (2) identify, document, and assess any new risks that emerge; (3) effectively manage the risk reserve; and (4) capture lessons learned for future risk identification and assessment efforts.

This section of the risk management plan should discuss how the project risks would be monitored on an ongoing basis. The key to risk monitoring is to ensure that it is used throughout the project cycle and includes the identification and use of trigger conditions that will accurately indicate if the probability of a risk occurring is increasing or has passed.

As stated previously, it is advantageous to the project manager to assign risk owners to high-level risks. A primary role of the risk owner is to continuously monitor the status of the risks he or she are responsible for, and periodically report that status to the project manager and team.

Since there is a time element to when risk events may affect a project, not all risks should be reported upon in each status meeting. Rather, as risk event triggers approach on the project schedule, the project manager should ensure that the appropriate risk owner provides the status updates at the appropriate time.

4.7 Risk Register

The risk register provides a record of identified risks relating to a project and serves as the central repository for all open and closed risk events [5]. The risk register typically includes a description of each risk event, a risk event identifier, risk assessment outcome, a description of the planned response, and summary of actions taken and current status.

The risk register can be represented in a number of ways, such as a database, a paragraph-style document, or a spreadsheet. The spreadsheet style is by far the most commonly used format. Therefore, in PRoTECT the risk register will be developed in a spreadsheet because it presents all the information pertaining to project risks without the user having to scroll through several pages. The current version of the PRoTECT Risk Register is presented in **Error! Reference source not found.** and it will be available online to all project partners in P RoTECT shared repository in [6].

The main elements of the PRoTECT Risk register are defined in the following paragraphs.

Risk Identifier

Each risk will have a unique identifier for cataloging and monitoring purposes. Each risk will be identified by its relation to the Work Breakdown Structure (WBS). For instance, risks associated with Management and Coordination of the Action (WP1) will be identified as R1.1, R1.2, and so on.

Risk Description

The risk description is related to the identification of risk events. We will use the "IF/THEN" format not only to describe the risk, but also to describe the potential consequences: "IF" this occurs (risk event), "THEN" that will be the outcome (consequences).

Dates

For risk timing, aging, and tracking purposes, the risk register will have a date component. Common and useful dates are the date that the risk was identified, the risk trigger date (when the risk is likely to occur), and the closure date.

Severity

In order to prioritize the risk events a severity component will be included in the risk register. A quantitative qualifier will represent the severity of a risk. Severity will be evaluated from two perspectives: i) the probability a risk event will occur, and ii) the severity of the impact if it does indeed occur. Total risk severity must factor in both probability and impact perspectives.

Response

For each risk event, the Project Coordination Group will decide to manage. A response approach must be decided upon and documented in the register for reference and tracking purposes. For low-priority risks and others that the team decides not to manage, the default response is *acceptance*. The risk register will contain a field to identify the chosen response for each risk event.

Owner

Every risk event, regardless of priority, will have an owner assigned. The risk register therefore will provide the owner component. The risk owner is the person who is responsible for monitoring the risk event and initiating the risk response action if and when it is necessary.

Status

Risk events are dynamic by nature, meaning they can change state over time. To facilitate communication, the risk register will include a risk status field. The most common risk statuses include *open, monitoring trigger event, response initiated*, and *closed*.

4.8 Roles and Responsibilities

Project Coordination Group

Ultimate responsibility for ensuring appropriate risk management processes are applied rests with the Project Coordination Group, and it should be involved in the initial risk identification and analysis process. The Project Risk Manager will provide the Project Coordination Group with clear statements of the project risks and the proposed risk management strategies to enable ongoing management and regular review.

The Project Coordination Group will review the project risks on a monthly basis via updated information provided in the Project Meetings and provide advice and direction to the Project Manager. The Project Coordination Group will also be provided with an updated Risk Register for consideration, as required, when additional threats emerge or the likelihood or potential impact of a previously identified risk changes.

Risk Manager

The Project Risk Manager will be responsible for:

- Development and implementation of a Project Risk Management Plan;

- Organisation of regular risk management sessions so that risks can be reviewed and new risks identified;
- Assessment of identified risks and developing strategies to manage those risks for each phase of the project, as they are identified;
- Ensure that risks given high priority are closely monitored; and
- Providing regular Status Reports to the Project Coordination Group noting any risk with high severity and specifying any changes to the risks identified during each phase of the project and the strategies adopted to manage them.

