NANCY

An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution [GA: 101096456]

Deliverable 1.1

Project and Risk Management Handbook

Programme: HORIZON-JU-SNS-2022-STREAM-A-01-06

Start Date: 01 January 2023

Duration: 36 Months

Document Control Page

Deliverable Name	Project and Risk Management Handbook
Deliverable Number	D1.1
Work Package	WP1 - Project, Innovation & Data Management
Associated Task	T1.1 - Administrative & Financial Coordination
Dissemination Level	Public
Due Date	31 January 2022 (M01)
Completion Date	30 January 2022 (M01)
Submission Date	31 January 2022 (M01)
Deliverable Lead Partner	UOWM
Deliverable Author(s)	Panagiotis Sarigiannidis (UOWM), Alexandros-Apostolos Boulogeorgos (UOWM), Thomas Lagkas (UOWM), Dimitrios Pliatsios (UOWM), Anna Triantafyllou (UOWM), Athanasios Liatifis (UOWM), Stylianos Trevlakis (INNO), Lamprini Mitsiou (INNO), Konstantinos Kyranou (SID), Ioannis Makris (MINDS)
Version	1.0

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	10 January 2023	Structure definition	Panagiotis Sarigiannidis, Dimitrios Pliatsios	UOWM
0.2	14 January 2023	Initial version of Sections 1-5	Panagiotis Sarigiannidis, Dimitrios Pliatsios	UOWM
0.3	16 January 2023	Review of Sections 1-5 and Contribution to Sections 6 and 7.	Thomas Lagkas, Alexandros-Apostolos A. Boulogeorgos	UOWM
0.4	17 January 2023	Review comments addressed	Dimitrios Pliatsios	UOWM
0.5	20 January 2023	Contribution to Sections 6 and 7	Anna Triantafyllou	UOWM
0.6	21 January 2023	Contribution to Section 7	Stylianos Trevlakis	INNO
0.7	21 January 2023	Contribution to Section 7	Konstantinos Kyranou	SID
0.8	22 January 2023	Acronyms definition	Lamprini Mitsiou	INNO
0.9	23 January 2023	Contributions to Sections 6 and 7	Ioannis Makris	MINDS
0.10	24 January 2023	Review of Sections 6 and 7	Panagiotis Sarigiannidis	UOWM
0.11	25 January 2023	Review comments addressed	Anna Triantafyllou, Athanasios Liatifis	UOWM

| 0.12 | 26 January 2023 | Revision of partner contacts | Thomas Lagkas, Dimitrios Pliatsios | UOWM |
| 1.0 | 30 January 2023 | Final version | Panagiotis Sarigiannidis | UOWM |

Internal Review History

Name	Organisation	Date
Stylianos Trevlakis	INNO	27 January 2023
Ioannis Makris	MINDS	28 January 2023

Quality Manager Revision

Name	Organisation	Date
Anna Triantafyllou	UOWM	30 January 2023

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Description
AI	Artificial Intelligence
B5G	Beyond Fifth Generation
CA	Consortium Agreement
CM	Communication Manager
DM	Dissemination Manager
DX.Y	Deliverable X.Y
EAB	External Advisory Board
EC	European Commission
EIM	Exploitation and Innovation Manager
EU	European Union
F2F	Face-to-Face
FO	Financial Officer
GA	Grant Agreement
IPR	Intellectual Property Right
LEAR	Legal Entity Appointed Representative
MEC	Multi-access Edge Computing
PC	Project Coordinator
PM	Participant Managers
PMO	Project Management Office
PO	Project Officer
QRM	Quality and Risk Manager
RAN	Radio Access Network
RP	Reporting Period
RPN	Risk Priority Number
SB	Sustainability Board
SC	Scientific Coordinator
SDN	Software Defined Network
STC	Scientific and Technical Committee
TAFGL	Technology Adopters Focus Group Liaison
TC	Technical Coordinator
TRL	Technology Readiness Level
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable presents the structures, tools, and processes that will be used for the administration and implementation of the NANCY project. It aims to serve as an overview of the administration and collaboration guidelines of the project. Through this deliverable, the NANCY consortium will establish a common understanding of the guidelines and processes to be adopted for the administration and implementation of the project. It is complimentary to the grant agreement (GA) and the consortium agreement (CA).

In this deliverable, the project administration structures and bodies are identified, namely: (i) the project coordinator (PC), (ii) the project general assembly, (iii) the scientific and technical committee (STC), (iii) the technical coordinator (TC), (iv) the scientific coordinator (SC), (v) the financial officer (FO), (v) the quality and risk manager (QRM), (vi) the communication manager (CM), (vii) the dissemination manager (DM), (viii) the exploitation and innovation manager (EIM), (ix) the project management office (PMO), (x) the participant managers (PM), (xi) the external advisory board (EAB), (xii) the technology adopters focus group liaison (TAFGL), and (xiii) the sustainability board (SB). In addition, the deliverable emphasizes the key documents that will be taken into consideration throughout the project's duration, namely the GA, the CA, and the current deliverable "D1.1 – Project and Risk Management Handbook". Additionally, it presents the project collaboration tools and processes, such as the collaboration platform, teleconference tool, project meetings, deliverables, and presentation templates, as well as the deliverable review process. Finally, the deliverable introduces the risk management procedures that will be followed throughout the NANCY's duration in order to ensure the successful implementation of the project.

1. Introduction

NANCY consortium combines multidisciplinary competences and resources from the academia, industry as well as research community that focuses on artificial intelligence (AI) and network analytics, distributed blockchain, resource allocation, and orchestration, beyond the fifth generation (B5G) radio access network (RAN), semantic communications, smart pricing, and cyber security. Figure 1 illustrates consortium partners in relation to the NANCY value chain. NANCY consortium consists of twenty-two (22) partners representing research organizations (i.e., research institutes, and universities), technology providers, testbed providers (end-users), and industrial partners (including nine (9) SMEs) from eight (8) EC member states, i.e., Cyprus, France, Germany, Greece, Italy, Luxemburg, Slovenia, and Spain-as depicted in Figure 2. This multinational cooperation is essential to implement the rising requirements of the next generation of intelligent connectivity solutions, based B5G RAN, smart pricing, AI and cyber security in Europe (EU) and beyond. To make the most out of its partners' collaboration, NANCY establishes a number of communication channels, tools, and procedures that are described in this deliverable.
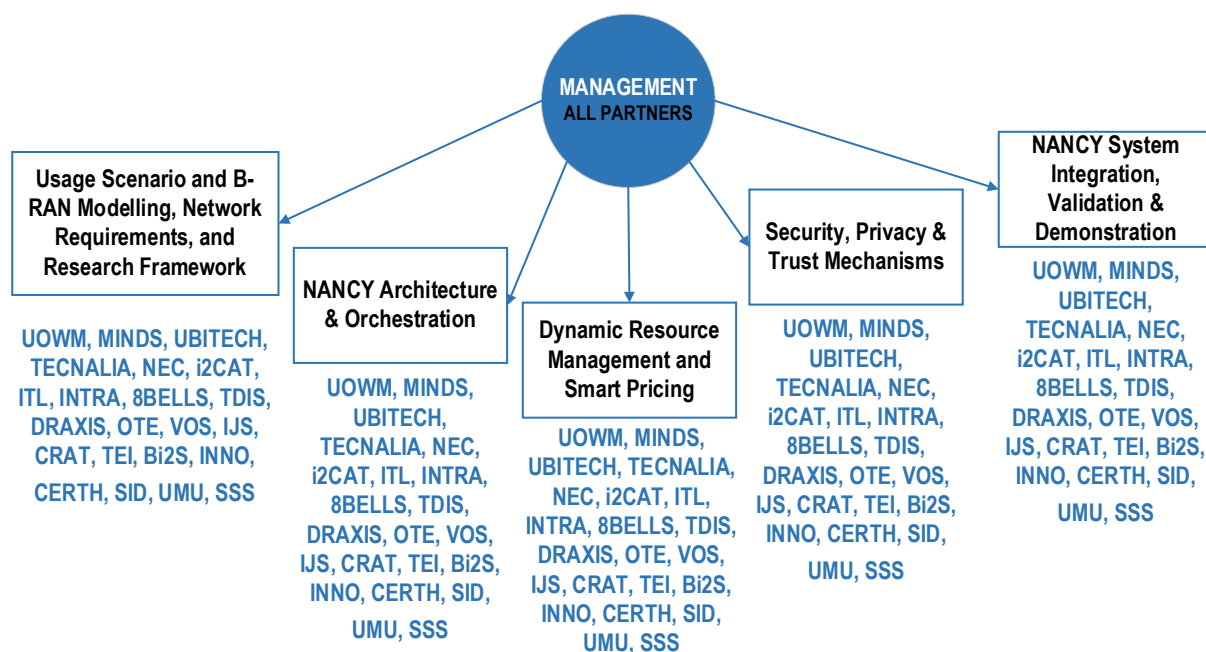
Figure 1: NANCY consortium interactions.

The rest of this section is organized as follows:

- Section 1.1 sets the objectives of the deliverable "D1.1 - Project and Risk Management Handbook";
- Section 1.2 documents the relations of the deliverable "D1.1 - Project and Risk Management Handbook" with the rest of the documents of the NANCY project; and
- Section 1.3 reports the structure of the deliverable "D1.1 - Project and Risk Management Handbook".
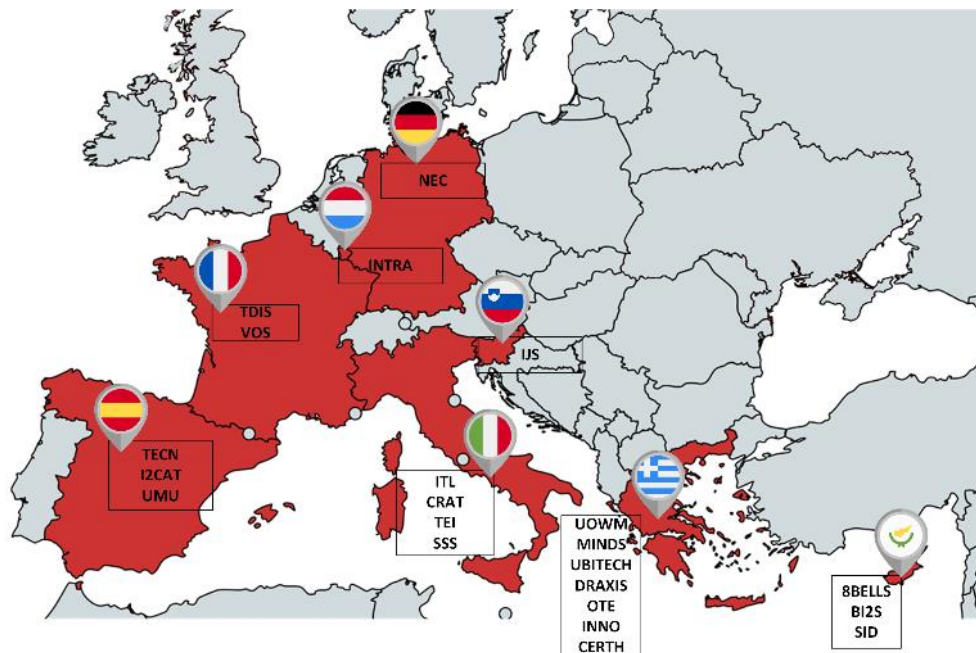
Figure 2: NANCY's consortium geographical distribution.

1.1. Purpose of the Deliverable

The management of the project has the following objectives:

- To guarantee that the NANCY project is conducted in accordance with European Commission (EC) rules and guidelines and it is in-line with the EC related legislations;
- To achieve the technical goals and objectives of the NANCY project within the agreed budget and time;
- To ensure effective communication between the partners and coordinate their work;
- To maximize the potential for exploiting and disseminating results and active involvement of industry through an external advisory board (EAB);
- To define the quality policy, including quality objectives for the project as well as to identify the deliverables quality assurance procedure;
- To manage properly foreground and intellectual property rights (IPR) related issues;
- To guarantee that all the project decisions are made based on data and factual information;
- To provide solutions to problems or conflicting situations;
- To define the quality assurance policy, including quality goals for the NANCY project;
- To create a risk management procedure;
- To guarantee that an infrastructure is set up in order to support the above.

Motivated by this and in order to present the NANCY project management procedures and the risk coordination policies, this deliverable (D1.1) repots the day-to-day rules of the NANCY project: documents and deliverables handling, project planning, and manpower, meeting organisation, internal reporting and information management, external information management, list of personal with corresponding responsibilities. It details beyond the terms of the EC GA and the CA, the internal project rules and guidelines concerning the daily management of foreground and IPR. All tools and processes are specified for monitoring and managing the project's progress. In more detail, the NANCY project management processes include the design and execution of a thorough monitoring plan for the implementation of the tasks throughout the project's duration. This plan includes procedures for

organizing, monitoring, and reviewing the performance and progress of the NANCY project. In this direction, the following activities are defined:

- **Partner communication and engagement**: Coordinating the communication and cooperation among partners as well as resolving conflicts.
- **Scientific and technical progress monitoring**: Organizing, monitoring, reviewing, and reporting the progress of all WPs. Based on this process, potential needs for amendments may arise.
- **Financial management and reporting**: Communicating with the funding authorities, establishing and maintaining financial records, managing EC installments, and distributing the shares based on the CA.
- **Risk control**: Documentation of current risks in the risk register; early detection and identification of emerging risks. According to the findings, amendments may be needed.
- **Innovation and quality progress monitoring**: Ensuring that the work carried out and the deliverables are of high quality.

1.2. Relation to other Deliverables

This deliverable's relations with other deliverables od the NANCY project are illustrated in Figure 3. This deliverable receives inputs from the GA and the CA. Also, it provides input to Task 2.1 of work package (WP) 2 and its respective deliverable, namely D2.1 – NANCY Requirements Analysis.
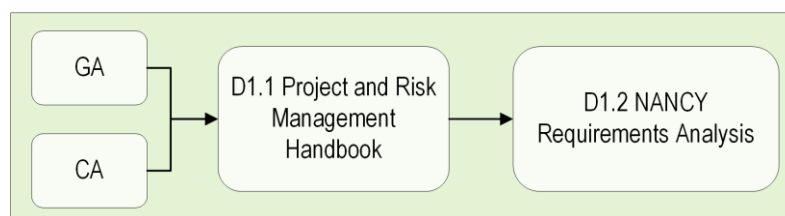
Figure 3: Relation to other deliverables.

1.3. Structure of the Deliverable

The deliverable is organized as follows:

- **Section 2 – Project Management Structure**: It defines the project management structure, which is in-line with the GA and CA.

- **Section 3 – Reference Documents**: This section lists the documents that should be considered by the consortium members for the day-to-day project management.

- **Section 4 – Project Management Processes**: This section overviews the processes and available tools for collaboration among partners and the management of the project.

- **Section 5 – Communication and Dissemination Activities**: This section presents the templates, the file naming, and versioning, and outlines the communication and dissemination requirements.

- **Section 6 - Quality Management:** This section provides an overview of the quality management process that will be followed towards ensuring high-quality project outputs.

- **Section 7 – Risk Management:** This section introduces the risk management process for the early detection, identification, and quantification of potential risks. Also, this section lists several administrative risks, technical and scientific risks, and business risks, as well as their respective mitigation plans.

