D7.1 - Project Handbook

Work Package:	WP7
Lead partner:	ENG
Author(s):	Gabriele Giunta (ENG)
Due date:	M2
Version number:	1.0
Status:	Final

Project Number:	101073909	**Project Acronym:**	ATLANTIS
Project Name:	Improved resilience of Critical Infrastructures AgainsT LArge scale transNational and sysTemic rISks		
Start date:	October 1st, 2022		
Duration:	36 months		
Call identifier:	HORIZON-CL3-2021-INFRA-01		
Topic:	HORIZON-CL3-2021-INFRA-01-01 European infrastructures and their autonomy safeguarded against systemic risks		
Instrument:	IA		

Dissemination Level	
PU: Public	✓
SEN: Sensitive	

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909

Revision History

Revision	Date	Who	Description
0.1	01/ 11/ 2022	ENG	Table of Contents
0.2	08/ 11/ 2022	ENG	PM and Dissemination
0.3	15/ 11/ 2022	ENG	Monitoring, Reporting, Project Meetings
0.4	22/11/2022	ENG	Quality and Risk
0.5	28/11/2022	ENG	Integrated feedback from SYN and CERTH peer review
1.0	30/11/2022	ENG	Final version

Quality Control

Role	Date	Who	Approved/Comment
Internal review	*28/11/2022*	SYN	Approved with minor revisions
Internal review	*28/11/2022*	*CERTH*	Approved with minor revisions

Disclaimer

Executive Summary

This document outlines the internal procedures of the ATLANTIS project in terms of project execution, administrative management, management structures, communication and collaboration. It contains all the guidelines, processes, procedures, tools to be adopted by all partners to refer during the lifetime of the project. In addition, it describes the risk management processes and internal Quality Assurance (QA) procedures to be applied within the ATLANTIS project. Along with the QA procedures, an initial list of quality management assignments to the partners regarding the quality control of ATLANTIS deliverables is also presented. Likewise, as part of the risk management methodology, the document presents the risk registry of the project. The latter will be periodically updated and reviewed by the coordinating team and the work package leaders.

Table of Contents

List of Figures

List of Tables

Definitions and acronyms

AB	Advisory Board
BDVA	Big Data Value Association
CA	Consortium Agreement
CEAB	CIP-Experts Advisory Board
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
C/P	Cyber/Physical
CPH	Cyber-Physical-Human
CTITF	Counter Terrorism Implementation Task Force
DAIRO	Data, AI and Robotics
DCM	Dissemination & Communication Manager
DE	Deliverable
DevOps	Development and Operations
DLT	Distributed Ledger Technology
DoA	Description of Action
EC	European Commission
ECSCI	European Cluster for Securing Critical infrastructures
ELM	Ethical & Legal Manager
EU	European Union
EUAB	End-Users Advisory Board
FAIR	Findability, Accessibility, Interoperability, and Reusability
GA	Grant Agreement
GAP	Grant Agreement Preparation
IPR	Intellectual Property Rights
IR	Internal Reviewer
IRMA	Incident Response Management
ITU	International Telecommunication Union
MHMS	Model Hospital Management System
ML	Machine Learning
MS	Microsoft
NATO	North Atlantic Treaty Organization
PC	Project Coordinator
PO	Project Officer
PU	Public
RP	Reporting Period
QA	Quality Assurance
QM	Quality Manager
QRM	Quality and Risk Manager
QMP	Quality Management Plan
QMS	Quality Management System
PMT	Project Management Team
PSC	Project Steering Committee
RM	Risk Management
SAB	Security Advisory Board
SEN	Sensitive
SIPS	Sensitive Industrial Plants and Sites
SME	Small and Medium Enterprise
TM	Technical Manager
TL	Task Leader
UNODC	United Nations Office on Drugs and Crimes
WP	Work Package
WPL	Work Package Leader

1. Introduction

The Project Handbook guarantees the processes applied throughout the project lifecycle by describing all procedures to assure delivery with the expected quality.

The purpose of this document is to provide the ATLANTIS consortium partners with a specific set of guidelines and procedures to be applied within the lifetime of the project ensuring that all the agreements with the European Commission and between partners will be respected. In particular, guidelines on the day-to-day project management and on the practical aspects of the project development, including reports, editing procedures, criteria for work results performance measurements as well as procedures for document handling are also included. In addition, this document provides risk management processes and internal QA procedures to be applied through the project in order to ensure quality of project's outcomes. It is relevant to mention that this document has a dynamic nature and therefore, it will be, if necessary, updated during the project lifespan.

This deliverable is a public deliverable (PU).

The structure of the deliverable can be shown below:

- Section 2 presents an overview of the ATLANTIS Project Management. In particular, an overview of the project including the consortium and the partners as well as the project structure and schedule are illustrated. Moreover, the ATLANTIS Management Structure accompanied by the Project Management Roles are analysed along with their main responsibilities and tasks.
- Section 3 presents the project's communication principles and tools to be used. In details, all the guidelines for internal communication and collaboration and external communication are illustrated along with the main tools used. ATLANTIS 's online collaborative environment and instructions on how to join it are illustrated.
- Section 4 depicts the project control processes, the procedure for submitting deliverables within the project, and reporting principles.
- Section 5 presents the procedure for ATLANTIS's meetings.
- Section 6 describes the Quality Management (QM) and Risk Management (RM) principles.
- Section 7 provides a conclusion of the deliverable.
- Annex I presents a set of templates that will be used within ATLANTIS.

2. Project Management

The general purpose of the project management is progress control of each work package, coordination of the different project activities and implementation of quality control mechanisms by issuing appropriate project standards. Project management will cover financial, administrative, scientific, as well as knowledge and innovation aspects. The ATLANTIS project is divided into eight work packages, and these are in turn divided into Tasks according to the goals and structure of each WP. Each Task has the number of partners required to fulfil the goals of the specific activity. One partner may contribute to more than one activity within one or more WPs.

2.1. ATLANTIS overview

ATLANTIS aims at enhancing resilience and Cyber-Physical-Human (CPH) security of the key EU Critical Infrastructures, going beyond the scope of distinct assets, systems, and single CI, by addressing resilience at the systemic level against major natural hazards and complex attacks that could potentially disrupt vital functions of the society. The mission of ATLANTIS is to guarantee the continuity of operations, while minimizing cascading effects in the infrastructure itself, the environment, other CIs, and the involved population, enabling public and private actors to meet current and emerging challenges by adopting sustainable security solutions.

The project's analytics capabilities will fulfil the reporting requirements listed in the call in terms of the number and the (semestrial) frequency of the reports. To facilitate information collection and analysis, the project will establish a FAIR data observatory of research projects, research outcomes, technologies, standards, and policies. Along with analytical capabilities for evidence-based policies, the project will organize and offer a rich set of innovation support services to EU projects and other innovators in CI security and resilience.

2.1.1. ATLANTIS Consortium

The thirty-eight (38) ATLANTIS partners come from 10 countries (Italy, France, Germany, Slovenia, Spain, Croatia, Greece, Luxemburg, Romania and Cyprus), while 8 additional countries (Austria, Albania Belgium, Hungary, Netherlands, Slovakia, Czech and Serbia) are indirectly associated. ATLANTIS partners have committed to work towards the goal of project: Enhancing European CI against systemic risks. The consortium exhibits great complementarity in technological skills and outreach/impact potential increasing the chances of ATLANTIS to achieve its ambitious impact-creation plan (Figure 2-1)

The ATLANTIS consortium is perfectly balanced in terms of company types, expertise, role in the value chain and geographical distribution to meet all EC criteria. All partners have world-wide expertise in their fields of activities and the capacity and resources to fulfil the project objectives, comprising:

1) **7 Technology Providers:** (1) *ENG* with more than 1.24B€ annual revenue in 2020 is a leading security and mission critical solutions provider with approximately 12,000 professionals in 40+ locations, with a clear focus in critical infrastructures, cybersecurity and energy utilities; (2) *CS group* is a leading cybersecurity company that designs, develops, deploys, maintains and operates surveillance, tactical and cybersecurity systems; (3) *RES* is VINCI's design office dedicated to adapting cities, territories, infrastructures and their uses to climate change (VINCI is one of the largest

construction companies in the world with 42B€ revenues in 2020); (4) *INTRA* is the leading European IT solutions' and, with strong international presence in more than 17 countries, and since 8 Oct. 2021, member of the NetCompany group, member of the EU blockchain observatory and board member of DAIRO/BDVA; (5) *SLG*, member of the Space Hellas Group, is a leading software and digital integrated solutions provider for large enterprises, also supplier of the Model Hospital Management System (MHMS) at all hospitals in HYGEIA Group in both Greece and abroad; (6) *TS* is the largest telecom operator in Slovenia already offering 5G services; (7) *SIEM* is a world leader in complex infrastructures solutions and an active provider of sustainable green technologies. SIEM develop hardware and software systems and solutions, and a broad range of services for the entire field of information and communication technologies, while the department participating in ATLANTIS encompasses fields like Data Analytics and Monitoring, Constraint Based Configurations and Schedulers, Complex Cybersecurity Event Processing, Industrial-grade DevOps and Federated Platforms

2) **6 Specialized SME**: (1) *SYN* a leading SME in ML and cybersecurity, partner of HPE and technical coordinator of large cybersecurity projects such as H2020 PHOENIX and IOT-NGIN; (2) *NetU* is a leading IT SME in the Eastern Mediterranean, that collaborates with the biggest banks and finance organizations in Cyprus and Greece and has implemented the Tax Administration System for the Tax Department of the Cyprus Ministry of Finance and the Schengen II Information System for border control of Cyprus, Greece and Croatia; (3) *BYTE* is leading IT SME in cybersecurity, E.H.R. and digital signatures and has implemented the Greek Electronic Prescription System; (4) *SNEP* builds digital twins software for CI, and (5) *ATC* builds solutions for smart banking and ML based disinformation detection systems. (6) *CRI* provides legal/ethical research institute, as well as advisory services SME in relation to strategy, policy and legislation in more than 50 countries and international organizations such as the International Telecommunication Union (ITU) High Level Expert Group on Cybersecurity, United Nations Office on Drugs and Crimes (UNODC) Core Expert Group on ID-Related Crime, United Nations Counter Terrorism Implementation Task Force (CTITF) and the North Atlantic Treaty Organization (NATO).