Project Partners

All members of the Project Team will be responsible for assisting the Project Risk Manager in the risk management process. This includes the identification, analysis and evaluation of risks and continual monitoring throughout the project life cycle.

5 Conclusions

We presented in this document the main components of the PRoTECT Quality Assurance and Risk Management plan.

We elaborated on the how quality management will be realised by providing goals and associated metrics along with quality control mechanisms.

We also provided guidance on document handling and quality control procedures along with specific responsibilities.

The production of project deliverables, the methodology to be followed by project partners with associated templates were also discussed in detail.

In the second part of this deliverable we provided a management framework to ensure that levels of risk and uncertainty are properly managed for the PRoTECT project. One essential part of risk management is related to risk assessment, in which we discussed how a risk is assessed in terms of probability of occurring (likelihood), its impact and how severity is scaled. At the end of the risk management plan, we provided the initial entries in the PRoTECT Risk Registry that is a lived spreadsheet available online in the project shared repository for easier access and review by all responsible functions and partners.

ANNEX I. REFERENCES

[1] Project Management Toolbox, 2nd Edition, Russ J. Martinelli, Dragan Z. Milosevic, John Wiley & Sons, Inc., Hoboken, New Jersey, 2016, ISBN 978-1-118-97312-7 (hard back), 978-1-118-97321-9 (ePDF), 978-1-118-97320-2 (ePUB), and 978-1-119-17482-0 (oBook).
[2] Graves, R. "Open and Closed: The Monte Carlo Model." PM Network 15 (2): 48–52, 2001.
[3] Graves, R. "Qualitative Risk Assessment." PM Network 14 (10): 61–66, 2000.
[4] Project Management Institute, 2013.
[5] TSO. Managing Successful Projects with PRINCE2. (London, England: TSO, 2012).
[6] PRoTECT Risk Register available for project in this link

ANNEX II. PRoTECT Risk Register

PRoTECT Project Risk Registry

Risk Re	Risk Description		Dates			Analysis			Response & Acti	Owner	Status
	IF	THEN	Opened	Triggered	Closed	Likelihood	Impact	Severity			
R1.1	Travel budget not adequate to support all project activities	lack of participation of project partners in physical meetings	1-Nov-18			3	4	12	Mitigate: plan for combined meetings and check project budget every 6	Project Manager	Inactive
R2.1	project outcomes release sensitive information	possible information leak to unauthorized parties	1-Nov-18			3	4	12	Avoid: Request Project Security Officer to review all deliverables	Project Manager	Active especially for deliverables D2.2, D2.3,D2.4,D2.
R2.2	vulnerability assessment tool not mature	incomplete vulnerability assessments	1-Nov-18	1-Jan-18		3	4	12	Mitigate: Start with the existing tool in the first assessment and take actions to find a more complete one	Project Manager	Active
R2.3	vulnerability assessments not completed in time	risks in project planning in WP3 and WP4	1-Nov-18			3	3	9	Accept	EFUS	Inactive
R3.1	low interest to open call for ideas	less attractive technologies to test and demonstrate within WP4	1-Nov-18			3	4	12	Mitigate: Be prepared to extend the duration of the project for 6 months	KEMEA	Inactive
R3.2	delays in subcontracting in WP3	out of schedule start on activities in WP4	1-Nov-18			3	5	15	Mitigate: Be prepared to extend the duration of the project for 6 months	KEMEA	Inactive
R4.1	test sites not available for technology demonstrations	incomplete project results and impact	1-Nov-18			2	4	8	Mitigate: be prepared to ensure at least one existing test site always available (e.g. EINDHOVEN living lab)		Inactive
R4.2	low participation of municipal authorities in tabletop exercises	low exploitation level of project results	1-Nov-18			3	4	12	Mitigate: plan for participation of external stakeholders via EFUS and ENLETS		Inactive
R5.1	Workshops not organised as initially planned	some impact in project exposure	1-Nov-18			3	2	6	Accept		Inactive