- **Section 8 – Conclusion**: This section summarizes and concludes the deliverable.

2. Project Management Structure

This section offers a thorough overview of the project management structure as specified in Section 3.2 and in the paragraph "Project management principles and structure" of the NANCY proposal.
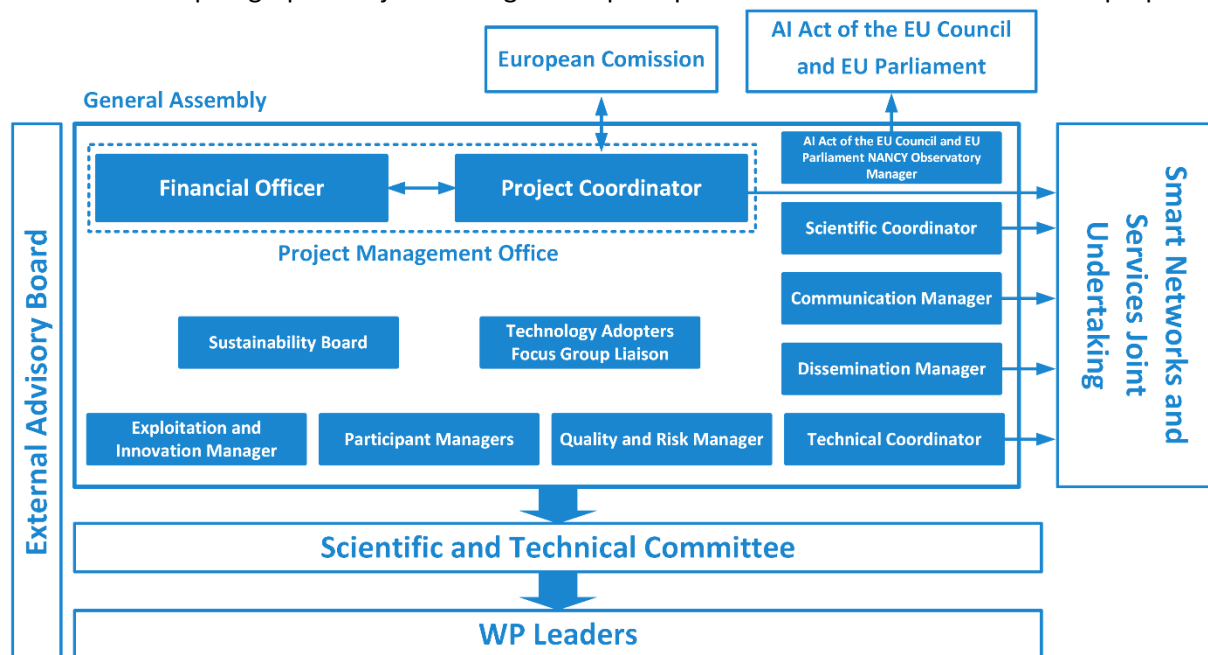
Figure 4 graphically presents the NANCY project management structure. It consists of: (i) the general assembly, (ii) the scientific and technical committee (STC), (iii) the project management office (PMO), and (iv) the external advisory board (EAB).
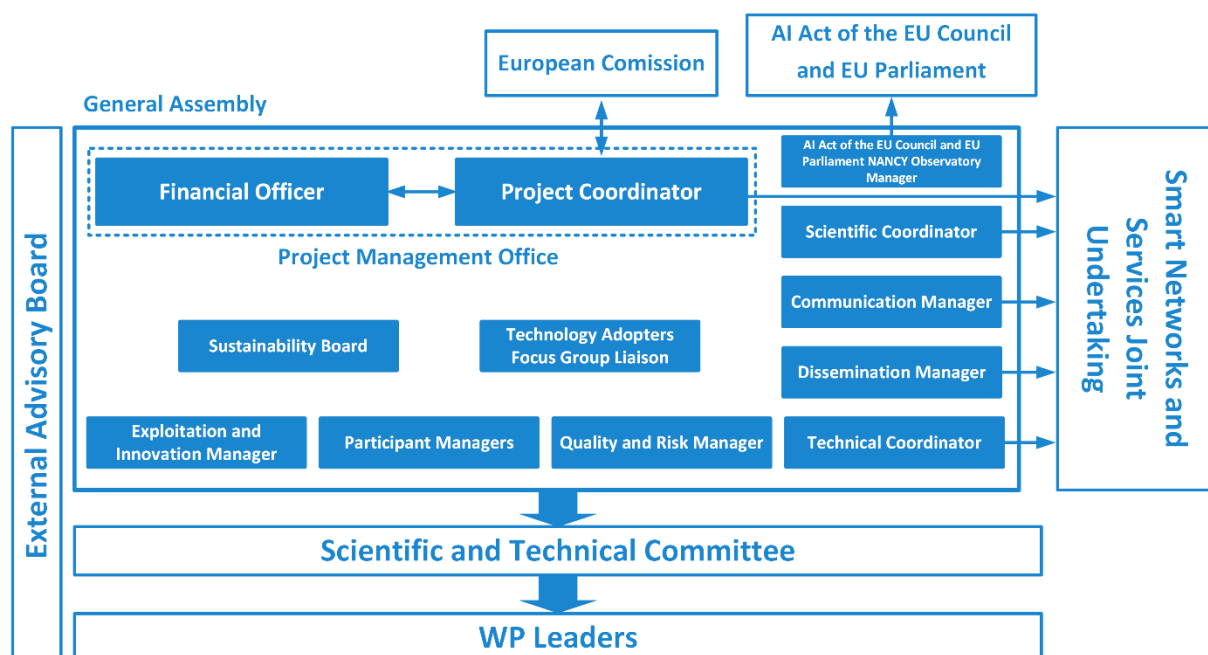
Figure 4: Project management structures and NANCY's administrative and technical bodies.

The rest of this section is organized as follows:

- Section 2.1 presents the role and composition of the GA;

- Section 2.2 briefly presents the role and organization of the STC. The members of STC are identified in this Section and its communication list is given.
- Section 2.3 reports the responsibilities and role of the PMO. Also, the members of the PMO are presented in this Section.

2.1. General Assembly

Role and responsibilities: The general assembly responsibility is to oversee the project's formal follow-up and to make important decisions, mostly on:

- Contract and CA amendment;
- Contract termination and actions against under-performing partners;
- Replacement of under-performing partners by choosing new contractors to sign the contract and CA;
- Budget follow-up and transfers; and
- Deciding on major changes and technical roadmaps in the project.

Composition: Each partner is represented by one member of the general assembly. As presented in Table 1, each partner designates a senior representative who will oversee the budget, be able to make decisions consistently, and represent the interests of the contractor. Moreover, the following members participate in the general assembly: (a) the Project Coordinator (PC) – Prof. Panagiotis Sarigiannidis (UOWM), (b) the Technical Coordinator (TC) – Dr. Alexandros-Apostolos A. Boulogeorgos (UOWM), (c) the Scientific Coordinator (SC) – Dr. Thomas Lagkas (UOWM), (d) the Quality and Risk Manager (QRM) – Ms. Anna Triantafyllou (UOWM), (e) the Dissemination Manager (DM) – Ms. Christina Dolianidi (DRAXIS), (f) the Communication Manager (CM) – Mr. Konstantinos Kyranou (SID), (g) the Exploitation & Innovation Manager (EIM) – Dr. Ioannis Chochliouros (OTE), (h) the NANCY Technology Adopters Focus Group Liaison (NANCY-IFGL) – Prof. Antonio Skarmeta (UMU), i) NANCY Head of Sustainability Board (SB) – Dr. Athanasios Tziouvaras (Bi2S), and j) AI act of the council of EU and EU Parliament NANCY observatory manager – Prof. Panagiotis Sarigiannidis (UOWM). UOWM, the coordinating partner, serves as the general assembly chair.

Table 1: General Assembly Members.

General Assembly		
Mailing List**:** nancy-ga@lists.uowm.gr		
Role	**Name**	**Email**
Chairman and PC	Panagiotis Sarigiannidis (UOWM)	psarigiannidis@uowm.gr
Vice chairman and TC	Alexandros-Apostolos A. Boulogeorgos (UOWM)	aboulogeorgos@uowm.gr
SC	Thomas Lagkas (UOWM)	tlagkas@uowm.gr
QRM	Anna Triantafyllou (UOWM)	atriantafyllou@uowm.gr
DM	Christina Dolianidi (DRAXIS)	chdolianidi@draxis.gr
CM	Konstaninos Kyranou (SID)	kkyranou@sidroco.com
EIM	Ioannis Chochliouros (OTE)	ichochliouros@oteresearch.gr
NANCY-IFGL	Antonio Skarmeta (UMU)	skarmeta@um.es
NANCY Head of SB	Athanasios Tziouvaras (Bi2S)	attziouv@bi2s.eu
AI act of the council of EU and EU Parliament NANCY observatory manager	Panagiotis Sarigiannidis (UOWM)	psarigiannidis@uowm.gr

PMs	Please refer to Table 2.

Meetings: By default, the GA will meet once a year. Ordinary meetings of the GA must be held concurrently with project meetings, however, under the norms and regulations of the CA, the coordinator or any partner may call an extraordinary meeting of the GA at any time. GA meetings can be held by teleconference to save on travel expenses.

Next, the role of the PC, TC, SC, PM, QRM, DM, CM, EIM, NANCY-IFGL, NANCY Head of SB, AI act of the council of EU, EU Parliament NANCY observatory manager and PMs roles and responsibilities are described. In more detail, the PC, TC and SC responsibilities are reported in Sections 2.1.1, 2.1.2, and 2.1.3, respectively. Moreover, in Section 2.1.4 the PMs are defined. The QRM, DM, and CM roles are reported in Sections 2.1.5, 2.1.6, 2.1.7, respectively. Also, in Sections 2.1.8, 2.1.9, 2.1.10, 2.1.11 the responsibilities of the EIM, NANCY-TFGL, NANCY Head of SB, AI act of the council of EU are presented.

2.1.1. Project Coordinator (PC)

The PC is responsible for the overall communication, administration, and coordination of the project. Specifically, the PC manages the liaisons with the funding authorities, the cooperation among partners, and the communication with subcontractors. Furthermore, the PC provides recommendations to the quality and risk manager (QRM), that monitoring and assessing also the progress of the reports and deliverables. The PC is the chair of the project meetings, relations, and dissemination. The PC reports to the GA and ensures that all payment installments are timely and accurately conducted. The PC is the liaison between the NANCY and the financial department of each participating partner, addressing potential contingencies. The PC works closely with the Work Package Leaders (WPLs) for coordinating all kinds of dependencies between various WPs and tasks, as well as reviewing and approving the deliverables and reports. The PC will also represent NANCY to the SNS JU Steering Board. The PC of NANCY is Prof. Panagiotis Sarigiannidis (UOWM), while Dr. Dimitrios Pliatsios (UOWM) serves as deputy PC.

2.1.2. Technical Coordinator (TC)

The TC coordinates and manages the integration of all technical results and implementations. The TC ensures that the technical project objectives are timely achieved. The TC is expected to lead the technical activities and resolve any technical issues that might arise. The PC will also represent NANCY to the SNS JU Technical Board. The TC of NANCY is Dr. Alexandros-Apostolos Boulogeorgos (UOWM), while Dr. Stylianos Trevlakis (INNO) serves as deputy TC.

2.1.3. Scientific Coordinator (SC)

The SC coordinates and manages all scientific decisions and addresses any research issues that might arise. The SC works closely with the TC, the dissemination manager (DM) as well as all the technical work package leaders (WPL) and monitors the technical advancements of the NANCY project as well as the scientific advances that are related to the NANCY project. The SC is responsible for the identification of the key scientific results of the project and the creation and implementation of optimal exploitation plans. Moreover, the SC is responsible for delivering high-quality scientific results by monitoring the scientific publications that are generated in the context of the project. The SC of NANCY is Dr. Thomas Lagkas (UOWM).

2.1.4. Participant Manager (PM)

Each partner designates a PM, who will represent the respective organization in the GA. Also, each PM participates in voting procedures regarding administrative or technical issues.

Table 2: Participant Manager Members.

No.	Partner	Representative	
		Name	E-mail
1	UOWM	Panagiotis Sarigiannidis	psarigiannidis@uowm.gr
2	UBITECH	Athanasios Bouras	bouras@ubitech.eu
3	TECNALIA	Cristina Regueiro	Cristina.Regueiro@tecnalia.com
4	NEC	Sebastien Andreina	sebastien.andreina@neclab.eu
5	I2CAT	Hatim Chergui	hatim.chergui@i2cat.net
6	ITL	Antonino Albanese	antonino.albanese@italtel.com
7	INTRA	Olga Segou	Olga.Segou@netcompany-intrasoft.com
8	8BELLS	Emmanouil Kafetzakis	mkafetz@8bellsresearch.com
9	TDIS	Jean-Paul Truong	jean-paul.truong@thalesgroup.com
10	DRAXIS	Anastasios Karakostas	akarakos@draxis.gr
11	OTE	Ioannis Chochliouros	ichochliouros@oteresearch.gr
12	VOS	Alvise Rigo	a.rigo@virtualopensystems.com
13	IJS	Blaz Bertalanic	Blaz.Bertalanic@ijs.si
14	CRAT	Giacinto Losquadro	giacinto.losquadro@crat.eu
15	TEI	Cosimo Zotti	cosimo.zotti @ericsson.com
16	Bi2S	Athanasios Tziouvaras	attziouv@bi2s.eu
17	INNO	Stylianos Trevlakis	trevlakis@innocube.org
18	CERTH	Dimitrios Kavallieros	dim.kavallieros@iti.gr
19	SID	Konstantinos Kyranou	kkyranou@sidroco.com
20	UMU	Antonio Skarmeta	skarmeta@um.es
21	SSS	Alessandro Biondi	alessandro.biondi@santannapisa.it
22	MINDS	Ioannis Makris	imakris@metamind.gr

2.1.5. Quality and Risk Manager (QRM)

The QRM is responsible for ensuring that all project outcomes, deliverables, and results are of high quality. The QRM is also responsible for the early identification, assessment, and mitigation of administrative and technical risks. Having in mind that in a low technology readiness level (TRL) project, like NANCY, a risk may have a significant impact on the project schedule and objectives; thus, leading to contractual issues, NANCY consortium has appointed a QRM, during the proposal preparation phase. The QRM will periodically review the project progress and the risk items table, which was initially defined in the proposal and is redefined in the second part of this deliverable, in order to ensure that NANCY is in-line with its pillars and technical objectives. Also, the QRM will be responsible for keeping up-to-date the risk management table that is provided in Section 7. To achieve this, the QRM will interact with the GA and the PC. The QRM of NANCY is Ms. Anna Triantafyllou (UOWM).

2.1.6. Dissemination Manager (DM)

The DM leads and organizes the dissemination activities of the project, as well as any standardization and clustering activities. The DM will also represent NANCY to the SNS JU Communications Team. The DM of NANCY is Ms. Christina Dolianidi (DRAXIS).

2.1.7. Communication Manager (CM)

The CM has the responsibility of managing the communication of the project and its outcomes, raising the project's public awareness, and engaging stakeholders. The CM will also represent NANCY to the SNS JU Communications Team. The CM of NANCY is Mr. Konstantinos Kyranou (SID).