3) **11 CI Owners/Operators/End-users:** (1) *Luka Koper (LUK)* and (2) *Luca Rijeka (LUR)* are international ports in Slovenia and Croatia respectively. They both feature passengers and cargo terminals, tanker peers and fuel tanks and cargo throughput of 25M and 13.6M tonnes respectively. They are both connected with highways and railway hubs. (3) *DARS* is the Slovenian National Highways operator, that guarantees road safety and uninterrupted traffic flow on more than 600km of highways, motorways and expressways and (4) *SZ* is the Slovenian National Railways, operating 1,229 km of standard gauge tracks and 331 km as double track. SZ connects with the Italian Railways, creating a continuous railway network that serves Slovenia and Italy. The Italian railway network is represented by (5) *FST*, the IT company of the group that implements new AI, robotics and IoT solutions targeting the railway infrastructure. (6) *PET* is not only the largest Slovenian energy company, but also the largest Slovenian importer, the largest Slovenian company in terms of revenues, and one of the largest Slovenian retail companies with fuel tanks in LUK and significant importance for Slovenia fuel stability. (7) *SITAF* is the Highway Concessionaire in north Italy and controller of the A32 Motorway - T4 Frejus tunnel, while (8) *SDIS73* is the French Fire and Rescue Services covering the Frejus tunnel. (9) *HYG* is the largest group offering healthcare services in Greece. It owns 3 hospitals in Greece, with a total capacity of 1,261 beds and until recently also Hygeia General Hospital in Tirana. (10) *JRC* is an

independent investment house specialized in Forex and Derivatives. JRC is regulated by the BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), is member of the compensatory fund of securities trading companies (EdW) and is supervised by the Bundesbank. (11) *CXB* is the global leader in card payments and mobile financial services – to date, CXB has rolled-out over 60,000 contactless POS terminals in Spain.

4) **9 Research Institutes:** (1) *KEMEA* is the Greek Center for Security Studies, conducting theoretical and applied research and studies, particularly at strategic level, overseen by the Greek Minister of Citizen Protection; (2) *ICS* is the Slovenian Institute of Security studies; (3) SatCen (*SAT*) is the EU Satellite Centre that supports via space assets the EU decision making in the field of Common Security and Defence Policy, including EU crisis management missions and operations; (4) *JSI* is the leading Slovenian scientific research institute; (5) *PRFI* is the biggest high maritime university in the Southeast Europe, specialized in port security; (6) *CEA* LIST Institute one of three CEA institutes with R&D activities in cyber-physical systems, artificial intelligence and digital health; (7) *CERTH* ITI is the leading Greek institution in cybersecurity and AI; (8) *LINKS* is a leading Italian research foundation in digital technology and regional development and (9) *VICOM* is a leading Spanish research institution in Data Analytics.

5) **5 Government entities responsible for security:** (1) *DMIA* is the French Ministry of Interior, responsible for Citizen Security in France; (2) MZI is the Slovenian Ministry for Infrastructure, responsible for Slovenian transport and energy infrastructure security and continuous improvements; (3) *UIV*, the Slovenian Ministry of Information Security, is the competent national authority in the field of information security, which acts as a government office. Its core mission is to increase resilience to cyber threats that can threaten individuals, businesses, government and society at large; (4) *HPL* is the Greek Ministry of Citizen Protection participating via the Greek police and (5) *MDI* is the Italian Ministry of Interior, Department of Public Security, participating via the specialized Italian Police Force responsible for Road, Rail and Communications Security.

Table 2-1 - ATLANTIS Consortium

Number	Role	Short name	Legal name	Country
1	COO	ENG	ENGINEERING - INGEGNERIA INFORMATICA SPA	IT
2	BEN	CS	CS GROUP-FRANCE	FR
3	BEN	RESA	SIXENSE ENGINEERING	FR
4	BEN	INTRA	NETCOMPANY-INTRASOFT SA	LU
5	BEN	SLG	SINGULARLOGIC ANONYMI ETAIREIA PLIROFORIAKON SYSTIMATON KAI EFARMOGONPLIROFORIKIS	EL
6	BEN	TS	TELEKOM SLOVENIJE DD	SI
7	BEN	SIEM	SIEMENS SRL	RO
8	BEN	SYN	SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA	EL
9	BEN	NetU	NET-U CONSULTANTS LTD	CY
10	BEN	BYTE	BYTE COMPUTER ANONYMI VIOMICHANIKIEMPORIKI ETAIREIA	EL
11	BEN	SNEP	SNEP D.O.O.	SI

12	BEN	ATC	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	EL
13	BEN	CRI	CYBERCRIME RESEARCH INSTITUTE GMBH	DE
14	BEN	LUK	LUKA KOPER, PORT AND LOGISTIC SYSTEM, D.D.	SI
15	BEN	LUR	LUCKA UPRAVA RIJEKA	HR
16	BEN	DARS	DRUZBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI D.D	SI
17	BEN	SZ	SLOVENSKE ZELEZNICE DOO	SI
18	BEN	PET	PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA	SI
19	BEN	FST	FSTECHNOLOGY SPA	IT
20	BEN	JRC	JRC CAPITAL MANAGEMENT CONSULTANCY & RESEARCH GMBH	DE
21	BEN	CXB	CAIXABANK SA	ES
22	BEN	HYG	DIAGNOSTIKON KAI THERAPEFTIKON KENTRON ATHINON YGEIA ANONYMOS ETAIREIA	EL
23	BEN	SITAF	SOCIETA ITALIANA TRAFORO AUTOSTRADALE DEL FREJUS SPA	IT
24	BEN	SDIS73	SERVICE DEPARTEMENTAL INCENDIE ET SECOURS DE LA SAVOIE	FR
25	BEN	KEMEA	KENTRO MELETON ASFALEIAS	EL
26	BEN	ICS	INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA	SI
27	BEN	SatCen	EUROPEAN UNION SATELLITE CENTRE	ES
28	BEN	JSI	INSTITUT JOZEF STEFAN	SI
29	BEN	PFRI	SVEUCILISTE U RIJECI, POMORSKI FAKULTET	HR
30	BEN	CEA	COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	FR
31	BEN	CERTH	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	EL
32	BEN	LINKS	FONDAZIONE LINKS - LEADING INNOVATION & KNOWLEDGE FOR SOCIETY	IT
33	BEN	VICOM	FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	ES
34	BEN	DMIA	MINISTERE DE L'INTERIEUR	FR
35	BEN	MZI	MINISTRSTVO ZA INFRASTRUKTURO	SI
36	BEN	UIV	URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST	SI
37	BEN	HPOL	HELLENIC POLICE	EL
38	BEN	MDI	MINISTERO DELL'INTERNO	IT

ATLANTIS consortium technological expertise is summarized at the Figure 2-1. For certain competences, ATLANTIS consortium includes more than one partner, to create a critical mass that minimizes any risk and ensures validation and impact creation.

Participants / Competencies	ENG	CS	RES	INTRA	SLG	TS	SIEM	SYN	NetU	BYTE	SNEP	ATC	CRI	KEMEA	ICS	SatCen	JSI	PFRI	CEA	CERTH	LINKS	VICOM
SW Architecture Solution	X	X	X	X	x	x	X	X	x	x	x				x				x		x	x
Privacy Preserving Federated ML	X			x	X		x	X		x								x	x	x	x	
Human Explainable AI (XAI)	X			x			X					X							x	X	X	x
Intelligence Amplification (IA)		x		x		x			x	x	X			x	x		x		x			
Earth Observation/Climate Change		X	X				x									X				x	x	x
PTN/ GNSS services	x		x	x		X	X	x											x		X	
Digital Twins	x			x					x		X		X	x					x	X	x	x
Disinformation Fight	X	x	x	X	x					x		X	X	x	x		x	x		X		
DLTs & Blockchain Technology	x			X	X	x		X			X							X	X		x	x
Decision Support Systems	x	X		X			X						x	x	x				x		X	
Treat Intelligence			X	x		x	x	x	x				x	x		x	x		X	X	X	x
Cybersecurity/Privacy	X	x	x	X			X	x	x	x			x									
Integrators /Lab testing			x	X	X			X			x			x		x	x	x		x		
Social Science Humanities (SSH)									x	x		x	X	X	x			x				x
Exploitation/Business Models	X	x	x	X	x	X	X									x	x	X				
Communication/Outreach	x	x										X	X	X	X							x
Open Science															X	X	X	X	X	X	X	X

Figure 2-1 - Consortium technological expertise

Some of the ATLANTIS support measures (e.g., validation services) may need access to experimentation infrastructures for validating solutions for resilient infrastructures. The consortium includes prominent European CI operators and authorities, which will provide access to some of Europe's most innovative transport, energy and telecoms infrastructures (LUK, LUR, DARS, SZ, PET, FST, TS, SITAF and SDIS73), financial/assets (CXB, JRC and NetU), hospitals and cloud facilities covering health cyberphysical, logistics/supply chains and border control systems (HYG, BYTE, SLG and NetU) and a micro-cloud of blade servers exclusively used for research and validation purposes to host ATLANTIS CI/CD part and required testing and experimentation in cloud computing, ML training and DLT technologies (SYN).

2.1.2. ATLANTIS Structure and Schedule

The project's workplan has a 36-month duration and is structured in eight (8) work packages (WP). Each WP is focused on as a specific aspect of the project and is internally split up into relevant tasks assigned to partners. The list of the WPs in shown in the Table 2-2:

Table 2-2 -ATLANTIS's list of WPs

WP No	WP Title	Lead beneficiary
WP1	Cross-CI Systemic Risk Assessment & Incidents Mitigation Strategies	25 - KEMEA
WP2	Preventive Technologies to reduce systemic risks by design	5 - SLG
WP3	Protective Technologies to reduce systemic risks by innovation	1 – ENG
WP4	Cooperative prevention, anticipation and mitigation of systemic risks	4 - INTRA
WP5	Cross-CI Large Scale Pilots validation & penetration testing	19 - FST

WP6	Impact Creation and Outreach	26 - ICS
WP7	Project Management	1 – ENG
WP8	Ethics Requirements	1 – ENG

The ethics requirements work package, which includes the ethics deliverables is automatically generated and included in the Grant Agreement by the EC system, during the Grant Agreement Preparation (GAP) phase. That package, if applicable, will need to be added and submitted along with the grant agreement, as soon as the ethics review is completed, and it will be the last package in the list of WP. It is recommended to keep the ''ethics requirements'' WP at the end of the list as to not affect the numbering of the other work packages.

A detailed Gantt chart for the ATLANTIS project is provided in Figure 2-2:

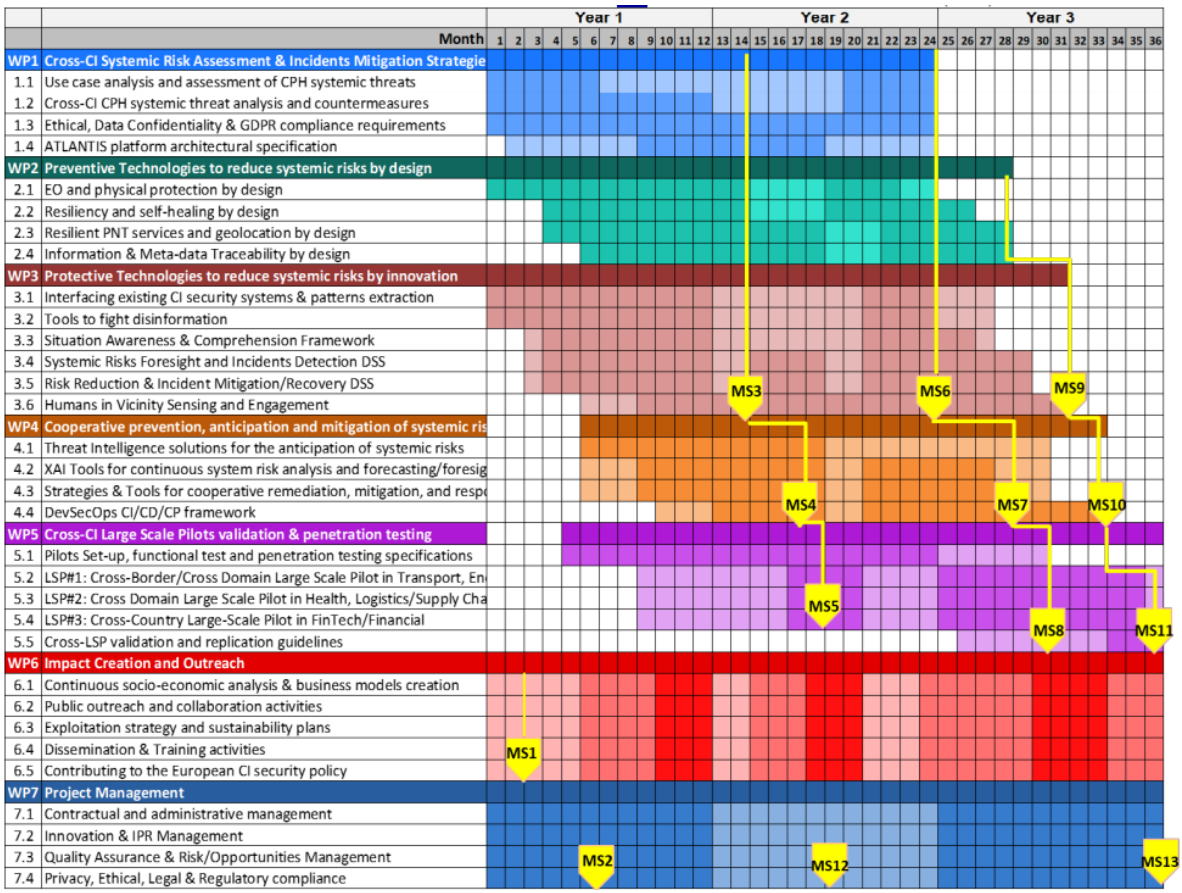


Figure 2-2 - ATLANTIS's Gantt chart

Moreover, a Pert Diagram is provided in Figure 2-3 - ATLANTIS's Pert Diagram and illustrates how all work packages contribute and impact to other work packages:

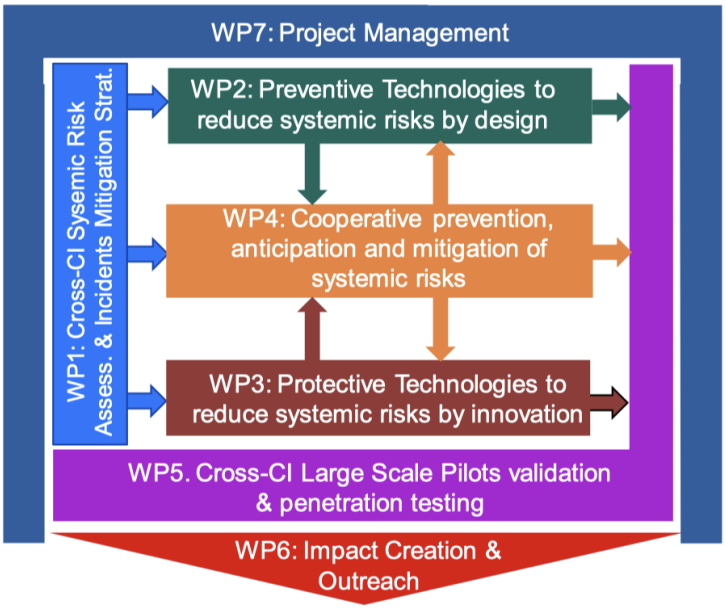


Figure 2-3 - ATLANTIS's Pert Diagram

2.2. Management Structure

European projects such as ATLANTIS are complex organisations which require collaboration between entities with different culture, approaches, and interests for achieving project's objectives. In order to be successful, a functional organisational structure must be in place that ensures efficient, result-driven management.

The different Management levels are described individually below in paragraph 2.3. The overall management of ATLANTIS project is based on the following points:

1) The *Organisational Structure* which defines the management structure in terms of **project governance** and **boards**.
2) Means of governance and control:
    a. The project *Description of Action (DoA)*, which describes the project objectives and expected results, the work plan in terms of WPs, tasks, deliverables, milestones, and finally the effort/cost distribution per WP/task and per partner.
    b. The *Consortium Agreement* (CA) and *Intellectual Property Right* (IPR) strategy in place, so that all partners of the consortium work collaboratively towards the achievement of common objectives. The CA defines the rules of collaboration among partners within ATLANTIS (roles, responsibilities and mutual obligations for the project life).
    c. The *Project Handbook* (this deliverable) defining in detail the structures, the procedures and the actors of the project, including also guidelines that should be followed for internal communication and to ensure high quality research, development and reporting. This document defines the procedures and standards for quality management and assurance of the project work and deliverables.
    d. The *Risk Management* plan included also in this report, defines a specific procedure for ensuring in time risk identification and mitigation actions.

e. The *Data Management* plan of the project will be defined in Deliverable D5.1 in M6 and in Deliverable D5.2 in M18 (final version) for ensuring a high level of data quality and accessibility for final users and stakeholders.

f. The *Periodic Report* including internal reporting, technical and financial reporting to the EC, and mid-term review & progress report where detailed reporting regarding project's progress will be demonstrated.

2.3. Project Management roles

ATLANTIS's management structure includes several *Roles* and *Bodies*.

2.3.1. General Assembly

The decision-making body of the consortium will be the **General Assembly**. It oversees the overall progress control and communication:

i. Ensuring that the consortium fulfils its contractual obligations.
ii. Ensuring the effective communication flow between partners of the Consortium and between the consortium and the European Commission.
iii. Planning and monitoring the overall progress and direction of the project, the performance and the accomplishment of the objectives.
iv. Identifying on time any upcoming risks of a delay or deviation from the Work Plan or resource allocation and requesting all necessary corrective actions from WP leaders.
v. Providing a mechanism for the prevention and resolution of disputes.
vi. Ensuring compliance with legal, contractual, ethical, financial and administrative regulations and self-assessment procedures, and
vii. Addressing partnership intercultural issues associated with team working, communications and management styles.