2.1.8. Exploitation and Innovation Manager (EIM)

The EIM is responsible for the activities related to the marketing and exploitation of the project outcomes and results. The EIM is also responsible for managing the project's innovation and the associated processes that will be followed, ensuring a proper uptake of the project outcomes by the market, and coordinating the technical developments with the business exploitation actions. Moreover, the EIM has the responsibility for Intellectual Property Rights (IPRs) management, market analysis, joint exploitation processes, and the development of a plan for supporting partners in establishing their commercialization and business plans. The EIM of NANCY is Dr. Ioannis Chochliouros (OTE).

2.1.9. NANCY Technology Adopters Focus Group Liaison (NANCY-TAFGL)

The TAFGL manages the activities associated with engaging stakeholders and adopters of the main NANCY technologies, such as artificial intelligence (AI), blockchain, wireless networks, multi-access edge computing (MEC), software defined networking (SDN), virtualization, and resource orchestration. The TAFGL of NANCY is Prof. Antonio Skarmeta (UMU).

2.1.10. Sustainability Board (SB)

The SB is responsible for monitoring the market and coordinating the general exploitation and dissemination activities for maximizing the sustainability of the project's outcomes and exploitation potentials. During the project's kick-off meeting, all partners will nominate a Market Evolution and Sustainability Representative who will participate in the project SB, representing the organization with respect to sustainability matters and issues. The Representatives can also be invited to attend the GA meetings. The Head of the SB is Dr. Athanasios Tziouvaras (Bi2S).

2.1.11. AI act of the Council of EU and EU Parliament NANCY Observatory Manager

The AI act of the Council of EU and EU Parliament aims to "ensure that artificial intelligence (AI) systems placed on the EU market and used in the Union are safe and respect existing law on fundamental rights and Union values." A significant component of the EU strategy to promote the development and adoption of safe and legal AI that respects basic rights is the draft rule that the Commission presented in April 2021. The proposal establishes a standard, horizontal legal framework for AI with the goal of ensuring legal certainty. It takes a risk-based approach. It encourages AI investment and innovation, improves governance and the efficient application of current laws pertaining to fundamental rights and safety, and makes it easier to create a single market for AI applications. It complements other programs, such as the Coordinated Plan on Artificial Intelligence, which seeks to increase AI investment in Europe.

The NANCY consortium is committed to achieving a trustworthy and secure set of AI products by satisfying key requirements. The impact of the implemented systems and methodologies shall be overviewed, following the state of the art (SoTA) trustworthy and explainable AI (XAI) principles and will be integrated into the design at the early stages of the project. Stakeholders and end-users that are affected by or utilize AI solutions developed by NANCY will be informed accordingly, while the respective requirements will also be considered in the design phase of the project. In addition, the model design will take into account the outputs, thereby ensuring that no discrimination or bias will

take place. Appropriate data preparation and evaluation activities with respect to the datasets will take place. In this direction, proper overseeing mechanisms will be employed, while any participant interacting with AI will be notified and a human contact person will be available and able to provide information regarding the underlying AI-based edge processing and the cloud-based data storing mechanisms. NANCY will support the human-AI collaboration, enabling humans to interact with intelligent systems responding to and assessing the AI-generated recommendations offering feedback. To this end, discrimination, and fundamental human rights and freedoms will be assessed. The AI model can only serve as a tool in the process and cannot and should not replace the decision of a qualified expert. Finally, NANCY envisages ensuring the computing security and privacy requirements of the distributed edge computing infrastructure.

The above motivates the role of the AI act of the Council of EU and EU Parliament NANCY Observatory Manager, who will closely monitor the activities of the council and inform the NANCY consortium of topics of interest. Moreover, the AI act of the Council of EU and EU Parliament NANCY Observatory Manager will guarantee that all the NANCY outcomes and results are in-line with the council's and EU Parliament's suggestions and recommendations.

The NANCY AI act of the Council of EU and EU Parliament NANCY Observatory Manager is Prof. Panagiotis Sarigiannidis (UOWM), while Dr. Dimitrios Pliatsios (UOWM) is serving as deputy.

2.2. Scientific and Technical Committee (STC)

The STC is responsible for the technical planning, monitoring, and implementation of the project with respect to scientific and technical matters. The STC oversees the progress of the project and makes decisions on all relevant technical and administrative matters including the technological and technical choices, redirection of the work in a WP, major transfer of partners or WPs resources, time plan modifications, the introduction of a new partner, substitution or exclusion of an existing partner, and resolving conflicts between WPs. In addition, the STC administers equipment provision, calls of tenders, specifications, and new partners' inclusion. The STC is under the control of and in compliance with the decisions of the GA.

The STC is chaired and vice-chaired by the SC and TC, respectively. In addition, WPLs, who are responsible for managing their WP as a self-contained entity, are also members of the STC. The WPLs activities consist of monitoring, coordinating, and evaluating the WP progress, as well as ensuring the respective timelines, costs, and quality of outcomes are met.

The NANCY WPLs and STC members are listed in Table 3.

Table 3: Scientific and Technical Committee Members

Scientific and Technical Committee			
Mailing List: nancy-stc@lists.uowm.gr			
Attribute	Name	Partner	Email
SC	Thomas Lagkas (Chairman and SC)	UOWM	tlagkas@uowm.gr
TC	Alexandros-Apostolos Boulogeorgos (Vice-chairman and TC)	UOWM	aboulogeorgos@uowm.gr
WP1 Leader	Panagiotis Sarigiannidis (PC)	UOWM	psarigiannidis@uowm.gr

WP2 Leader	Stylianos Trevlakis	INNO	trevlakis@innocobe.org
WP3 Leader	Blaz Bertalanic	IJS	Blaz.Bertalanic@ijs.si
WP4 Leader	Antonio Skarmeta	UMU	skarmeta@um.es
WP5 Leader	Sebastien Andreina	NEC	sebastien.andreina@neclab.eu
WP6 Leader	Antonella Clavenna	ITL	antonella.clavenna@italtel.com

2.3. Work package (WP) technical groups

Role and responsibilities: The WP leader (WPL) is responsible for planning, managing, coordinating, and monitoring the work contained in the work package. The WPL also ensures that the work is completed in complete conformity with the GAP and suggests appropriate steps as needed. Through the GA meetings, he or she represents the WP's interests and interacts with other WP. WPs are further divided into tasks. Task leaders (TLs) are chosen and managed by the WPL.

Composition: Each WP Technical Group is led by the WP Leader and includes all of the WP's members. In reality, the following project operational tasks are carried out by the WP Technical Groups under the supervision of the WP Leaders (see Table below). Table 3 lists the NANCY technical WP leaders.

2.4. Project Management Office (PMO)

The PMO has the responsibility for the administrative and financial management of NANCY, including management of the tasks and activities in collaboration with the PC, the TC, and the SC. The PMO, comprising a staff familiar with administrative, legal, communication, and IPR issues acts as the daily project management instrument and supports the PC in administrative activities. The PMO tasks will be performed by UOWM staff. In more detail, the PMO tasks are:

- Setting up a mailing list and a secure document repository, creating the necessary templates for reports, deliverables, change requests, etc., and enforcing the rules established for document management.
- The organization of project online and in-person meetings and the preparation of minutes; the organization of the quality review of deliverables and the preparation of the review reports to the coordinator; the assistance to the coordinator in the preparation of the quarterly, annual, and final activity reports.

The PMO encompasses two roles, namely the role of the PC, and the role of the NANCY's financial officer.

2.4.1. Role of PC in the PMO

The PC is responsible for all project management activities, including the in-budget and timely achievement of project results, the timely submission of deliverables, the preparation of the Project and Risk Management Handbook (i.e., this deliverable), the preparation of the progress and cost reports, and the adherence to the agreed procedures and processes. The PC leads the PMO, thus, the PC has the responsibility for all administrative tasks undertaken by the PMO. The PC activities described in this section do not override the ones documented in Section 2.1.1.

2.4.2. Role of NANCY's Financial Officer in the PMO

The NANCY's financial officer (FO) is responsible for the financial supervision and management of the project. In more detail, the FO administers the distribution of the shares to the consortium. The FO of NANCY is Mrs. Christina Petaloti (UOWM).

2.5. External Advisory Board (EAB)

The EAB will consist of experts from the AI, blockchain, MEC, SDN, virtualization, and resource orchestration/optimization domains. The EAB members will be defined within three (3) months from the start of the project. The EAB will monitor the technical developments and activities throughout the project's duration. Furthermore, the EAB will offer consultation to the consortium towards ensuring that the project outcomes and results are of high quality and will match the stakeholders' requirements and needs. In this direction, the liaison for the EAB will propose four (4) members for the EAB (one expert for each one of the fields AI, blockchain, MEC, SDN, virtualization, and resource orchestration/optimization), and after the GA approval, will contact them. Moreover, the liaison for the EAB will organize three (3) virtual meetings with the EAB member, where the related WP technical groups will present the project advances and outcomes. The liaison for the EAB is Mr. Konstantinos Kyranou (SID).

3. Reference Documents

There exist three documents that define the obligations and rights that apply to all entities involved in the project, namely (a) the GA, which specifies the contractual agreements with the European Commission (EC), (b) the CA which is an internal contract between the partners of the NANCY consortium, and (c) D1.1 – Project and Risk Management Handbook, which acts as a complementary to the first two documents, by presenting the project management structure, bodies and committees, the collaboration and communication tools, and the NANCY templates.

3.1. Grant Agreement (GA)

The GA specifies the rights, conditions, terms, and obligations of the consortium beneficiaries for carrying out the action. The GA is signed by the beneficiaries and the EC and consists of the following sections:

- Preamble
- Terms and Conditions (including Data Sheet)
- Annex 1: Description of the action
- Annex 2: Estimated budget for the action
- Annex 2a: Additional information on unit costs and contributions
- Annex 2e: Complex funding rate calculator
- Annex 3: Accession Forms
- Annex 4: Model for the financial statements
- Annex 5: Specific rules

3.2. Consortium Agreement (CA)

The CA is jointly accepted and signed by all beneficiaries and will be in force and effect until the complete fulfillment of all obligations that are described in the GA.

The aim of the CA is to define the relationships among parties with respect to the project, regarding the parties' obligations and rights concerning inter alia liability, management of the project, organization of the work between the parties, access rights, and dispute resolution supplementing the GA, where appropriate, regarding access rights, and obligations of the parties.

The CA consists of the following sections:

1. **Definitions:** Introduces and explains all definitions that are used in the subsequent sections.
2. **Purpose:** States the purpose of the document.
3. **Entry into force, duration and termination:** Defines the start and duration of the parties' obligations.
4. **Responsibilities of Parties**: Defines the responsibilities of the parties.
5. **Liability towards each other:** Specifies the liabilities to other parties, as well as the liability limitations.
6. **Governance structure:** Defines and describes the governance structure of the project and the operational procedures.
7. **Financial provisions:** Specifies the payment procedure, timeline, and rules.
8. **Results:** Clarifies the ownership, joint ownership, and transfer of ownership with respect to the project results. Also, it defines the rules related to the result dissemination and contributions to standards.

9. **Access rights:** Defines the access rights to the project results and the associated parties' obligations.
10. **Non-disclosure of sensitive information:** Specifies the obligations and exceptions with respect to non-disclosure of sensitive information.
11. **Privacy and data protection:** Specifies the rules associated with storing, processing, and transferring personal data.
12. **Miscellaneous:** Outlines various rules and obligations that are not included in the aforementioned categories.
13. **Signatures:** Consists of the signatures of the authorized representative of each party.
14. **Attachments:** Consist of several documents attached to the CA. The documents are as follows:
    I. Background included
    II. Declaration of accession
    III. List of third parties for simplified transfer according to Section 8.3.2. of this CA
    IV. List of any additional affiliate pursuant to Article 1's definition of Affiliate
    V. Template for non-disclosure agreement for the NANCY consortium external advisory board

3.3. Project and Risk Management Handbook

The current deliverable, entitled "D1.1 - Project and Risk Management Handbook," presents the structures, procedures, and tools that will be used for the administration and implementation of the NANCY project. It aims to present the administration and collaboration processes for the successful implementation and completion of the project. Moreover, it serves as a complimentary to the GA and CA provisions.

4. Project Management Processes

4.1. Events Requiring Immediate Report

Any events that can significantly impact or delay the project activities or compromise the EU's financial interest must be immediately reported to the PC, who will then update the rest of the partners and the PO. Such events include, but are not limited to:

- Change of the Legal Entity Appointed Representative (LEAR).

- Change of the financial, legal, organizational, technical, or ownership situations of those referred to linked third parties.

- Change of the name, organization type, legal form, and address.

- Any kind of event or action that may affect the project or its adherence to the GA/CA requirements.

Additionally, the Portal Beneficiary Register should continuously be updated by all partners, more particularly when personal information, legal representatives, legal forms, and organization types are concerned.

4.2. Reporting Periods and Process

This section focuses on defining the reporting periods and processes. In this direction, Section 4.2.1 presents the reporting periods, while Section 4.2.2 the corresponding process that will be followed.

4.2.1. Reporting Periods

Figure 5: Reporting Periods
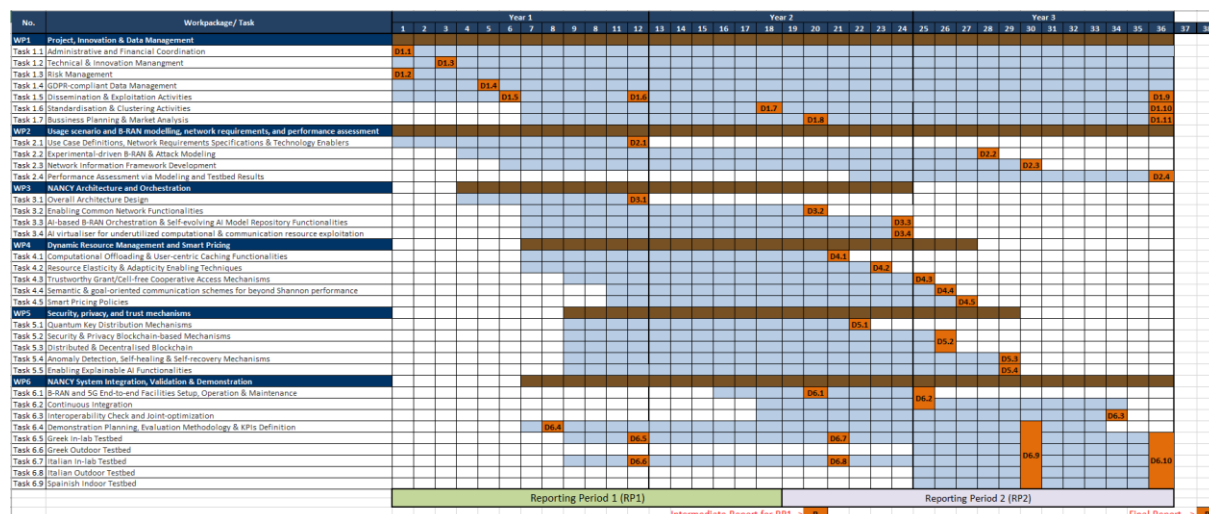
As demonstrated in

Figure 5, two (2) reporting periods are specified, namely Reporting Period 1 (RP1), which covers M01 to M18, and Reporting Period 2 (RP2) which covers M18 to M36. A financial and technical periodic report must be submitted within sixty (60) days following the end of each reporting period. In addition, upon completion of the project, a Final Report must be submitted within sixty (60) days following the end of the last reporting period.