The project is coordinated, and its overall management guaranteed by the **Engineering Ingegneria Informatica S.p.A. (ENG)** which has exhibited an extensive experience in the management and implementation of research and innovation projects funded under national and European schemes, with several contracts with the European Commission and large industries.

The General Assembly is constituted by one representative from each partner. The members of the General Assembly will have sufficient seniority to take binding decisions without referring back to higher authority at their employing organisation. The General Assembly will meet twice a year, but extraordinary meetings will be convened any time required. Decisions in the General Assembly will ideally be made on the basis of consensus. If this is not possible, they will be made on the basis of a majority vote, with the Project Coordinator having the casting vote. Each partner has one vote.

In addition to the General Assembly, a **Project Steering Committee (PSC)** is established as part of the project management structure. It has the primary purpose to assist the General Assembly in fulfilling its oversight responsibilities on specific matters which are beyond the scope or expertise of non-technical members. The PSC consists of the Project Coordinator (PC), the Technical Manager (SM) and WP leaders (WPLs).

Table 2-3 reports the key personnel involved in ATLANTIS.

Table 2-3 - ATLANTIS's Key Personnel

Member	Role
Gabriele Giunta (ENG)	Project Coordinator and WP7 Leader
Artemis Voulkidis (SYN)	Technical Manager
Marco Gercke (CRI)	Data Controller
Theodoros Semertzidis (CERTH)	Dissemination Manager
Denis Caleta (ICS)	Communication Manager and WP6 leader
Véronique Beloulou (DMIA)	Security Policy Maker
Emilia Gugliandolo (ENG)	Exploitation Manager
Vasileios Ieronymakis (KEMEA)	WP1 Leader
Stamatia Rizou (SLG)	WP2 Leader
Carmela Stira (ENG)	WP3 Leader
DEDE Georgia (INTRA)	WP4 Leader
Emiliano Altobelli (FST)	WP5 Leader
Ioana Cristina Cotoi (ENG)	WP8 Leader

2.3.1.1. Project Coordinator

The **PC of ATLANTIS is Gabriele Giunta from ENG**. The PC is the key person in the assessment of the achievement of the objectives and risks within the project throughout its complete duration and in the implementation of contingency plans. Specifically, the PC is responsible for the following tasks:

i. Establishing and monitoring efficient communication flows within the Consortium.

ii. Monitoring the progress of the project according to work plan, time schedule and resources-budget established in the contract.

iii. Monitoring time and resource deviations from the original Work Plan and promote corrections.

iv. Resolving any potential conflicts within the project following the corrective mechanisms for conflict rectification as established in the Quality Assurance Plan.

v. Coordinating the bi-annual meetings of the General Assembly.

vi. Monitoring the quality of deliverables, together with the General Assembly and the WP leaders.

vii. Implementing contingency plans.

viii. Coordinating the consortium's representation at major meetings and publications of project results.

2.3.1.2. Technical Manager

The **Technical Manager of ATLANTIS is Artemis Voulkidis from SYN**. The role of the TM is to design and monitor the scientific directives in accordance with the objectives outlined in the Implementation Plan. TM is responsible for:

i. Ensuring that the project achieves its scientific objectives.

ii. Monitoring risks and adjusting manpower assignment, together with the PC and the WP leaders.

iii. Facilitating the information flow, collaboration effects between partners of the Consortium.

iv. Monitoring the quality of the deliverables from the scientific and technical point of view, together with the PC and the WP leaders.

v. Coordinating and leading cross disciplinary WP-meetings, and

The TM will work closely in matters of Quality Management and work planning in accordance with the Project Handbook (D1.1).

2.3.1.3. Data Controller

The ATLANTIS Data Controller is Marco Gercke from CRI. The concept of data controller and its interaction with the concept of data processor play a crucial role in the application of Directive 95/46/EC, since they determine who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate[1].

The data controller determines the purposes for which and the means by which personal data is processed. Therefore, who decides 'why' and 'how' the personal data should be processed is the data controller.

2.3.1.4. Dissemination Manager

The **Dissemination Manager of ATLANTIS is Theodoros Semertzidis from CERTH**. He is responsible for dissemination activities which include the project meetings, forums/workshops and conferences that will be organised for the dissemination of project results.

2.3.1.5. Communication Manager

The **Communication Manager of ATLANTIS is Denis Caleta from ICS**. He is responsible for the coordination of the project's collaboration, clustering and networking activities will be carried out for the communication of project results, as well as the relevant third-party events where the project partners will participate to represent ATLANTIS.

2.3.1.6. Security Advisory Board

Given the nature of the topic addressed by ATLANTIS, the Consortium has planned to establish a Security Advisory Board (SAB) to assess the security sensitivity of some of the project results. The ATLANTIS Consortium includes several partners that can bring the necessary expertise and experience to provide the resources needed to conform the SAB. The SAB will be an integral part of the project's management structure. The proposed initial members of the SAB are listed in the table below. All members have sufficient experience / knowledge of security issues related to the project activities. The responsibility of the SAB is to assess the emergence of sensitive information handled by participants and, in case, propose – if appropriate – corresponding measures for preventing misuse of such an information.

Security Advisory Board			
Member's name	**Nationality**	**Profession**	**Areas of competence**
Fabio Barba	Italy	Director of the Defence, Space	Fabio Barba is the Defense, Space and Homeland Security Business Unit

[1] Article 29 Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169)

		and Homeland Security Business Unit at ENGINEERING Ingegneria Informatica	Technical Director in Engineering. The Business Unit, inter alia, is responsible for the whole suite of EII's maritime awareness technologies. He concurrently fulfils the role of EII's Deputy Security Officer, being part of the organisation taking care of obligations deriving from the management of classified information. Before Engineering, he was an Italian Navy Officer; Fabio Barba graduated in Maritime and Naval Sciences at the Italian Naval Academy in 1995 and completed his education with an Engineering MSc in Command & Control Systems at the US Marine Corps University – Quantico, Virginia in 2000. He has 24 years of work experience including 14 in the ICT domain; furthermore, he has 10 years of exercise in complex projects
Denis Caleta	Slovenia	Associate Prof. and President of the Board at Institute for Corporative Security Studies	Denis Čaleta holds Ph. D. from Faculty of state and European studies, Slovenia in 2007. He is associate professor at Faculty of state and European studies and Faculty of Entrepreneurship/GEA College where he's a Head of Department for Management of Corporate Security. He's author of many scientific articles and books related to Critical Infrastructure Protection, Counter Terrorism and other security issues. He worked as a Slovenian representative in the framework of NATO in the field of intelligence standardization matters in "Joint Intelligence Working Group at the period 2002-2008. He served as an Adviser for Counter Terrorism to the CHOD of Slovenian Armed Forces at the period 2002-2010. He was also member of the Government Coordination Group to coordinate the preparations for critical infrastructure protection for more than 10 years and was representative of the Slovenian Armed Forces in the working body for transnational threats inside the

			National Security Council (NSC) primarily concern for Counter terrorism activities. He is national representative in EU RANNET (Radicalization Awareness Network).
Boris Kankaras	Slovenia	Director of Port Security at Luka Koper, Port and Logistic System	National security, data security, corporate security, counter terrorism expert. Over the last twenty years he has been appointed in the following roles: security management, risk management emergency and disaster Associated with document Ref. Ares(2022)6148556 - 06/09/2022 [101073909] [ATLANTIS] — Part B – [59] management, crisis management at Luka Koper; head of security service at the Ministry of Foreign Affairs; Advisor in Multinational Police Advisory Mission to Albania. Acting as Head of advisory team for CID, and Advisor to counter terrorism unit.
Michael Papadopoulos	Cyprus	Chief Technology Officer at NetU Consultants Ltd	Mr. Michael Papadopoulos is the Chief Technology Officer at NetU Consultants Ltd and has extensive experience and knowledge on enterprise information technology solutions. He has been working with public sector customers in Europe for more than 15 years, and has been involved in the architectural design, implementation and support of multiple mission critical systems. He is mainly involved with law enforcement and border control solutions, including European systems which requires handling of EU Classified Information, and regularly participates in project forums and industry round table discussions for European large-scale information systems in the area of freedom, security and justice.

2.3.2.Project Management Team

The PC, TM, DC, DM and CM will be supported by a **Project Management Team (PMT)** in the day-to-day research and technical coordination and for all administrative matters. PMT in ATLANTIS is recruited from ENG. It will be responsible for the following tasks:

i. Creation and maintenance of project communications mechanisms and business administration.
ii. Acting as interface between the EC and the Consortium.
iii. Monitoring of budget use by all partners.
iv. Receipt of all payments made by the consortium, and transfer of funds to consortium members according to the agreed budget.
v. Ensuring preparation, quality and timely submission of deliverables, reports, and cost statements.
vi. Coordination of all contractual issues: contract amendments, consortium Agreement, submission of audit certificates, etc.

2.3.3.Work Package Leaders

Each WP in the Work Plan is assigned a WP leader, who will have the following responsibilities:

i. Planning the scientific and technical work of the WP, in coordination with all partners that are involved in this WP.
ii. Ensuring that the time-schedule is maintained and indicate any discrepancies to the PC.
iii. Initiating corrective actions for project deviations (if required).
iv. Consolidating partner information and preparing the reports for submission to the PC.
v. Ensuring that the objectives and milestones of the whole WP as well as of the detailed activities within the WP are achieved in time.
vi. Ensuring that the deliverables are provided according to the time schedule.

2.3.4.Advisory Board

ATLANTIS will regularly interact with external stakeholders (i.e., CI actors outside the consortium) with a dual objective: (i) Obtaining feedback about findings from other channels (e.g., desk research findings); (ii) Soliciting additional information on policies, technologies, and standards. To collect such external feedback, the project will setup an external Advisory Board (AB) which includes CI operators from different sectors, as well as different CIP/CER experts from industrial organizations, research organizations and policy makers.

3. Collaboration, Communication and Dissemination Guidelines

An important key of success for the ATLANTIS project is to ensure a good communication among project partners and towards outside entities. A fast, reliable, and easily accessible collaboration and communication infrastructure is crucial for the proper operation within a large-scale pan-European project. This will be realised through the intensive use of electronic communications tools including emails, web-based exchanges, teleconferences etc. An operational environment where all partners can work together has been foreseen and provided to since M2 of the project. Moreover, a project web site will also be used to enable fast and efficient exchanges of information on the achieved results, such as publications, reports, workshops, and the main project activities and it will be accessible to the public.

3.1. Internal Communication and Collaboration

An efficient communication between partners is critical for successfully completing a project and therefore through ATLANTIS several tools have been adopted namely: the collaboration and communication Microsoft Teams along with emails and conference calls.

3.1.1. Guidelines for internal communication

The project has been launched by a plenary kick-off meeting held on 25th and 26th October 2022. The meeting has been the first opportunity to focus in detail on the work plan, to refine the common understanding of tasks and to build up an operational team spirit among partners. The communication flow between partners will be granted by using periodic videoconferences, Webex forums, teleconferences, mailing lists, collaborative web-based shared space (Wiki) and meetings of the General Assembly. ENG will be responsible for establishing and managing communication channels, especially mailing lists setting, for the consortium as a whole and for sub-groups working on particular tasks. In parallel to a number of consortium meetings, meetings for specific technical issues will take place. In order to closely monitor the work progress, the PC will organise monthly conference calls with the WP Leaders and TM in the context of the Project Steering Committee. Additionally, WP leaders should keep an updated list of actions, detailing the open issues of their WP, the severity of the task, the deadline (probably a new deadline if the task is for a reason postponed), the name or initials of the responsible assigned with the task, a small description and the issue status.

3.1.2. Project management and collaboration tools

The project management and collaboration tools will be implemented through the intensive use of electronic communication tools (e.g., email, web-based exchanges, file sharing, video-conference, etc.).

The main collaboration and project management tools used in the project are:

- Emails and project mailing list(s):
    - General project communications (i.e., all partners)
    - Possibility to create other dedicated mailing lists if needed (e.g WPs, administrative, ethics, etc.)

- Project people email directory spreadsheet.

- Audio/video conferencing tools: *Microsoft Teams*
- Internal web portal
  - Private (i.e., partners only) access
  - File-share and exchange with partners
  - Document library, official documents, work-page spaces
  - Additional online tools if needed (e.g., post, wiki)

3.1.2.1. E-mails and mailing lists

Direct e-mails will be used among project partners and several distributions/email lists will be created for efficiently managing communication. The members who participate in a mailing list should be able to send messages only to other list's members. Each person is responsible for the content of his/her message and its relevance to the purpose of the mailing list.

ATLANTIS has already set up different mailing lists, namely a consortium list, a mailing list for each WP and an administrative mailing list. The ATLANTIS mailing lists are the following:

- ATLANTIS-consortium@eng.it which contains all project partners
- ATLANTIS-wpx@eng.it where *x* defines the corresponding WP
  - ATLANTIS-wp1@eng.it
  - ATLANTIS-wp2@eng.it
  - ATLANTIS-wp3@eng.it
  - ATLANTIS-wp4@eng.it
  - ATLANTIS-wp5@eng.it
  - ATLANTIS-wp6@eng.it
  - ATLANTIS-wp7@eng.it
  - ATLANTIS-wp8@eng.it
- ATLANTIS-financials@eng.it which contains administrative members

A good communication recommends using mailing list only for topics of interest to all and to also reply / CC only to interested people. Moreover, it is important to update and use mailing lists spreadsheet (download, rename with organisation and data, modify, upload) in order to have all the updated email addresses. Moreover, for a clear communication, use clear subject lines in emails and always use the project acronym in subject lines (e.g., "[ATLANTIS]"). If needed, open or create a new "thread" (do not just reply to any email) but use same threads for related topic (possibly change subject line). Another recommendation is to propose short (online) call / meeting for fast action and to avoid 'never-ending' email discussions/arguments.

3.1.2.2. Conferencing tools

For the effective collaboration of partners regular conference calls are required. On ATLANTIS Microsoft Teams, it is possible to organise conference calls through the "Meet" functionality shown in the Figure:

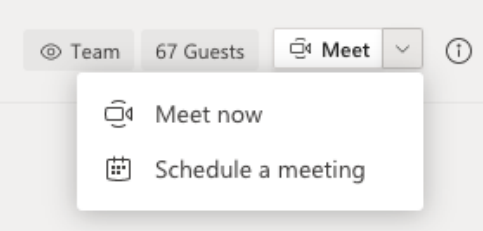


Figure 3-1 – ATLANTIS operational environment - "Meet" functionality

This functionality allows to launch an instant meeting or to schedule a meeting. Moreover, several tools are going to be used such as Skype, GoToMeeting; GoogleMeet etc. based on partners' preferences and availability.

The call organiser is responsible for:

- Creating an event for the call and notifying the participants on time.
- Providing the agenda of the event and any documents that may are relevant to the call.
- After the event has finished, the organiser should provide the meeting minutes using ATLANTIS's template, any shared documents or links to external sources.

3.1.2.3. ATLANTIS operational environment

An operational environment where all partners can work together has been foreseen and provided to since M2 of the project. The infrastructure chosen to hold the documentation produced by the project (interim reports, cost statements, working papers, and deliverables) has been based on Microsoft (MS) Teams. MS Teams (Figure 3-2) has been used as project collaborative and sharing tool and not only as Video/Audio Conference tool but as project repository.

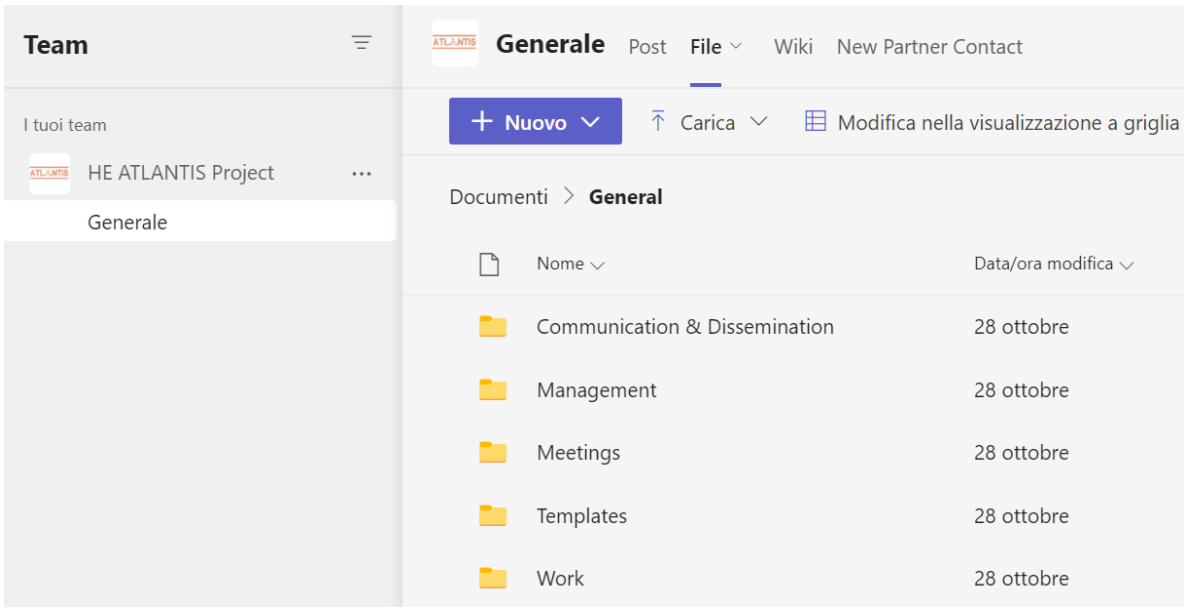


Figure 3-2 - ATLANTIS MS Teams

The ATLANTIS operational environment is dedicated to support all the project activities, related to both management and operational issues, like sharing documents, templates, work done etc. Moreover, this environment is also used for conference calls among the consortium members. The ATLANTIS Teams environment is essentially a central document repository for the project, used for internal communication and for interchanging documents, multimedia files, presentations etc. Moreover, it is possible to chat directly with

partners and to organise video/audio calls. In order to assure the proper confidentiality level of the hosted personal data (e.g., contact information such as full name and email address) project documentations (e.g., deliverables, presentations, minutes and so on) and credentials, a Data Policy has been prepared and shared with the consortium members (Annex I). Each member that needs to have access to the **ATLANTIS Team** has to accept the **Data Policy.**

By accessing to the ATLANTIS repository with an account, each member agrees to:

- Immediately notify the PC of any unauthorised use of password or username or any other breach of security.
- Exit from account at the end of each session.
- Defend, indemnify, and hold harmless the PC from any loss or damage arising from unauthorised use of password or username.