The STC is responsible for updating the GA with respect to administrative matters. Concerning the scientific and technical reporting, the task leaders report to the WP leaders, who in turn report to the SC. Finally, the SC is responsible for reporting to the STC, which in turn reports to the GA.

4.2.2. Reporting Process

Internal (within Consortium): Each partner commits to writing a monthly report to the PMC with a copy to the WPL. The report will describe the technical and management project work done, listing effective time spent on the project. It will mention difficulties and challenges, milestones and deliverables (or contributions to deliverables in case of joint deliverables) that have been reached, patents, publications, travel, and visits.

External (to EC): The PMO will coordinate and consolidate the reports, as well as management and financial reports, and submit them for the project/technical/scientific coordinators' approval. After their approval, the reports will be delivered to the EC. Each partner will provide audit certificates when needed (according to HE rules), prepared by an external auditor selected by the partner, and certifying that the costs incurred during the period meet the conditions required by the GA.

4.3. Project Meetings

WP-level meetings will take place on-demand based on the respective WP needs. In addition, face-to-face (F2F) meetings will be held every six (6) months. Moreover, meetings concerning various project activities will take place during the same days, yet in separate sessions, in order to minimise travel expenses. Moreover, NANCY partners may also use teleconferencing software in addition to physical meetings.

4.3.1. GA Meetings

The GA will convene at least twice a year; also, upon written request of the PC or upon written requests of 1/3 of the GA members. The meetings may take place using teleconference software.

4.3.2. Scientific and Technical Committee Meetings

The STC will convene at least bi-monthly, as well as at any time upon written request of any STC member. The meetings may take place using teleconference software.

4.3.3. Technical WP Group meetings

The WPL of each technical WP (WP2-WP6) is responsible for the organization of bi-weekly virtual meetings that will last from the beginning till the completion of the WP. The coordinating organization (UOWM) will provide the bridge for these meetings. All the technical WP groups will have F2F meetings twice per year on the same days as the project meetings. The meetings will be paused during international and national holidays.

4.3.4. Physical Meetings Hosting

The following guidelines should be followed for hosting F2F meetings:

- The appointed meeting venue/location should be easily reachable. The hosting partner must provide information regarding meeting logistics (e.g., reaching the venue, travel information, and accommodation details).
- The hosting partner will cover the costs associated with the hosting of the meeting, while each participant will cover their own travel costs.
- The host must offer an appropriate meeting room, equipped with visual and audio infrastructure for facilitating the presentation of material. Also, the room meeting should offer access to the Internet.
- Although not obligatory, it is suggested that the host provides water, coffee, and lunch during breaks, and organises a social event, such as a dinner.

4.3.5. Minutes of Meeting

The chairperson will keep the meeting minutes, as well as any decisions made, in a formal record. Minutes should be kept for all meetings (i.e., virtual and physical ones) in an easy-to-read and compact form. Moreover, the chairperson should share a draft of the meeting minutes with all participants within fifteen (15) calendar days of the meeting. The meeting minutes will be considered accepted if no objection has been expressed within fifteen (15) calendar days of the sharing. The objection has to be expressed in written form. Then, the chairperson will send the final meeting minutes to the PC and GA members, who shall safeguard them. Also, the PC should provide authenticated duplicates to the partners upon request.

4.4. Deliverable Review and Submission Processes

Each of the deliverables must be reviewed by the QRM, the PC, and two internal reviewers prior to the submission. Also, an external expert can be invited to serve as a reviewer in special cases. In case the deliverable does not satisfy a particular quality level, the corresponding deliverable leader will be informed and requested to make the necessary amendments within five (5) working days.

4.4.1. Deliverable Review Process

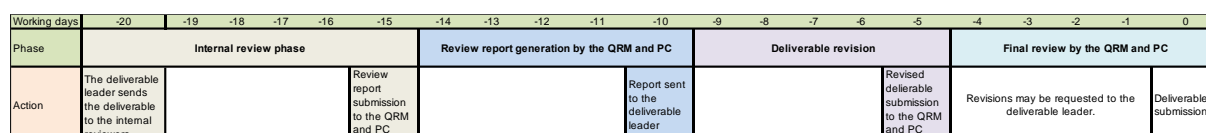| Working days	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
Phase	Internal review phase						Review report generation by the QRM and PC					Deliverable revision					Final review by the QRM and PC				
Action	The deliverable leader sends the deliverable to the internal reviewers					Review report submission to the QRM and PC					Report sent to the deliverable leader					Revised deliverable submission to the QRM and PC	Revisions may be requested to the deliverable leader.				Deliverable submission

Figure 6: Deliverable review process.

As presented in Figure 6, the internal review process of the deliverables is as follows:

1. The deliverable leading partner should send the deliverable to the internal reviewers fifteen (15) working days before its due date.
2. The internal reviewers will generate a review report and forward it to the deliverable leader within five (5) working days. The particular template for the review report should be used.
3. The deliverable leader responds to the reviewers' comments, makes the requested changes, and sends the revised deliverable, along with the review report, within five (5) working days to the QRM and PC.
4. The QRM and the PC will check the modifications and (if needed) request final revisions.
5. Finally, the PC will submit the deliverable.

4.4.2. Deliverable Reviewer Assignments

Each of the NANCY deliverables is assigned to two internal reviewers according to Table 4.

Table 4: Deliverable Reviewer Assignments

ID	Title	Leader	Type, Dissemination	Reviewer 1	Reviewer 2
D1.1	Project and Risk Management Handbook	UOWM	R, PU	INNO	MINDS
D1.2	NANCY web site, social network pages and open access server	OTE	DEC, PU	UOWM	INNO
D1.3	Plans for Publicity, Dissemination and Exploitation	DRAXIS	R, PU	CERTH	SSS
D1.4	Project Scientific/Technical Plan	INNO	R, PU	MINDS	UOWM
D1.5	Data Management Plan	SID	R, PU	OTE	DRAXIS
D1.6	Initial Impact Creation Report	TEI	R, PU	INTRA	I2CAT
D1.7	Initial Standardisation Activities Report	TDIS	R, PU	UMU	TEI
D1.8	Market Analysis, Roadmap and Business Modelling Report	8BELLS	R, PU	TDIS	TECN
D1.9	Final Impact Creation Report	DRAXIS	R, PU	ITL	VOS
D1.10	Final Standardisation Activities Report	TEI	R, PU	8BELLS	NEC
D1.11	Techno-economic Analysis and Commercialization Plans	8BELLS	R, PU	CERTH	INNO
D2.1	NANCY Requirements Analysis	OTE	R, PU	UMU	SSS
D2.2	NANCY Experimental-Driven Modelling	INNO	R, PU	UOWM	SID
D2.3	NANCY Network Information Framework	8BELLS	R, PU	OTE	INNO
D2.4	NANCY System Performance Assessment	INNO	R, PU	IJS	CRAT
D3.1	NANCY Architecture Design	IJS	R, PU	ITL	VOS
D3.2	NANCY Network Functionalities	SSS	O, PU	8BELLS	UMU
D3.3	NANCY AI-based B-RAN Orchestration	INTRA	O, PU	SID	CERTH
D3.4	NANCY AI virtualiser	VOS	O, PU	IJS	INNO
D4.1	Computational Offloading and User-centric Caching	UMU	R, PU	8BELLS	IJS

|					
D4.2	Resource Elasticity Techniques	IJS	O, PU	OTE	VOS
D4.3	Trustworthy Grant/cell-free Cooperative Access Mechanisms	UMU	R, PU	SID	INNO
D4.4	Semantic & goal-oriented communication schemes for beyond Shannon performance	INNO	R, PU	UOWM	MINDS
D4.5	Smart Pricing Policies	8BELLS	R, PU	TECN	OTE
D5.1	Quantum Key Distribution Mechanisms	TDIS	O, PU	NEC	ITL
D5.2	NANCY Security and Privacy Distributed Blockchain-based Mechanisms	NEC	O, PU	UMU	UBITECH
D5.3	Self-healing and Self-recovery Mechanisms	CRAT	O, PU	DRAXIS	UMU
D5.4	NANCY Explainable AI Toolbox	MINDS	O, PU	NEC	UBITECH
D6.1	B-RAN and 5G End-to-end Facilities Setup	UBITECH	R, PU	TDIS	SSS
D6.2	NANCY Integrated System – Initial Version	INTRA	R, PU	TEI	CERTH
D6.3	NANCY Integrated System – Final Version	INTRA	R, PU	VOS	I2CAT
D6.4	In-lab testbeds definition	CERTH	R, PU	TDIS	CRAT
D6.5	Greek in-lab testbed dataset 1	OTE	DATA, PU	MINDS	CERTH
D6.6	Italian in-lab testbed dataset 1	ITL	DATA, PU	VOS	CRAT
D6.7	Greek in-lab testbed dataset 2	OTE	DATA, PU	UOWM	UBITECH
D6.8	Italian in-lab testbed dataset 2	ITL	DATA, PU	TEI	SSS
D6.9	Outdoor Demonstration Planning, Evaluation Methodology and KPIs	ITL	R, SEN	IJS	INTRA
D6.10	NANCY Pilots' Documentation and Evaluations	INTRA	R, SEN	NEC	ITL

4.5. Conflict resolution
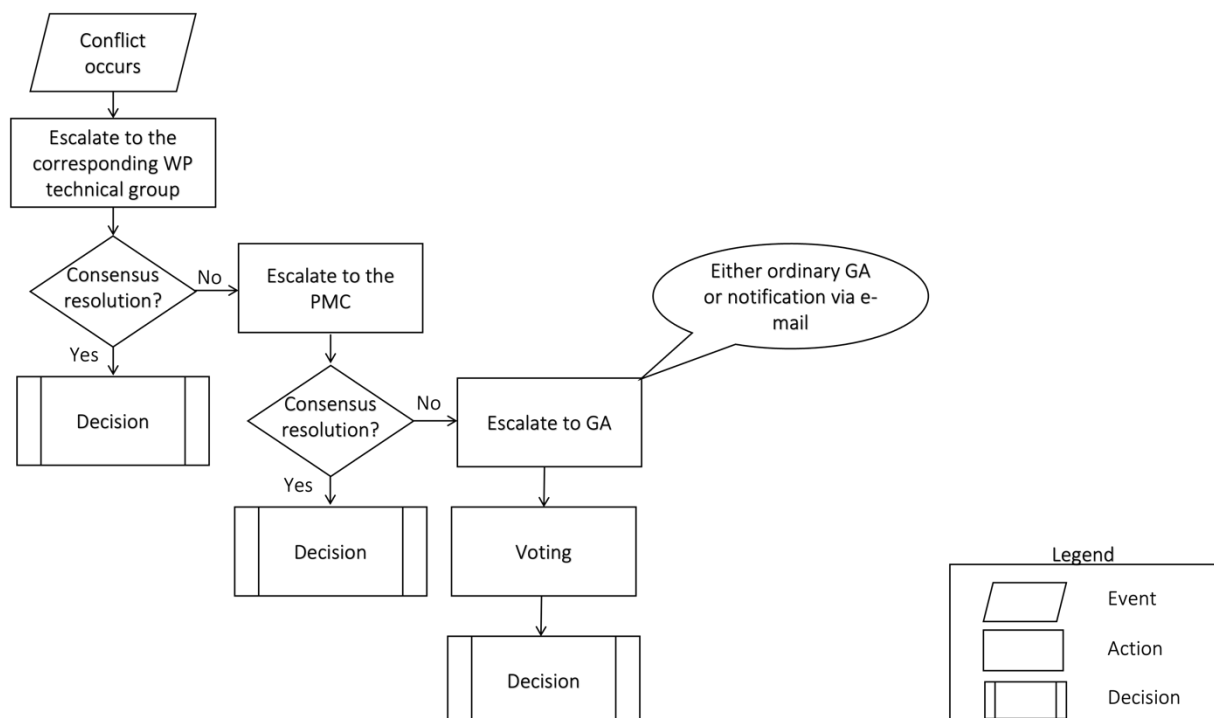
As depicted in Figure 7, a straightforward dispute resolution process is made possible by clear decision-making methods:

- Consensus is used to try to resolve disputes inside WP technical groups.
- If agreement cannot be reached within the GA, the TC escalates it to the General Assembly and a vote takes place, requiring a simple majority. If the problem cannot be solved, it is escalated to the GA: the WPL prepares a description of the problem and its potential solutions.

Because:

- Voting through email is permitted;
- Extraordinary GA meetings can be held using audio-conference (under the conditions and with the delay specified in the Consortium Agreement); and
- Extraordinary GA meetings can be organized using audio-conference (again according to the rules defined in the Consortium Agreement).

Thus, the conflict resolution process established in NANCY can be considered a straightforward and fast one.

4.6. Communication and Collaboration Tools
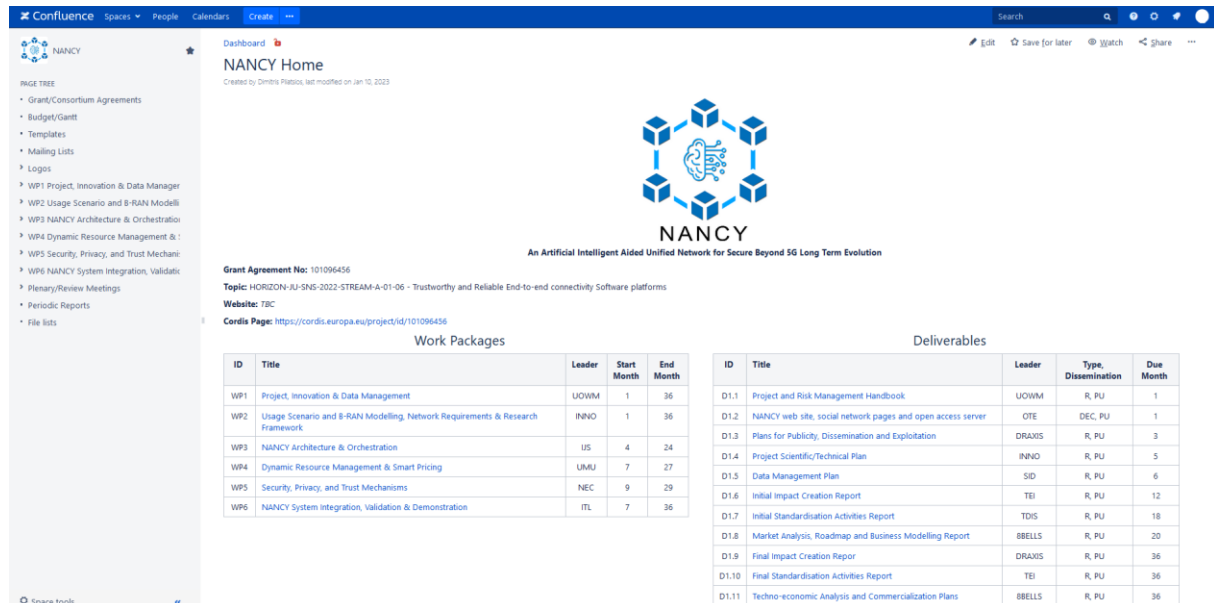
4.6.1. Teleconference Platform

The Zoom teleconference platform has been selected as the project's main teleconference software. A Zoom client is required, while the client is supported by all major operating systems. Participants can join a meeting using the meeting link, generated by the meeting host. Alternatively, participants can also join by dialing in. In addition, WP and/or task leaders may utilize their own teleconference software for the communication needs of the respective WPs/tasks.