Each partner is responsible to notify the PC for any changes regarding project participants within their organisation in order to disable access to no longer participants or to give access to new ones. Each partner has received an email, asking to open a Microsoft Teams and to login using an already existing Microsoft account or to create a new one.
The workspace is managed by ENG and offers a collaborative working environment equipped by useful tools and functionalities to support collaboration and collective knowledge management within the consortium in all phases of the project. All ATLANTIS participants are granted access to the ATLANTIS Teams environment where they are able to:

- Start new discussions (**Post**), shown in Figure 3-3:

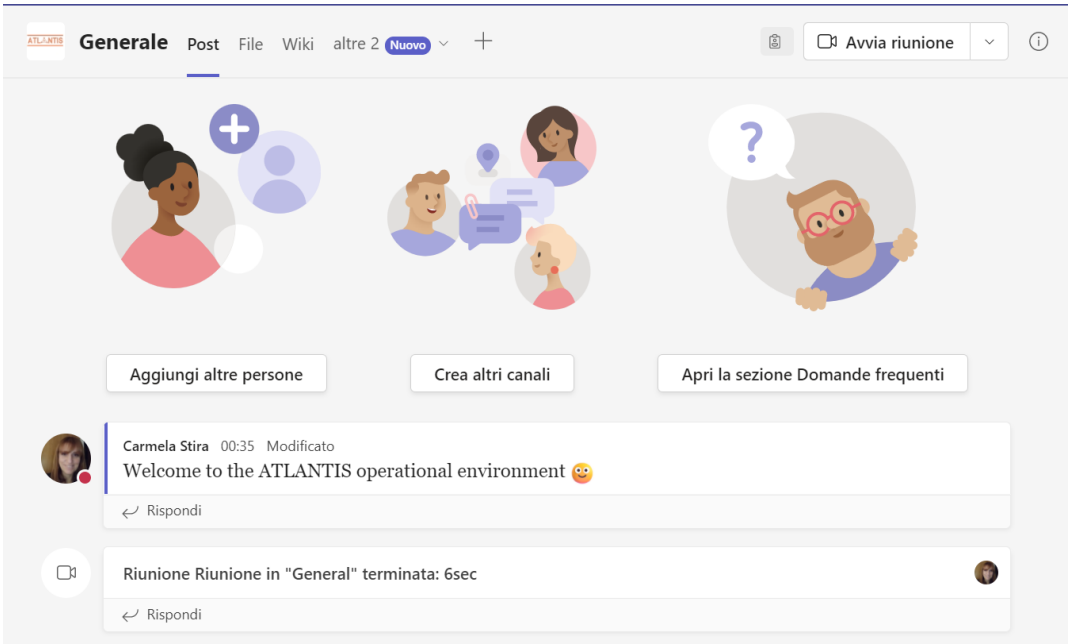


Figure 3-3 – ATLANTIS operational environment - New discussions

- See the project documents (**File**), shown in Figure 3-4:

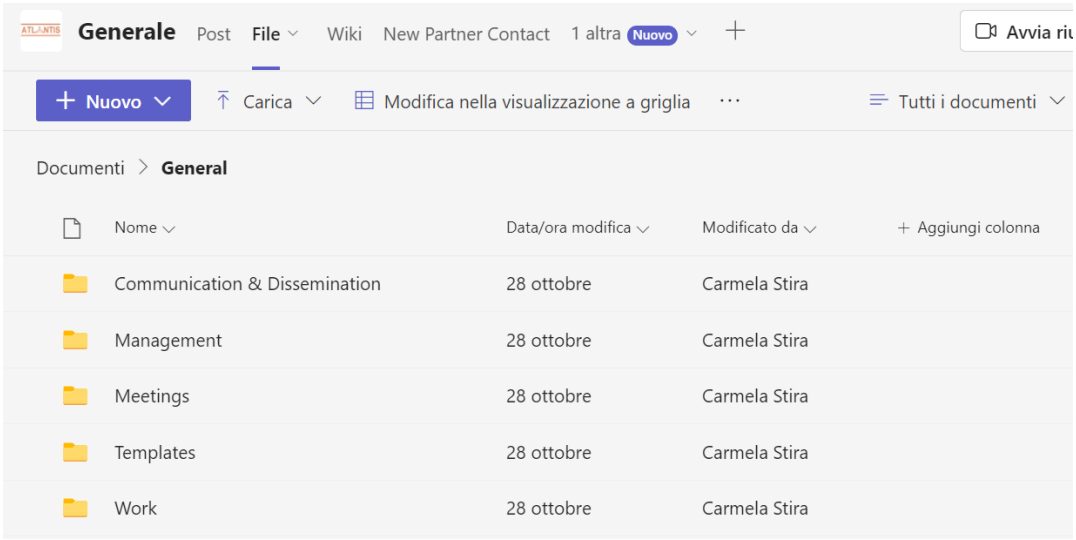


Figure 3-4 – ATLANTIS operational environment – Document Server

- Create new wiki pages (**Wiki**), shown in Figure 3-5:

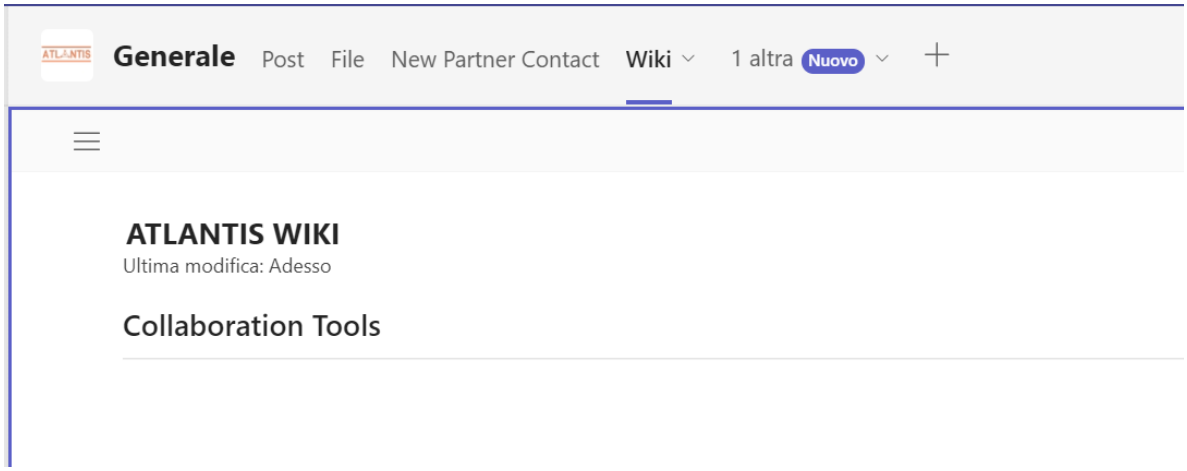


Figure 3-5 – ATLANTIS operational environment – create new wiki

- Schedule a Meeting (**Meet**), shown in Figure 3-6:

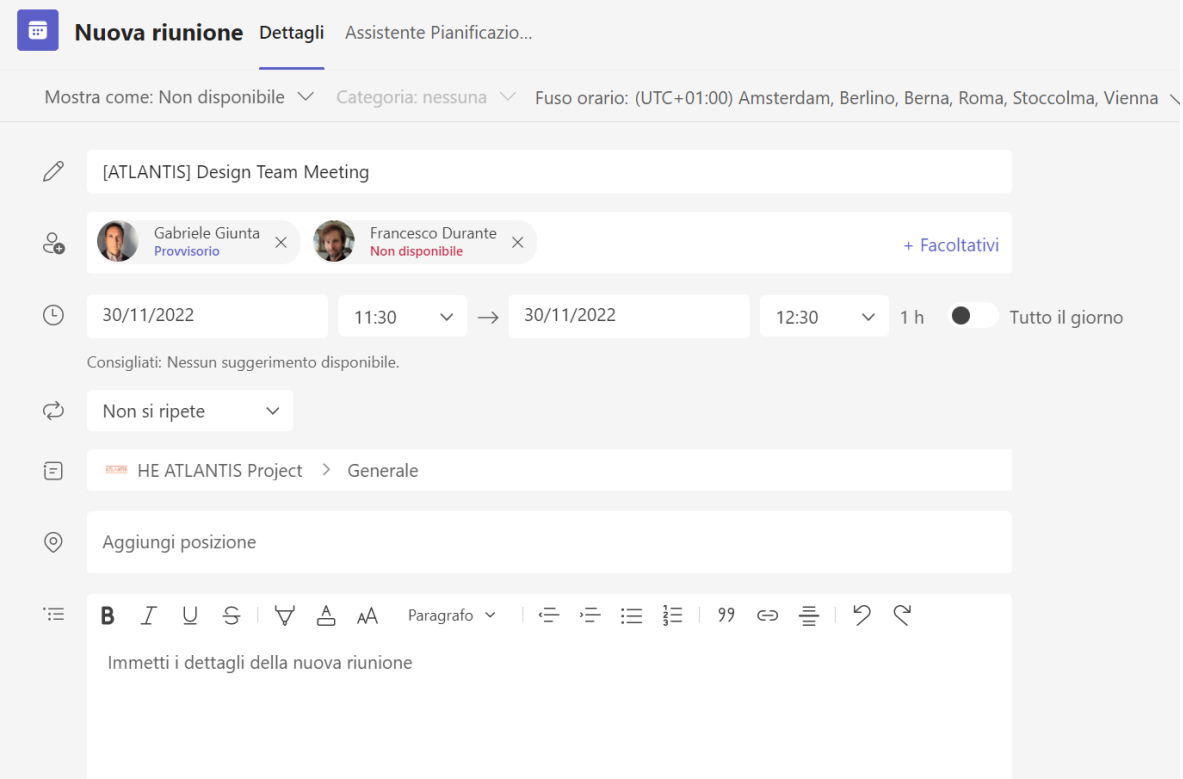


Figure 3-6 – ATLANTIS operational environment – Schedule a meeting

The content of ATLANTIS Teams environment is regularly updated, and contributions are made by all project partners who have been provided with an account, while a strong commitment is expected mainly from WP leaders and from communication manager as well as from the project coordinator and by the technical manager.