4.6.2. Collaboration Platform

The Atlassian Confluence software is used to create a collaboration space for all consortium partners. The space will serve as a reference point for storing confidential and public information related to the project. The Confluence collaboration space is organized into pages and sub-pages. The following pages have been created for enabling quick access to important project information:

- The NANCY homepage provides an overview of all WPs and deliverables, along with the associated information (e.g., WP start/end months, WP & deliverable leaders, etc.)
- The GA and CA page.
- The page including the project Budget, Person Month, and Gannt Chart information.
- The page containing all NANCY templates that will be used for the reporting and dissemination activities.
- The page containing the aforementioned mailing lists.
- The page containing the project, as well as the consortium members', logos.
- Respective pages for each WP that includes WP information and consists of multiple sub-pages for the respective WP tasks and deliverables. All WP/task presentations, documents, and meeting minutes will be stored under the respective pages.
- The Plenary and Review Meetings page, for storing the presentations, documents, and meeting minutes.
- The Periodic Report page for facilitating the preparation of the project's periodic reports.

The Confluence space structure may change throughout the duration of the projects and based on the consortium's needs. Access to the Confluence space is only provided to project members to safeguard the confidentiality of the documents and information. Finally, UOWM is responsible for hosting and managing the Confluence space. The NANCY homepage in Confluence is illustrated in Figure 8.

Figure 8: NANCY Homepage in Confluence.

4.6.3. Mailing Lists

The following mailing lists have been established in order to facilitate the administration, communication, and technical management activities of the project:

- Project Administration Mailing Lists:
  - nancy-all@lists.uowm.gr
  - nancy-admin@lists.uowm.gr
  - nancy-ga@lists.uowm.gr
  - nancy-stc@lists.uowm.gr
  - nancy-eab@lists.uowm.gr
- Work Packages/Technical Mailing Lists
  - nancy-wp1@lists.uowm.gr
  - nancy-wp2@lists.uowm.gr
  - nancy-wp3@lists.uowm.gr
  - nancy-wp4@lists.uowm.gr
  - nancy-wp5@lists.uowm.gr
  - nancy-wp6@lists.uowm.gr
- Demonstrator Mailing Lists
  - nancy-demonstrator1@lists.uowm.gr
  - nancy-demonstrator2@lists.uowm.gr
  - nancy-demonstrator3@lists.uowm.gr

5. Communication and Dissemination Activities

This section includes the information for preparing the project deliverables, as well as other reporting material for the dissemination and communication of the project and its outcomes.

5.1. Project Logo

The project logo is illustrated in Figure 9. It will be used by the project partners as a visual identification of the project. The logo and its variations have been uploaded to Confluence and can be found at: https://space.uowm.gr/confluence/display/NANCY/Logos

Figure 9: NANCY Logo

5.2. Documentation Templates

Documents will be stored and edited in .docx or .tex format, while presentations will be stored and edited in .pptx or .key format. All the reports, presentations, scientific publications, white papers, and newsletters will be also stored in the repository also as .pdf files. The deliverable/presentation leader may select the most appropriate software and format based on the particular needs and document type. Templates have been created for each document type for establishing a common visual consistency.

The project's templates have been uploaded to Confluence and can be accessed at: https://space.uowm.gr/confluence/display/NANCY/Templates

5.2.1. Deliverable Template

The deliverable cover and document control page are illustrated in Figure 10.

Figure 10: Deliverable Template

5.2.2. White Papers Template

The white papers cover, and document control page are illustrated in Figure 11.

Figure 11: White paper Template

5.2.3. Newsletters Template

The newsletter template cover is depicted in Figure 12.

Figure 12: Newsletter Template

5.2.4. Presentation Template

The first slide of the presentation template is illustrated in Figure 13.
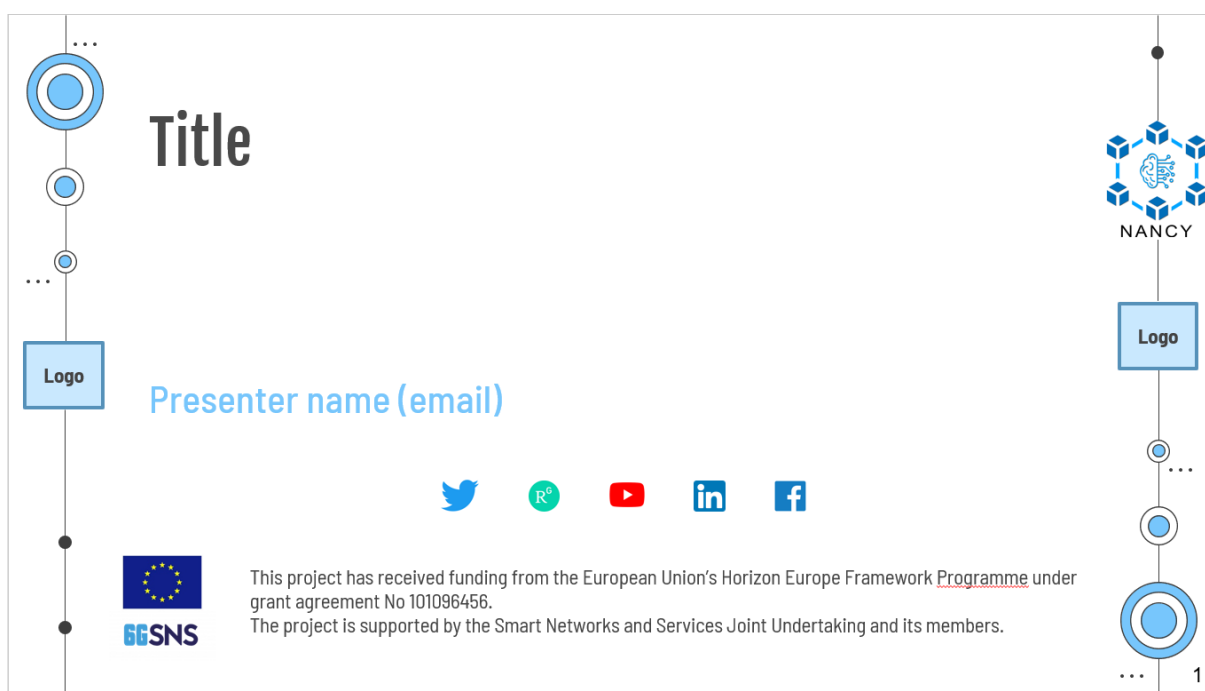
Figure 13: Presentation Template

5.2.5. Deliverable Review Template

The template for the deliverable peer-review report is illustrated in Figure 14.
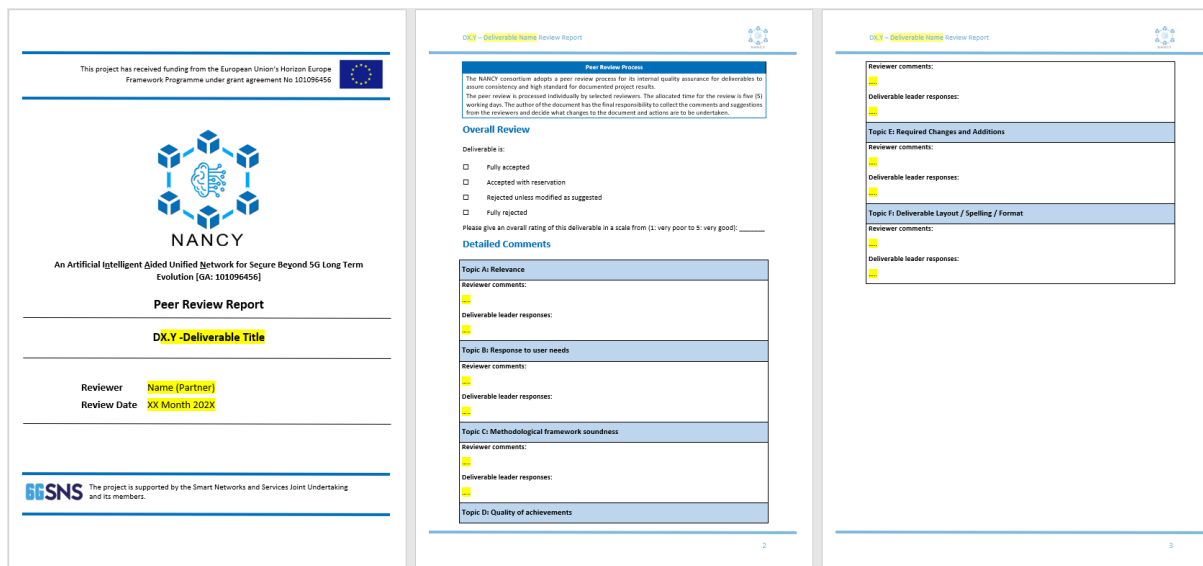
Figure 14: Review Report Template

5.2.6. Internal Report Template

The template for the internal report is illustrated in
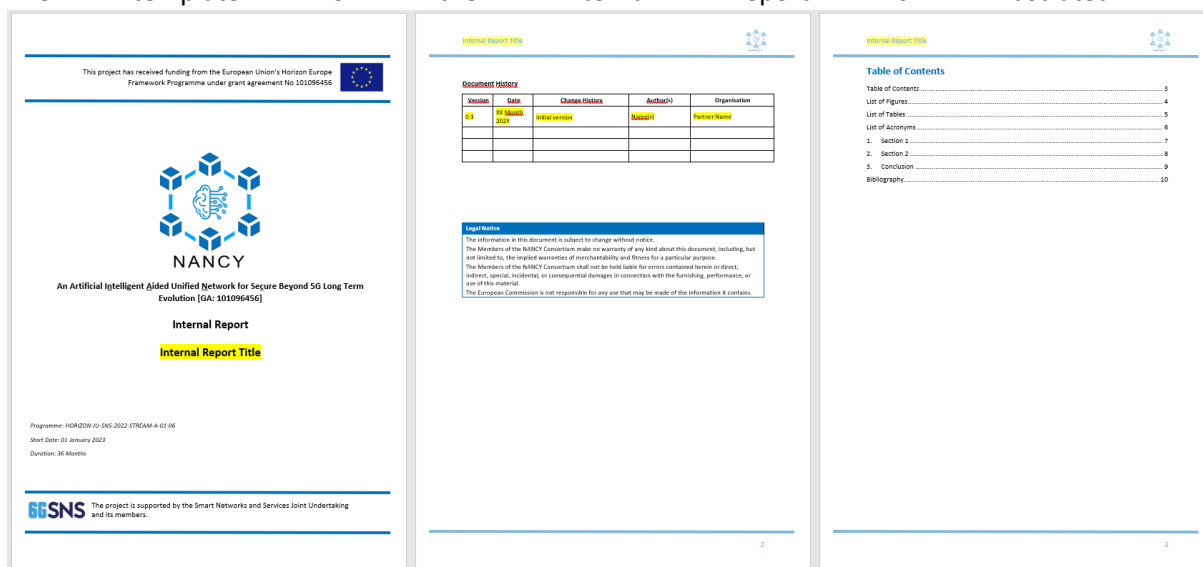
Figure 15.
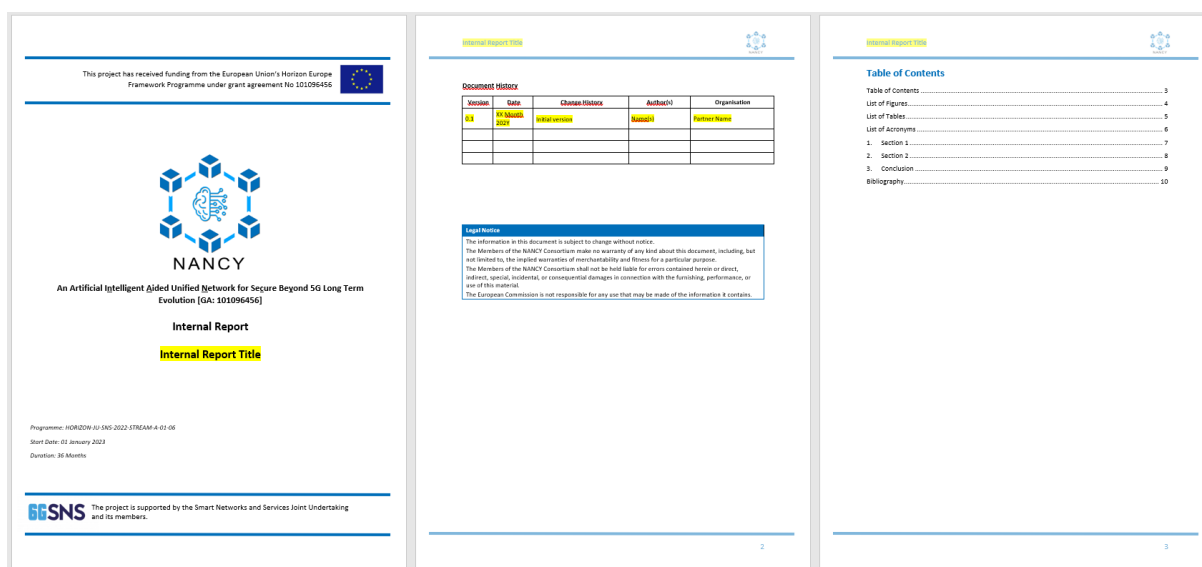
Figure 15: Internal Report Template

5.3. Naming and Versioning of Documents

Adopting a consortium-wide common file naming pattern is strongly recommended for facilitating editing and minimizing errors. To this end, the document name will contain:

- NANCY
- <WPX> or <TX.Y> or <DX.Y>, where <WPX> denotes the WP number, <TX.Y> stands for the task number, and <DX.Y> stands for the deliverable number
- <Document's title>
- <vX.Y> which stands for the revision number
- [Partner], which includes the partner name that uploads/publishes the revision.

Of note, the underscore (_) should be used instead of spaces to avoid any compatibility issues when sharing the file. For example, "NANCY_D1.1_Project_Management_Handbook_v0.2_[UOWM].docx" denotes version 0.2, which was authored/revised by UOWM. The final deliverable version which will be forwarded to the PC for submission will be versioned as v1.0. In case of deliverable rejection and resubmission, higher numbers can be used (e.g., v1.1, v2.0, etc.).

5.4. Communication and Dissemination Requirements

All dissemination and communication activities, both in physical and digital forms (e.g., social media) and any results, equipment, or infrastructure funded by this grant must:

(a) Include the EU emblem ( ) and the following text:
- For dissemination and communication activities:
  "This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement No 101096456.".
- For results, equipment, and infrastructure:
  "This [infrastructure][equipment][result] has received funding from the European Union's Horizon Europe Framework Programme under grant agreement No 101096456.".

(b) Include the 6GSNS logo ( ) and the following text:

"The project is supported by the Smart Networks and Services Joint Undertaking and its members."