3.2. External Communication

The communication strategy to reach external audiences is described in *D6.5 – Dissemination & Standardization & Communities Liaison* (due at M6). The deliverable will specify the target stakeholders and the concrete channels and activities that will be used to target them. It provides the partners with the necessary processes and tools to facilitate the effective communication of the project information to its target audiences and an effective dissemination of its results.

An updated version of the dissemination and communication strategy will be provided at M18 as *D6.6 - Dissemination & Standardization & Communities Liaison v2*.

The online promotion of the project and dissemination of its results will be done via two main channels: a) the ATLANTIS website, and b) the ATLANTIS LinkedIn page.

3.2.1. ATLANTIS Website

The communication outside the ATLANTIS consortium, will be mainly performed by the public ATLANTIS website (Figure 3-7).

The ATLANTIS website (https://www.atlantis-horizon.eu/) – developed by CERTH and that will be released in M2 – will serve as the main source of up-to-date information about the activities and outputs of the project. It will be regularly updated by CERTH with input by all project partners and its traffic will be monitored using Google Analytics. The website

is the main means of communication of the project with external stakeholders. The website contains the project overview (Figure 3-8) and detailed information about ATLANTIS Consortium, Reports & Publications, Media, news and events and contacts.

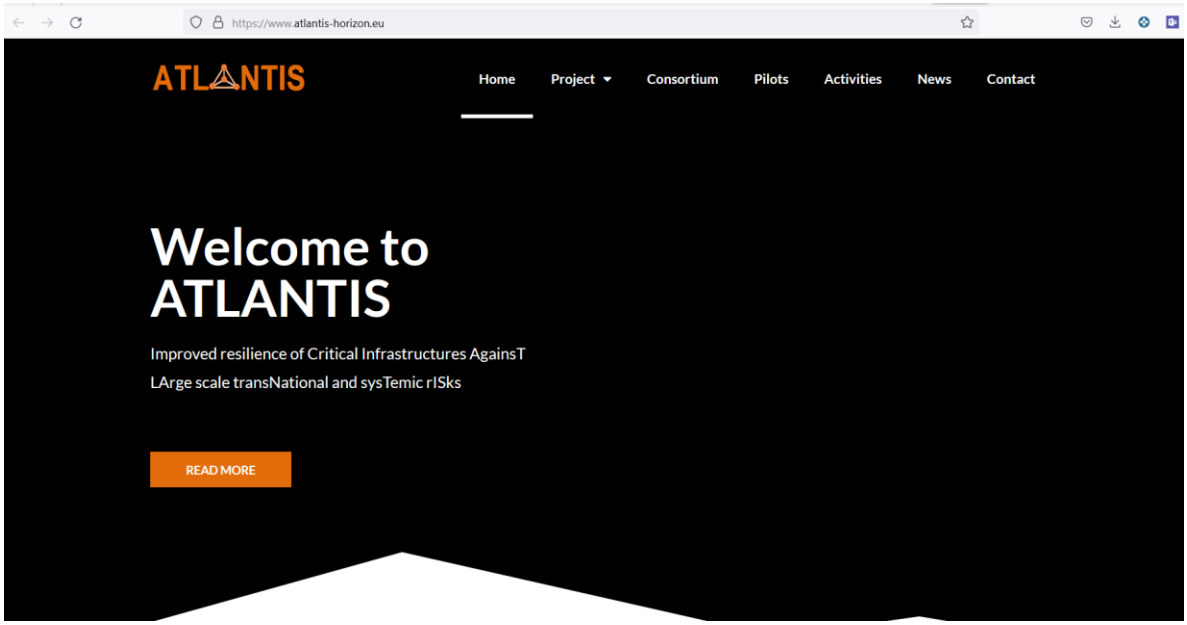


Figure 3-7 – ATLANTIS Website

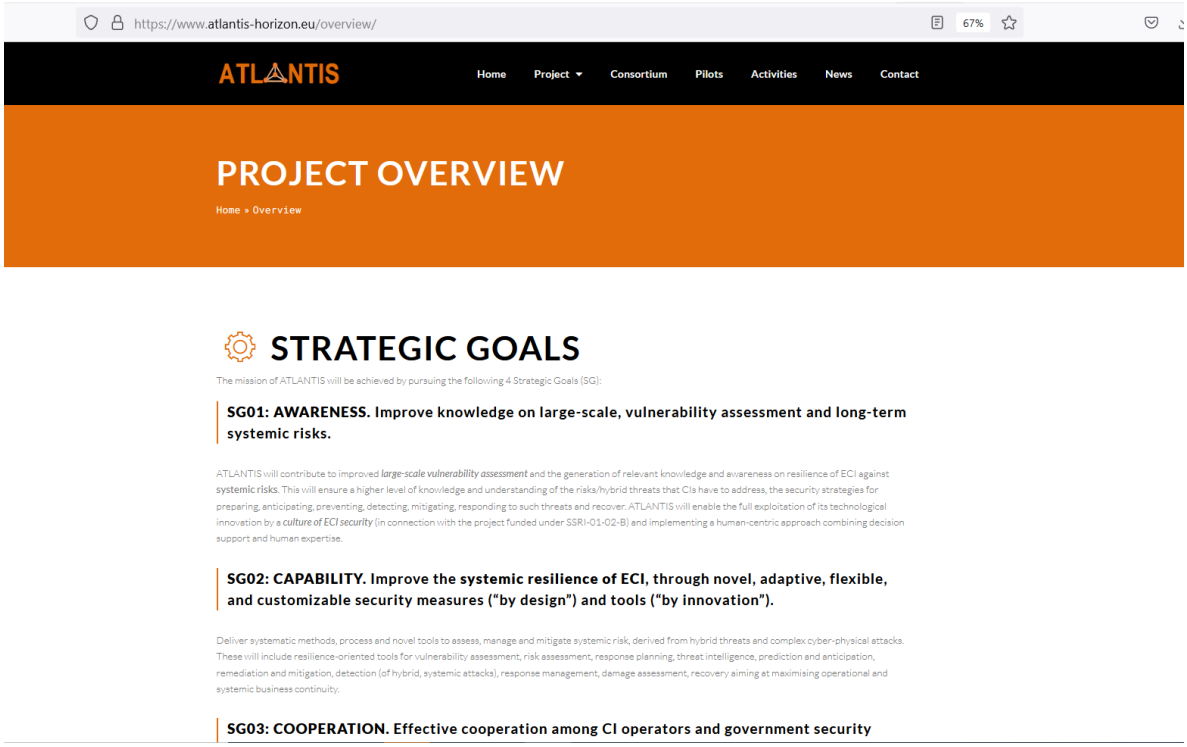


Figure 3-8 – ATLANTIS Website Project Overview

Any news relevant to the project will be reported on the website throughout the duration of the project.

3.2.2.ATLANTIS in Social Media

For disseminating ATLANTIS's results and maintaining its awareness, regular posts will be made on ATLANTIS LinkedIn page (https://www.linkedin.com/in/ATLANTIS-

750b31254/) shown in Figure 3-9. These pages have been set up and will be maintained by CERTH with regular inputs from all partners.

Figure 3-9 – ATLANTIS LinkedIn page

More details about the ATLANTIS Social Media presence will be given in *D6.5 – Dissemination & Standardization & Communities Liaison*.

3.2.3.ATLANTIS publication and papers

If a partner wants to submit a scientific publication describing a part of work performed within the project, the partner should inform the PC, the TM, the DM, the CM, the SAB as well as the consortium partners **30 calendar days** before the final submission. Any objection from the consortium to the publication to be submitted should be made in accordance with the Grant Agreement in writing to the Project Coordinator and to dissemination Leader **within 15 calendar days** after receiving the notice. If no objection is declared within the aforementioned time limit, the publication is permitted. Any justified objection should be accompanied by specific request for the necessary amendments. The involved parties should discuss how to overcome the issues which drove to the objection on a timely basis (for example by amendment to the planned publication and/or by protecting information before publication) and the objecting partner shall not unreasonably continue the opposition if actions have been performed following the discussion. The objecting Party can request a publication delay of **not more than 90 calendar days** from the time it raises such an objection. After 90 calendar days the publication is permitted.