Of note, both (a) and (b) are required. Additionally, when displayed along with other logos, the EU emblem and 6GSNS logo must have appropriate prominence.

Moreover, any communication activity related to the action must indicate that it reflects only the author's view and that the EC is not responsible for any use that may be made of the information it contains.

The NANCY partners are strongly advised to refer to the GA and specifically Articles 17 and 18 of Annex 5. Any breach or deviation from these requirements can result in grant reduction and/or other measures as stated in Chapter 5 of the GA.

6. Quality Management

The TC and the QRM will be required to monitor technical progress on a regular basis to ensure that the project continues to be innovative, driven by end-user requirements, open to partnerships, responsive to market needs, and forward-looking. This will guarantee that the NANCY project is churning out high-caliber technical output.

The handling of deliverable quality is covered in Section 4.4, but quality must also be taken into account for the project process as a whole. As a result, the project's management process and developments will be periodically reviewed in light of:

1. Maintaining attention to the project's goals, which include end-user requirements, high-quality technical outputs, and market accessibility;

2. The project management plan's suitability and the extent to which the work completed complies with it, including the management of IPR and the distribution of outcomes;

3. How synchronized and connected the project processes are;

4. Identification and assessment of actions and outcomes that would compromise the project's ability to fulfill its goals;

5. Project process improvement by recognizing deviations and modifications.

All partners are jointly responsible for quality assurance, which will be used at all project activity levels. Expenses, resources, and schedules (i.e., technical and financial annexes to the EC GA) will be continuously monitored and controlled (i.e., by taking corrective action initiated by the QRM). Cost, resource, and schedule deviations must have their underlying reasons determined, documented, and used as a basis for ongoing improvement. It is important to assess any potential effects of schedule modifications on the project's budget, resources, and level of output.

7. Risk Management

In both industry and academia, management and analysis of risks are essential for the successful management of a project. The consortium will need to deal with new dangers as they emerge throughout the course of the project's lifecycle. In order to effectively manage risks, it is necessary to first recognize them, assess their likelihood, severity, and impact, and then implement the most suitable actions. The success of the risk management strategy depends on its ability to lessen the likelihood of these risks happening and to mitigate their potential impact on the project.

Because risk analysis is an ongoing cycle, the lists of identified risks, impacts, and mitigation strategies will be continuously updated until the NANCY project is complete. It is also important to note that there is no way to completely exclude the chance of a risk materializing. The goals of the risk management strategy are to foresee and mitigate the effects of any potential risks.

7.1. Risk Management Plan

A five-stage risk management plan is adopted in the NANCY project for identifying, quantifying, responding, monitoring, and documenting risks. Specifically, the five stages are:

- The process of identifying risks related to the project entails meticulously documenting every potential threat.
- The quantification step receives potential threats and provides an estimate of their potential repercussions to the project. Moreover, it produces information that may be utilized to choose the best course of action.
- The information gathered in the previous two stages is used in risk response development to create mitigation strategies, and take preventative measures.
- In the monitoring stage, a record of potential threats is maintained, the execution of mitigation strategies is ensured, their effectiveness is quantified, and modifications are applied to the risk management strategy.
- Finally, objectives, sources, assumptions, choices, and responses to the identified risks are documented.

7.2. Risk Assessment and Analysis Frameworks

Based on the aforementioned, there is no shortage of risk assessment tools. In this section, the ones used in the NANCY project are analyzed and compared.

7.2.1. What-if Analysis

A what-if analysis is less of a methodical exercise and more of a creative thought experiment. It is a form of computer simulation used to examine the operation of a complicated system or project under controlled conditions. It evaluates how a change in a few parameters can influence the system based on a set of assumptions. Scenarios are often constructed by posing the question "what if?" and documenting each possible consequence.

7.2.2. Failure Mode and Effects Analysis (FMEA)

Another methodical strategy for discovering and recording potential points of failure is FMEA, which is enlisted throughout the lifespan of the project. Specifically, in the early stages, FMEA provides important input to the system design process, while during the project's later stages, it contributes towards monitoring failure modes, evaluating their importance, and ensuring that proper mitigation measures are performed. Furthermore, FMEA assesses the impact of documented risks by answering

the following: (i) "What may fail and how?", (ii) "How frequently it fails?", (iii) "What effect the failure has on the process?", and (iv) "Whether or not the failure has any bearing on the system's safety and/or reliability?".

7.2.3. Expanded Failure Mode and Effects Analysis (EFMEA)

As a modification of the aforementioned FMEA technique, EFMEA is meant to address its shortcomings. Using this technique, supervisors may identify potential system weak spots. Additionally, it offers resources for identifying and assessing feasible countermeasures. Specifically, EFMEA is comprised of two phases, namely risk identification and risk mitigation, while it classifies risks into four categories: (i) behavioral, (ii) legal, organizational, and (iv) technical.

7.2.4. Risk Assessment Decision Matrix Analysis (RADMA)

RADMA is a useful decision-making approach that is also utilized for assessing risks. It provides informative visual depictions of risks, their effects, and their likelihood. It is more useful when used in conjunction with other risk analysis techniques since it provides a brief overview of the situation and allows for the ranking of the risks, rather than as a replacement for them.

7.2.5. Hazard and Operability Analysis (HAZOP)

HAZOP is one of the most prominent analytical risk analysis techniques that aim to identify potential vulnerabilities in terms of people, machinery, and the general viability of a task or process. Step-by-step instructions and careful evaluation of all relevant factors form the assessment procedure. The results of HAZOP reveal risks that are generated when deviating from the norm. By breaking down a large, complicated design into manageable chunks, or "nodes," this technique helps to identify possible design and technical flaws. Reviewing individual nodes facilitates the quick and simple detection of any points of failure.

7.3. Risk Identification

The risk register is the fundamental tool for managing project risks and plays an invaluable role in keeping track of the identification, assessment, and management of risks at a level that is sustainable for the project's objectives. This method is reviewed and updated on a regular basis. The risk register is meant to document all of the potential threats and their associated analyses, as well as any agreed-upon countermeasures.

The consortium will be able to keep track, manage, and document the respective mitigation actions of potential risks as they arise in the project's lifecycle with the use of a central registry that will be regularly updated. Specifically, it details all of the detected risks accompanied by context about their severity, area of concern, impacted WPs, as well as any corrective measures that have been taken to mitigate them.

The partners of the NANCY project will use, maintain, and update the registry, which will be stored in a central repository hosted by the project coordinator.

When a partner identifies a previously unknown risk, the procedure that must be followed is comprised of the following steps:

- Partners who discover a potential risk related to the project's work should first consult with the responsible WP leader, the QM, the PC, and the management board via the PO. The risk register must be kept up-to-date by the WP leader, QM, and PC as soon as a new risk is identified.

- Every two months, there will be a scheduled meeting for discussing potential risks. In this procedure, the status of monitoring and updates of the risk register will be modified. During GA meetings, both potential dangers and strategies for preventing them are considered, while a record will be kept of any new risks.
- A suitable strategy with remedial measures must be developed by the WP leaders, the management board, and the people connected to a particular risk. The amount of specificity in the contingency plan will be determined by the significance and potential consequences of the risk. For risks with a high likelihood, thorough and specific mitigation measures are essential, while if the danger is low, then possible countermeasures will be explored and recorded.

7.4. Risk Register Format

The Risk Register is a table containing several columns where various information about the risks is stored. Its format enables the ordering and grouping of the risks based on this information. Table 5 presents the table structure and describes the respective information.

Table 5: Risk Register Structure

Risk ID	A unique identification number assigned to each risk
Type	- General Risk - Managerial Risk - Technical Risk - Ethics Risk - Communication Risk
WP	Indicates the WP that is concerned with this risk.
Risk Event	Describes the issue that may take place and its associated cause.
S	Severity of the risk
O	Occurrence of the risk
R	Recoverability of the risk
D	Detectability of the risk
Risk Priority Number	This number is used for assigning priorities to the risk.
Risk Level	Describes the severity of the risk based on the following scale: I. Extremely Severe II. Severe III. Moderate IV. Slight V. Insignificant
Mitigation Plan	Outlines the agreed mitigation plan for minimizing the probability of risk occurrence and limiting its impacts.
Mitigation Feasibility	Indicates the level at which the plan can limit the risk impacts. Five levels are defined, with 1 being the highest and 5 the lowest.
Status	Summarizes the risk status and it is updated upon risk occurrence. Also, it includes the relevant mitigation actions that were carried out.

The Risk Register is continuously updated upon risk occurrence or upon new risk identification and reviewed in each plenary meeting. For ensuring the effective monitoring and update of the Risk Register, the following remarks are established:

- The involved partners are promptly informed about the plan the need to follow when a risk occurs.
- The risk mitigation plan is well specified and can efficiently and effectively address the risk.
- All partners are informed about the potential impact of the various risk on their work and the project in general.
- The risks and the associated impacts should be unambiguous and clear.

7.5. Failure Mode and Effects Analysis (FMEA)

The failure mode and effects analysis (FMEA) provide methods for the systemic and qualitative analysis of risks. Its purpose is to increase preparation and forestall the emergence of unanticipated risks. In addition to the potential failure points being identified, focus is also placed on the factors that led to those failures, as well as the preventative measures and recommendations that can assist eliminate those failures or make up for them.

FMEA is widely utilised in a variety of industries due to the fact that its features enable the early examination of possible problems. Early analysis is advantageous as it enables managers to promptly implement corrective measures to reduce risks. The ability to prepare and avoid problems via adequate design and planning is a benefit of anticipating failures at an early stage.

FMEA is able to capture and document the impact of each identified failure, identifying critical failure nodes. In addition to the severity of the effect, failure nodes are classified according to the likelihood of their occurrence. This methodology enables prior experience with similar processes to successfully contribute to the identification of failure modes. Since these are available even before design, they can be incorporated into the design process seamlessly and at no additional expense to avoid or minimise their negative impact.

The FMEA can be used a) during the design phase of a process, service, or product, b) when a process, service, or product will be applied in a novel method with previously unknown outcomes, c) before the development of control plans for that particular process, services, or product, d) during the design of improvements, e) periodically, in order to safeguard its normal operation.

Failures are also ranked depending on a number of factors, namely ease of detection, probability of detection, and harmfulness. The risk priority number (RPN) for each failure mode is determined based on these three factors. The objective of FMEA is to design strategies to eliminate or mitigate these problems based on the RPN. The FMEA process is illustrated in Figure 16.
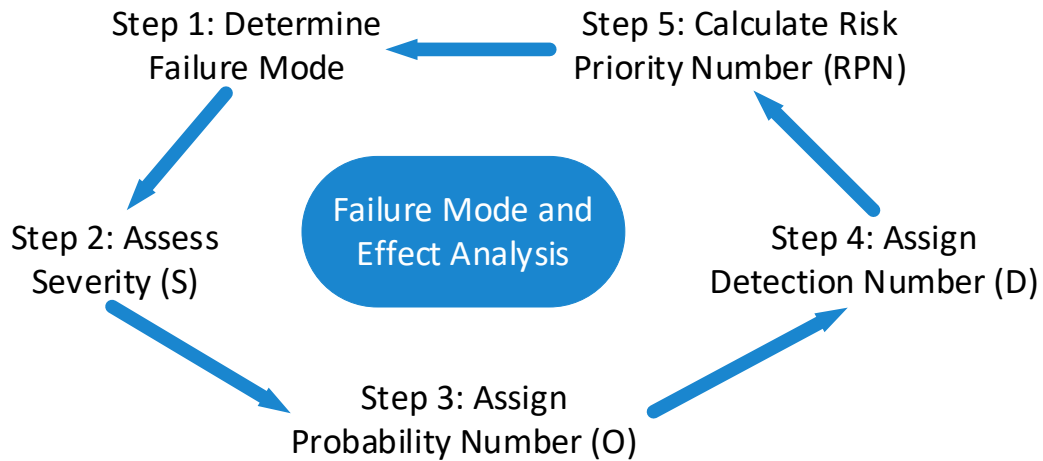
Figure 16: Failure Mode and Effect Analysis

FMEA is a widely used and popular Risk Analysis technique. However, it does have certain restrictions. It has been described as tedious in the computation process, devoid of significant failures, and unable to play a significant role in decision-making if applied late. The Expanded version of the approach, namely the EFMA, aims to address some of these limitations and expand its applicability.

7.5.1. Risk Priority Number Calculation

The RPN is used to differentiate critical failure and to rank the discovered nodes. The scale utilised spans from 1 for the highest possible rating to 1000 for the lowest possible rank. This analysis encompasses a variety of variables that are used to assess the criticality of the failure, namely the severity, frequency, detectability, and recoverability. Severity reflects how severe the impacts of such a failure would be, occurrence indicates the likelihood of such a failure occurring, and detectability indicates the likelihood of such a failure being identified prior to affecting end users.

These concern all forms of legal, administrative, technical, and behavioural failures. Legal risks involve the country's legislation and the system's conformity with it. Moreover, administrative risks involve difficulties with the organization's structure and processes, while technical risks pertain to any potential technical problems that may arise throughout the project. Finally, behavioural risks are associated with user behaviour, their response to the system, and the possibility of a negative reaction.

The RPN is obtained using the following equation:

$$RPN = S \times O \times \frac{R+D}{2} \qquad (1)$$

where S and O stand for severity and occurrence, respectively, while R and D denote the recoverability and detectability, respectively.

To preserve the consistency among the NANCY consortium partners, the work of [1] is leveraged. In this direction, the following list is generated based on the question "What can go wrong?" as a standard way for the identification of potential Failure Modes.

1. The intended operation is not carried out.
2. The intended operation is not carried out adhering to the expected standards concerning its safety.
3. The intended operation features a worse performance than expected.
4. The intended operation is not carried out in the expected way.

5. The intended operation is not carried out in the expected place.

6. The intended operation is not carried out in the expected timeframe.

7. The lifetime of the operation is lower than expected.

8. The intended operation results in higher operational and maintenance costs than expected.

9. Operations are performed unexpectedly and without intention.

10. Unavailability, or partial availability, of support for the intended operation.

To this end, Tables 6 to 9 aim to assist in the assessment of the risk level and calculating the respective RPN[1]. Specifically, Tables 6 and 7 list the severity and occurrence levels, respectively, while Tables 8 and 9 respectively list the recoverability and detectability levels.

Table 6: Severity Levels

Severity Level	Technological issues	Behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (extremely severe)	The failure could endanger user safety, possibly causing injury or fatality	User-generated errors in system operations could lead to an incident (i.e., safety effects)	National or international laws that prohibit the use of the system	Organizational framework needed that is completely missing (i.e., new services)	General issues considered vital for the system.
7-8 (severe)	The failure results to complete loss of system functions, resulting in user's dissatisfaction	Errors caused by user behaviour may negate system benefits	The existing legislation cannot support the system implementation and relevant work needs to be done.	Organizational framework adaptation is needed (some initial actions have been taken on this domain)	General issues considered severe for the system.
5-6 (slightly severe)	The failure implies the partial loss of the system function, resulting in user's dissatisfaction	User's behavioural changes may significantly reduce the positive effects of the system	New legislation is required for system implementation and work required has already been performed	Organizational framework adaptation is needed which has already started being realized	General issues considered slightly severe for the system.
3-4 (significant)	The failure leads to slight user dissatisfaction	Changes to User behaviour may affect the positive system aspects	New legislation is needed for system implementation, but consensus exist	There is a necessity for adopting a limited number of organisational changes	General issues considered significant for the system.
1-2 (insignificant)	The failure does not conceivably affect the system function and user's satisfaction	Changes to user behaviour is not expected to affect the system benefits, may even further enhance them	No new legislation is needed for implementation	There is no necessity for organizational changes	General issues considered insignificant for the system

---

[1] https://www.isixsigma.com/uncategorized/fmea-quick-guide/

Table 7: Occurrence Levels

Occurence Level	Technological issues	Behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (very high)	It is virtually certain that some errors/failures will occur	It is virtually certain that behavioural effects will occur (by the system users)	It is virtually certain that some legal issues/ problems will occur	It is virtually certain that there will be a need for organizational restructuring	It is virtually certain that some general issues/problems will occur
6-8 (medium-high)	An error/failure can well occur.	Certain behavioural effects can occur	Possible legal problems/issues could occur	Organizational restructuring is required (depending on needs of service, after system is operational)	General difficulties and problems/issues could well occur
3-5 (medium-low)	It is unlikely that a failure/error will occur	It is doubtful that any behavioural effects will occur	It is improbable that any legal issues/problems will occur	It is improbable that a need for organizational restructuring will occur	It is improbable that general problems/issues and difficulties could occur
1-2 (highly improbable)	It is improbable that an error/fault will occur	It is very improbable that any behavioural effects will occur	It is very unlikely that any legal issues/problems will occur	It is very unlikely that a need for organizational restructuring will occur	It is very unlikely that general issues/problems could occur

Table 8: Recoverability Levels

Recoverability Level	Technological issues	Behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (null)	No action is issued for recovery	The system does or does not comply with the user's behavioural effects	The legal framework accepts or rejects the system	A fixed organizational environment is necessary for the system to operate	No recovery action is provided for a general issue
6-8 (low)	Only on the case of failure is the user advised	The system takes under consideration the behavioural effects	The system may be slightly adapted to comply with legal restrictions	The system is in need of a fixed organizational framework with limited adaptations	System may be slightly adapted to meet a general issue
3-5 (high)	Effective action is issued for recovery	The system modification might compensate for user's behavioural effects	The system encloses different versions to meet legal demands	The system may be functioning within various organizational frameworks	Effective recovery action is provided for a general issue
1-2 (full recoverability)	The failure effect is completely avoided by the recovery action	System does not allow user's behavioural effects	System is easily reconfigurable to meet legal demands	System does not require organizational changes	The effect of a general issue is completely avoided by the recovery action

Table 9: Detectability Levels

Detectability Level	Technological issues	Behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (improbable)	It is unlikely or not possible to detect a problematic area	It is unlikely or not possible to detect a user's behavioural effect	It is unlikely or not possible to detect a legal problem	It is unlikely or not possible to detect an organizational problem	It is unlikely or not possible to detect a general issue
7-8 (slight)	The detection of the problematic area is achieved only in particular cases	The detection of a user's behavioural effect is achieved only in particular cases	The detection of a legal problem is achieved only in particular cases	The detection of an organizational problem is achieved only in particular cases	The detection of a general issue is achieved only in particular cases
5-6 (moderate)	It is likely to detect the problem (depending on the situation)	It is likely to detect the user's behavioural effect	It is likely to detect the legal problem	It is likely to detect the organizational problem	It is likely to detect a general issue
3-4 (high)	It is very likely to detect the problem	It is very likely to detect the user's behavioural effect	It is very likely to detect the legal problem	It is very likely to detect the organizational problem	It is very likely to detect a general issue
1-2 (very high)	It is certain to detect the problem	It is certain to detect the user's behavioural effect	It is certain to detect the legal problem	It is certain to detect the organizational problem	It is certain to detect a general issue

7.5.2. Total Risk Estimate and Critical Items Identification

The estimated RPN is utilised by the partners involved to determine which regions are susceptible to failure, allowing them to take preventative actions to avert a potential failure. High RPN values indicate crucial regions that should be prioritised. There is a plethora of preventative and mitigating activities that may be utilised to solve them, including adjustments to the design, modifications to various parameters, additional inspections, testing, and re-evaluation to maintain quality, among others. Table 10 outlines a correlation between the RPN value and the overall severity level.

Table 10: Correlation between RPN and Overall Severity level

RPN	Overall Severity Level
1-8	V – Insignificant
8-64	IV – Slight
64-216	III – Moderate
216-512	II- Severe
512-1000	I- Extremely severe

The authors of [2] emphasize the importance of calculating a project's overall risk estimate, namely the Total Risk Estimate (TRE). To this end, the TRE value can be obtained by

$$TRE = \frac{\sum_{i=1}^{n} RPN_i}{1000n} \times 100\% \qquad (2)$$

where n stands for the total number of identified risks. Of note, TRE values above 17% are considered as 'risky' [2].

7.5.3. Mitigation Actions

Following the identification of critical points, the implementation of strategies and activities to minimise or mitigate the risks occurs. The success of these activities and strategies should also be continuously assessed. Typically, risks may be managed in a variety of ways; also, several of them may depend on others.

A mechanism for the suitable choice of these strategies is one of the FMEA method's shortcomings. Numerous crucial elements, such as the practicability and appropriateness of the suggested plans and actions are ignored. To this end, the authors of [1] suggest an approach for evaluating the success of these strategies and actions. The first step of the approach involves ranking each action according to its feasibility, while the second step involves comparing the RPN values before and after corrective actions are applied.

The effectiveness of the corrective actions can be quantified using the following equation:

$$\Delta RPN = \frac{\sum_{i=1}^{n} RPN_i^{before} - \sum_{i=1}^{n} RPN_i^{after}}{\sum_{i=1}^{n} RPN_i^{before}} \times 100\% \qquad (3)$$

Finally, Table 11 summarises feasibility level ranks, with 1 being the highest and 10 the lowest.

Table 11: Ranking of Corrective Actions Feasibility

Feasibility of Corrective Actions	Rank
Safety issues and/or non-compliance with regulations No resources available Unacceptable consumption of time/cost/resources Zero chance of success 100% probability of unwanted impact	10
Very remote availability of required resources Almost unacceptable consumption of time/cost/resources Very low chance of success ~90% probability of unwanted impact	9
Remote availability of required resources Near unacceptable consumption of time/cost/resources Remote chance of success ~80% probability of unwanted impact	8
Very low availability of required resources Very high consumption of time/cost/resources Very low chance of success ~70% probability of unwanted impact	7
Low availability of required resources High consumption of time/cost/resources Low chance of success ~60% probability of unwanted impact	6
Rather low availability of required resources Relatively high consumption of time/cost/resources	5

Rather low chance of success ~50% probability of unwanted impact	
Moderate availability of required resources Medium consumption of time/cost/resources Moderate chance of success ~40% probability of unwanted impact	4
Some availability of required resources Rather low consumption of time/cost/resources Some chance of success ~30% probability of unwanted impact	3
Good availability of required resources Low consumption of time/cost/resources Good chance of success ~20% probability of unwanted impact	2
Full availability of required resources Very low consumption of time/cost/resources High chance of success 0-10% probability of unwanted impact	1

7.6. EFMEA in NANCY

The risk management approach that will be used in NANCY is based on the EFMEA. The risks are organized into three categories, namely a) administrative risks, b) technical and scientific risks, and c) business risks, while the EFMEA is applied to each category. Initially, the risks are identified and the corresponding RPNs are calculated using the Severity, Occurrence, Recoverability, and Detectability values. Next, the respective mitigation strategies are outlined for each risk.

7.6.1. NANCY Risks Identification

The identified risks for the NANCY project are presented in the following tables, along with the respective RPN values and risk levels. Specifically, Table 12 presents the administrative risks, Table 13 presents the technical and scientific risks, and Table 14 presents the business risks.

Table 12: Administrative Risks

WP	Risk	S	O	R	D	RPN	Risk Level
WP1	AR1: Insufficient consortium coordination	8	3	2	8	120	III – Moderate
WP1	AR2: Lack of communication among the partners	8	3	2	7	108	III – Moderate
WP1	AR3: Shortage of resources and/or change of personnel	8	4	2	7	144	III – Moderate
WP1	AR4: Partner withdrawal	7	5	5	1	105	III – Moderate

Figure 17 illustrates the sorted RPN values, along with a threshold that is employed to distinguish critical risks. The threshold value is set to 180 based on empiric estimations and knowledge of the project's domain.

Figure 17: Administrative Risks RPN Values

Using (1), the TRE value is **11.93%.** Taking into account that the value is below 17%, NANCY features an overall low risk level with respect to administrative risks.

Table 13: Technical and Scientific Risks

WP	Risk	S	O	R	D	RPN	Risk Level
WP2, WP3, WP4, WP5, WP6	STR1: Insufficient consortium R&D competence / effectiveness	6	4	3	2	60	IV – Slight
WP2	STR2: Tight schedule for the Reference Architecture	6	6	3	1	72	IV – Slight
WP2	STR3: Disagreement on scenarios/requirements	6	7	4	3	147	III – Moderate
WP2	STR4: Unrealistic use cases or impossible deployments	9	6	3	1	108	III – Moderate
WP3	STR5: Disagreement on the overall architecture design	6	4	3	2	60	IV – Slight
WP3	STR6: Underestimate problems coping with new technology (e.g., SDN connectivity, MEC, blockchain)	6	6	3	1	72	IV – Slight
WP3	STR7: Particular devices and embedded systems (e.g., AI accelerator) not mature enough, or not available.	1	5	1	2	7.5	V - Insignificant
WP4	STR8: Designed resource management and orchestration schemes are too complex for practical implementation	7	4	2	2	56	IV – Slight
WP4	STR9: Optimal cooperative access mechanism may require a practically unaffordable synchronization overhead	7	3	2	2	42	IV – Slight
WP5	STR10: Designed blockchain-based mechanisms cannot be implemented in the low-computational nodes	7	3	2	2	42	IV – Slight

WP	Risk					RPN	Risk Level
WP5	STR11: Lack of data for methods related to privacy and anomaly detection	4	5	2	2	40	IV – Slight
WP2, WP6	STR12: Development risks associated with ambitious development objectives and obsolescence of technology may result in general delays for the whole project.	9	6	3	1	108	III – Moderate
WP6	STR13: Delays in the deployment of the Application layer	5	6	3	4	105	III – Moderate
WP6	STR14: Inability to perform integration/verification due to (a) lacking support for specific applications, or (b) underperformance of partners with respect to integration tasks	6	6	3	1	72	III – Moderate
WP3	STR15: The utilized training models are insufficient for a specific use case	5	6	3	4	105	III – Moderate

Figure 18 illustrates the sorted RPN values, along with a threshold that is employed to distinguish critical risks. The threshold value is set to 180 based on empiric estimations and knowledge of the project's domain.
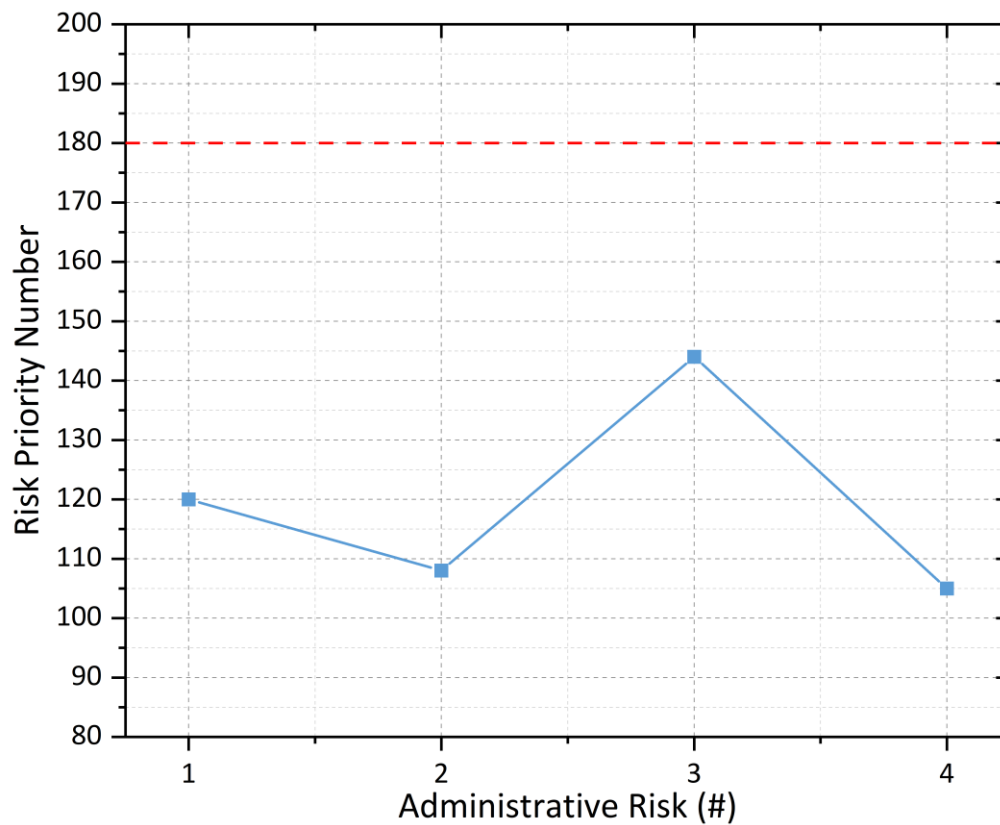

Figure 18: Technical & Scientific Risks RPN Values

Using (1), the TRE value is **7.31%.** Taking into account that the value is below 17%, NANCY features an overall low risk level with respect to technical and scientific risks.

Table 14: Business Risks

WP	Risk	S	O	R	D	RPN	Risk Level
WP1	BR1: Conflicts over ownership	7	5	2	2	70	III – Moderate
WP1, WP6	BR2: Insufficient Project Impact / Low Community Building & Stakeholders Engagement	6	4	4	3	84	III – Moderate

WP2	BR3: Failure to provide comprehensive use cases and elicit solid requirements	6	4	4	3	84	III – Moderate
WP1, WP6	BR4: Low awareness of the calls/ Communication actions is not effective	6	3	3	4	63	IV – Slight
WP6	BR5: Proposals received are not fitting with the type of project expected	2	3	3	2	15	IV – Slight
WP1	BR6: Low level of engagement of the 5G and communications Community	6	4	3	4	84	III – Moderate

Figure 19 illustrates the sorted RPN values, along with a threshold that is employed to distinguish critical risks. The threshold value is set to 180 based on empiric estimations and knowledge on the project's domain.
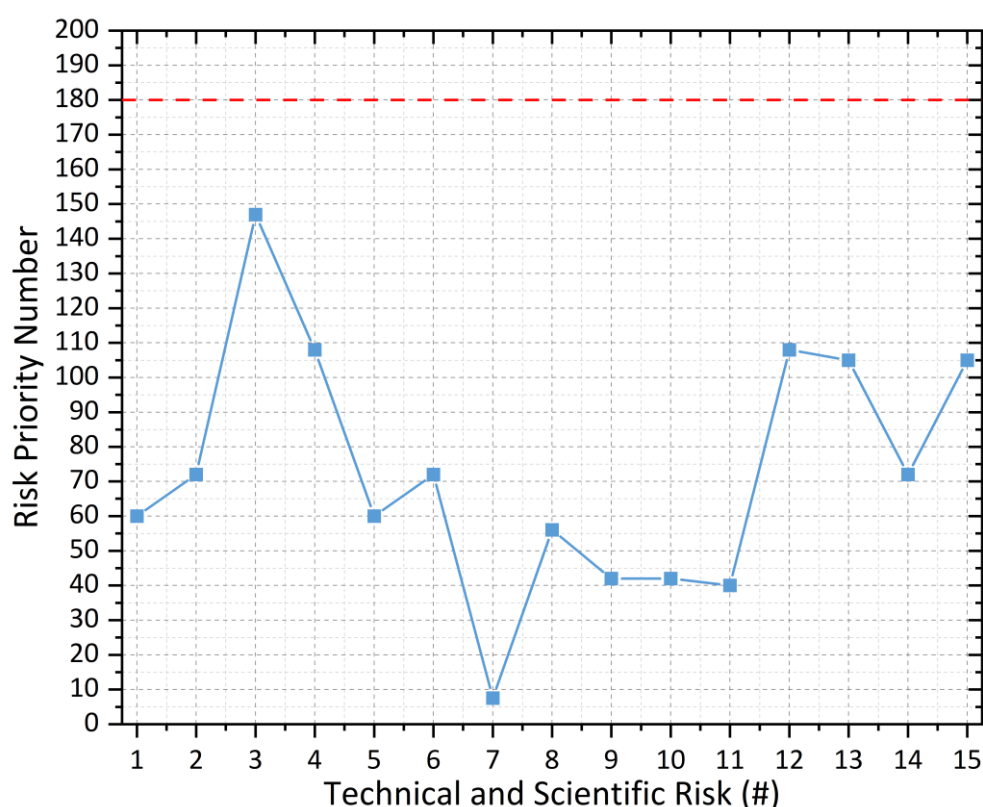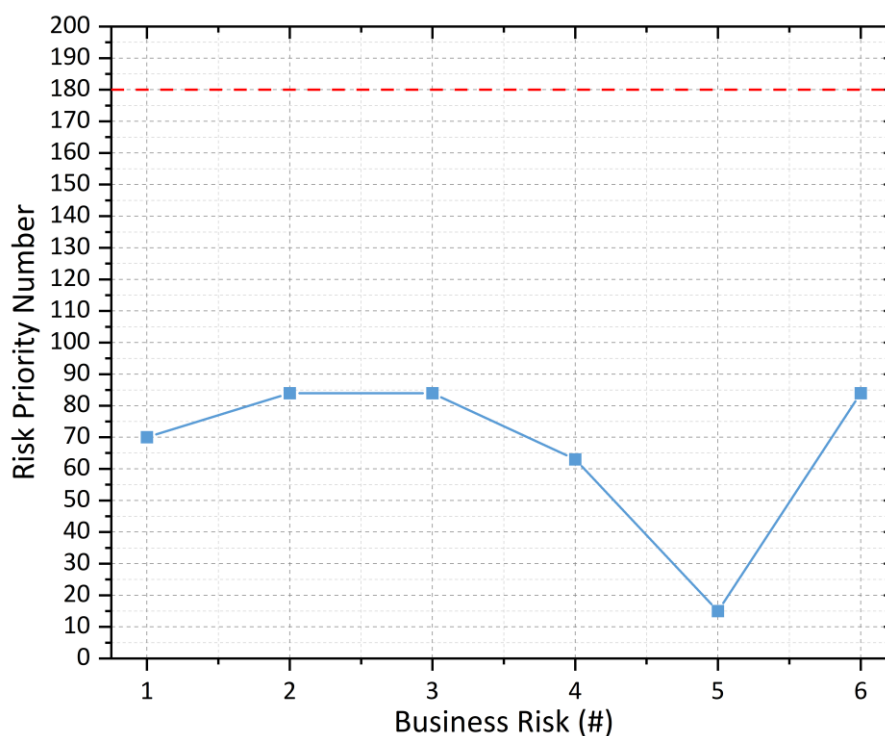

Figure 19: Business Risks RPN Values

Finally, using (1), the TRE value is **6.67%.** Taking into account that the value is below 17%, NANCY features an overall low risk level with respect to business risks.

7.6.2. NANCY Risks Mitigation Actions

After the risk identification and the respective RPN values calculation, the design of mitigation actions takes place. To this end, an indicator measuring the possibility of the mitigation action is introduced (Table 15).

Table 15: Mitigation Possibility Indicator

Mitigation Possibility	Description
Improbable	The mitigation action is too expensive in relation to the reduction of risk(s) and the benefits gained do not justify its application.
Low	An expensive mitigation action may be applied, but benefits may not justify it and/or further investigation is required.
Medium	A mitigation action may be possible at a reasonable cost.
High	The mitigation action is low-cost and can be easily applied.

Tables 16, 17, and 18 outline the administrative, technical and scientific, and business risks, along with the respective RPN values, risk levels, mitigation strategies, and mitigation possibility.

Table 16: Administrative Risks

WP	Risk	RPN	Risk Level	Mitigation Strategy	Mitigation Possibility
WP1	AR1: Insufficient consortium coordination	135	III – Moderate	The effective management of the consortium will be assured with the appropriate Project Management (Section 3.2.1). If the need arises, UOWM will assign a deputy to assist the PC. In the unlikely event of the PCC receiving complaints about the quality of the coordination activities, the consortium will vote for the substitution of the coordinator.	Medium
WP1	AR2: Lack of communication among the partners	108	III – Moderate	Regular remote and physical plenary and technical meetings will be organized at the consortium and WP levels, as well as at Task level to safeguard smooth technical implementation & communications among partners. Insufficient communication amongst partners will be escalated to the PC, who will try to encourage smoother collaboration. If the issue persists, solid goals will be set for all teams involved which will be monitored closely. Failure to meet the goals set will be penalized.	High
WP1	AR3: Shortage of resources and/or change of personnel	144	III – Moderate	All partners have assured they will allocate the appropriate personnel to implement all agreed activities and will make binding agreements on resource availability. In case of personnel substitution with another team member, the new member must demonstrate comparable competencies. The same applies to the shortage of (personnel) resources. Shortage of financial resources will be evaluated with the FO, PO, and PC to identify if resources have been misspent and remediation actions will be taken (cover from own resources or re-allocate remaining resources).	Medium
WP1	AR4: Partner withdrawal	105	III – Moderate	Immediate substitution by another partner, from existing research partnerships or through dissemination activities. The establishment of the NANCY TAFGL will help expand options in such a case	Low

Table 17: Technical and Scientific Risks

WP	Risk	RPN	Risk Level	Mitigation Strategy	Mitigation Possibility
WP2, WP3, WP4, WP5, WP6	STR1: Insufficient consortium R&D competence / effectiveness	60	IV – Slight	The project team is highly complementary and gathers together the requested skills for the main streams of RTD. All technologies to be used in the implementation of the project will be carefully selected so as to minimize potential risks based on these technologies. If consortium incompetence is identified, the consortium partners will try to fill this gap either through their own pools of resources or through subcontracting.	Medium

WP2	STR2: Tight schedule for the Reference Architecture	72	IV – Slight	WP2 is diverse: it covers requirements analysis (T2.1), supported use cases definition (T2.3), and a rigorous start of developing the reference architecture (T2.2). By consolidating this in a single WP, it ensures top coordination and execution for tasks equally needed for the project to advance. The workplan needs to start strong. Additional resources will be allocated if needed	Medium
WP2	STR3: Disagreement on scenarios/requirements	147	III – Moderate	A project management meeting will be organised to harmonise disputed areas and agree upon a backup time plan.	High
WP2	STR4: Unrealistic use cases or impossible deployments	108	III – Moderate	Definition of use cases by relevant internal stakeholders, which will take into account the feedback from external stakeholders through workshops and demos	Medium
WP3	STR5: Disagreement on the overall architecture design	60	IV – Slight	Decisions will be consensus-based. If this fails, the technical committee will propose alternative solutions and a majority decision after a GA will be taken.	High
WP3	STR6: Underestimate problems coping with new technology (e.g., SDN connectivity, MEC, blockchain)	72	IV – Slight	The PC and TC will monitor development progress, detect development problems early and proceed with corrective actions. Re-schedule and re-evaluate assigned PMs towards delivering on time the NANCY platform for intervention study and use. Resources have been allocated for technical meetings	Medium
WP3	STR7: Particular devices and embedded systems (e.g., AI accelerator) not mature enough, or not available.	7.5	V - Insignificant	NANCY will support device-independent rendering in order to simplify migration to different devices.	High
WP4	STR8: Designed resource management and orchestration schemes are too complex for practical implementation	56	IV – Slight	Develop a sub-optimal framework (by relaxing constraints) that is implementable.	High
WP4	STR9: Optimal cooperative access mechanism may require a practical unaffordable synchronization overhead	42	IV – Slight	Sub-optimal (selection-combine-based) CoMP mechanisms will be developed in order to guarantee the low-latency requirement.	High
WP5	STR10 Designed blockchain-based	42	IV – Slight	Nodes with more computational resources will need to be provided, as security is a mandatory requirement	Medium

	mechanisms cannot be implemented in the low-computational nodes				
WP5	STR11 Lack of data for methods related to privacy and anomaly detection	40	IV – Slight	The partners will consider alternative solutions in case data availability is low such as synthetic or artificially generated data.	High
WP2 , WP6	STR12 Development risks associated with ambitious development objectives and obsolescence of technology may result in general delays for the whole project.	108	III – Moderate	Strong reuse of results from other projects and available open-source tools. Continuous monitoring of results/trends from on-going RTD activities in this domain.	Medium
WP6	STR13 Delays in the deployment of the Application layer	105	III – Moderate	Integration partner (INTRA) has a long experience in the running of platforms	Medium
WP6	STR13 Inability to perform integration/verification due to (a) lacking support for specific applications, or (b) underperformance of partners with respect to integration tasks	72	III – Moderate	The Integration WP leader (INTRA) has long standing experience in the field, and has taken into account the following considerations to ensure a smooth integration process: (a) WP6 does not explicitly depend on a single technology that is irreplaceable for the purpose of integration/verification/testing. The WP6 partners have extensive experience in integration and verification processes to identify appropriate solutions and measures for the support of each application in the context of integration and verification. (b) This risk of underperformance is highly mitigated by the careful selection of participating partners. In case a partner underperforms and significantly hinders the integration process, alternative solutions with respect to APIs and abstraction layers will be investigated. Otherwise, the project general assembly (according to the stipulations of the GA) will decide on partner effort redistributions.	Medium
WP3	STR14: The utilized training models are insufficient for a specific use case	105	III – Moderate	The training models will be carefully designed and refined from the early NANCY stages and throughout all use cases. Therefore, potential shortcomings will be identified and addressed early.	High

Table 18: Business Risks

WP	Risk	RPN	Risk Level	Mitigation Strategy	Mitigation Possibility
WP1	BR1: Conflicts over ownership	70	III – Moderate	Disagreements over ownership may result in non-agreement on IPR. The principles and the existing assets included in the CA, and the continuous Task 1.4 on IPR handling & innovation management will ensure proper protection of the IPRs of foreground and background knowledge. All conflicts over ownership will be resolved at consortium level based on the CA and the agreed assets ownership and IPR management.	High
WP1, WP6	BR2: Insufficient Project Impact / Low Community Building & Stakeholders Engagement	84	III – Moderate	The extended networks of the project consortium partners will reassure the reach out of a critical mass of stakeholders, policy makers, and vendors. Dissemination, communication, and industrial clustering activities will safeguard significant project impact creation. If need be, these activities will be enhanced, additional events may be organized and additional resources will be mobilized to boost stakeholders' reach out.	Medium
WP2	BR3: Failure to provide comprehensive use cases and elicit solid requirements	84	III – Moderate	As of Day #1, the consortium will try to aggregate and analyse all functional and non-functional, generic, and demonstrator-specific requirements. These requirements will be translated into technical requirements, and in turn into technical components. These activities will be orchestrated by experienced project partners. Should additional requirements be identified in the future, because of the agile development process, the consortium will try to integrate the new functionalities in the platform to the extent possible.	Medium
WP1, WP6	BR4: Low awareness of the calls/ Communication actions is not effective	63	IV – Slight	This risk has a low probability to happen due to the great network and experience of the project partners in the 5G and communication domains. In any case, special measures will be taken, making available the Operating Committee submissions board/reception checking regularly the process, submissions, visits to the relevant pages and announcements, and participation in the webinars. If the reception of proposals is lower than expected, the dissemination activities will be increased. Online actions will be reinforced, also actions with Partners' Networks, and even organising additional Webinars.	High
WP6	BR5: Proposals received are not fitting with the type of project expected	15	IV – Slight	The project is looking for specific profile researchers, SMEs and corporates, and Internet innovators and it will be clearly communicated from the beginning with a clear and targeted communication plan. The evaluation process, experts, and criteria applied will ensure the quality of the proposal. In case during the evaluation, we found out that the proposals are not good enough for the type of project expected, we would only select the proposals reaching the desired level. The non-compromised funds will be added to the following open call or, if needed, a new open call will be scheduled focusing even more on the actions to be done to get good proposals.	Medium
WP1	BR6: Low level of engagement of	84	III – Moderate	The probability that this will happen is very low due to the comprehensive community building	High

	the 5G and communications Community			and engagement plans defined, in combination with the strong engagement of the consortium members in the communications area, which will ensure the effective outreach and involvement of the community.	

After applying the EFMA methodology, it can be deduced that NANCY does not pose any critical risks. Nevertheless, to ensure the quality of the project outcomes, the "moderate" risks will be monitored thoroughly. The monitoring, identification, and analysis of risks will be a continuous process throughout the NANCY's duration.

The primary aim of this continuous process is the assessment of the proposed risk management plan, the documentation of newly identified risks, the evaluation of the adequacy of agreed mitigation actions, and the documentation of historical data about risks, including the dates they were identified or modified.

Currently, none of the aforementioned risks have materialised. EFMEA analysis and the iterative process of monitoring and re-evaluation of the management plan and Register ensure that risk levels will remain low until the NANCY project is completed.

8. Conclusion

This deliverable provides an overview of the main principles that should be followed while coordinating and administering the NANCY project. All tools and processes are defined for monitoring and managing the project's progress. Specifically, the deliverable outlines the design of a thorough monitoring plan for the implementation of the tasks throughout the duration of the project. This monitoring and management plan includes processes for organizing, monitoring, and reviewing the performance and progress of the NANCY project. Moreover, the deliverable introduces the risk management process that will be followed throughout the project's duration in order to safeguard the quality of the project outcomes and the successful completion of the project. This deliverable will be used by the NANCY consortium in order to establish a common understanding of the guidelines, rules, and processes for project monitoring, management, and implementation.

References

[1] Z. Bluvband, P. Grabov and O. Nakar, "Expanded FMEA (EFMEA)," in *Annual Symposium Reliability and Maintainability, 2004 - RAMS*, Aug. 2004.

[2] Z. Bluvband and P. Grabov, "Failure analysis of FMEA," in *2009 IEEE Annual Reliability and Maintainability Symposium*, Jan. 2009.