4. Monitoring and Reporting Guidelines

The infrastructure chosen to hold the documentation produced by the project (reports, working papers, templates and deliverables) will be based on the online MS Teams used as a collaboration and communication tool.

The following kinds of libraries are kept on the MS Teams:

- Management: All the official documents, submitted deliverables, financial sheets, internal review information.
- Meetings: All the information and presentations done during a meeting or a teleconference.
- Templates: The deliverables template and ppt presentation.
- Work Files: All WP documentation including deliverables, internal documents, bibliography and so on.

4.1. Project Deliverables

The project will deliver a comprehensive package of deliverables alongside the developed tools and the overall system.

The PC has to monitor the quality of deliverables, together with the General Assembly and the WP leaders. The PMT has to ensure the preparation, quality and timely submission of deliverables, reports, and cost statements while each WP Leader is responsible for the organisation of the deliverables within his/her WP and their on-time submission. The external AB act as consultants on scientific and exploitation issues, follow up the production of different outputs and deliverables.

The SAB shall ensure the proper handling of sensitive information and review all deliverables and publications prior to dissemination.

Particular emphasis will be put on quality control of deliverables. The **deliverable Quality Assurance process** foresees that:

- Each deliverable will be reviewed by **2 internal reviewers** (IR) appointed by the PC and approved by the General Assembly.
- Normally internal reviewers are partners external to the WP or at least not initially involved in the writing process.
- To optimise work ahead of time, a **project-wise review plan** containing the internal peer reviewers for each deliverable has been proposed and shared with all partners.
- An ethics and security check will be done by DC and SAB members.
- A last quality check will be done by the PC.

4.1.1. Identification of deliverables

The deliverables are listed in the following Table 4-1 by WP and due date.

DE No	DE Name	WP No	Lead Beneficiary	Type	Dissemination Level	Due Date
D1.1	Cross-CI Risk Assessment and GD compliance	WP1	25 - KEMEA	R — Document, report	R-UE/EU-R - EU Classified	M6
D1.2	ATLANTIS meta-architecture countermeasures definition	WP1	8 - SYN	R — Document, report	SEN - Sensitive	M12
D1.3	ATLANTIS meta-architecture countermeasures definition v2	WP1	8 - SYN	R — Document, report	SEN - Sensitive	M24
D2.1	Physical Preventive measures	WP2	3 - RESA	R — Document, report	R-UE/EU-R - EU Classified	M10
D2.2	Physical Preventive measures v2	WP2	3 - RESA	R — Document, report	R-UE/EU-R - EU Classified	M19
D2.3	Cyber Preventive measures	WP2	2 - CS	R — Document, report	R-UE/EU-R - EU Classified	M11
D2.4	Cyber Preventive measures v2	WP2	2 - CS	R — Document, report	R-UE/EU-R - EU Classified	M20
D3.1	Systemic Risks and Incidents Awareness	WP3	1 - ENG	R — Document, report	SEN - Sensitive	M14
D3.2	Systemic Risks and Incidents Awareness (alpha version)	WP3	1 - ENG	OTHER	SEN - Sensitive	M24
D3.3	Systemic Risks and Incidents Awareness (beta version)	WP3	1 - ENG	OTHER	SEN - Sensitive	M30
D3.4	Incidents Mitigation by Innovation	WP3	7 - SIEM	R — Document, report	SEN - Sensitive	M16
D3.5	Incidents Mitigation by Innovation (alpha version)	WP3	7 - SIEM	OTHER	SEN - Sensitive	M26
D3.6	Incidents Mitigation by Innovation (beta version)	WP3	7 - SIEM	OTHER	SEN - Sensitive	M31
D4.1	CCI-SAAM Coordinated Framework	WP4	4 - INTRA	R — Document, report	SEN - Sensitive	M16
D4.2	CCI-SAAM Coordinated Framework (alpha version)	WP4	4 - INTRA	OTHER	SEN - Sensitive	M26
D4.3	CCI-SAAM Coordinated	WP4	4 - INTRA	OTHER	SEN - Sensitive	M32

	Framework (beta version)					
D4.4	ATLANTIS Integrated Framework	WP4	10 - BYTE	R — Document, report	SEN - Sensitive	M17
D4.5	ATLANTIS Integrated Framework (alpha version)	WP4	10 - BYTE	OTHER	SEN - Sensitive	M28
D4.6	ATLANTIS Integrated Framework (beta version)	WP4	10 - BYTE	OTHER	SEN - Sensitive	M33
D5.1	LSP set-up and Data Management Plan (DMP) (initial version)	WP5	13 - CRI	R — Document, report	R-UE/EU-R - EU Classified	M6
D5.2	LSP set-up and Data Management Plan (DMP) (final version)	WP5	13 - CRI	DMP — Data Management Plan	R-UE/EU-R - EU Classified	M18
D5.3	LSP use cases evaluation results	WP5	19 - FST	R — Document, report	R-UE/EU-R - EU Classified	M30
D5.4	LSP use cases evaluation results v2	WP5	19 - FST	DATA — data sets, microdata, etc.	R-UE/EU-R - EU Classified	M36
D6.1	Project Web site & Social Channels	WP6	31 - CERTH	DEC — Websites, patent filings, videos, etc	SEN - Sensitive	M2
D6.2	Market study and exploitation plans (initial version)	WP6	1 - ENG	R — Document, report	SEN - Sensitive	M6
D6.3	Market study and exploitation plans (intermediate version)	WP6	1 - ENG	R — Document, report	SEN - Sensitive	M18
D6.4	Market study and exploitation plans (final version)	WP6	1 - ENG	R — Document, report	SEN - Sensitive	M36
D6.5	Dissemination & Standardization & Communities Liaison	WP6	26 - ICS	R — Document, report	PU - Public	M6
D6.6	Dissemination & Standardization & Communities Liaison v2	WP6	26 - ICS	R — Document, report	PU - Public	M18
D6.7	Dissemination & Standardization & Communities Liaison v3	WP6	26 - ICS	R — Document, report	PU - Public	M36
D7.1	Project Handbook	WP7	1 - ENG	R — Document, report	PU - Public	M2
D8.1	POPD - Requirement No. 1	WP8	1 - ENG	ETHICS	SEN - Sensitive	M6
D8.2	AI - Requirement No. 2	WP8	1 - ENG	ETHICS	SEN - Sensitive	M8

4.1.1.1. Deliverables Naming – File Naming Conventions

All of the deliverables follow the file naming convention presented below:

- All filenames will start with the project name i.e., ATLANTIS
- This will be followed by the deliverable code/number as part the DoA e.g., D7.1 for the present deliverable.
- The title of the deliverable should be accordingly included in Title Case i.e., in a from where all words are capitalized, except non-initial articles like "a, the, and". Moreover, the words will be separated using underscores e.g., Project_Handbook. Please not that Underscore (_) is the preferred separator of all fields.
- The revision number will then be included, including a major release version and a minor version used in the deliverable's preparation stage only.

As an example, in the title ATLANTIS_D7.1_[Title]_vA.B_[DE responsible], A is used to indicate a major release versioning, while B is updated during the preparation phase. According to this convention:

- *ATLANTIS_D7.1_Project_Handbook_v1.0_ENG* is the version for submission to the EC.
- *ATLANTIS_D7.1_ Project_Handbook_v2.0_ENG* is the second major release of the deliverable (e.g., a revised/updated version after comments from EC experts).
- *ATLANTIS_D7.1_Project_Handbook_v0.1_ENG* indicates a version for internal updates and submission for internal review, towards producing a version for submission.

The partner that initiated and has the responsibility for the document will have the authority to change the version number. In case a partner aims to send comments on the document, track changes can be used, adding the partner's acronym at the end.

- *ATLANTIS_D7.1_ Project_Handbook_v0.1_ENG_SYN*

After each internal iteration and when the deliverable is finalised, the responsible partner (editor) has the authority to increment the version number and date of the document.

4.1.1.2. Template for deliverables

There is an official template for the deliverables according to their dissemination level (Sensitive and Public Deliverables).

The official project deliverables should have a first page as for the reference/template in Annex I. Furthermore, they should comply with the following rules:

- Have a document revision history table
- Have a document quality control table
- Have the Disclaimer
- Have a Table of Contents
- Have a list of Figures, if relevant
- Have a list of Tables, if relevant
- Have a list of definitions and acronyms used within the deliverable
- Start with one-page max Executive Summary

- End the main part with a Conclusions and future outlook section
- Include a References section after the Conclusions section and an Annex if relevant

4.1.1.3. Abbreviations and Acronyms

Each deliverable must provide a complete list of the abbreviations and acronyms used in the document. Acronyms must be explained (i.e., spelled out) in the first instance of their introduction and use in the deliverable. Accordingly, authors can use the acronyms inside the deliverable text. However, it is advised to avoid excessive use of abbreviations in order to boost readability. In this direction, terms and acronyms commonly used in Critical Infrastructure (CI) should be primarily abbreviated, while the excessive use of non-standards and less common acronyms should be avoided.

The deliverable leader may also opt to define terms in a dedicated terminology section. This is very important, to avoid misinterpretation of technical and security terms, which can lead to lower document quality.

4.1.1.4. Files and Archives

The "submitted" versions of the project deliverables classified as "SEN" and "PU" are centrally stored for download on the project web repository. Public deliverables produced in the frame of ATLANTIS work programme are available for download also in the project website in the section devoted to "Deliverables".

4.1.2. Deliverable Production and Review

4.1.2.1. Deliverables Production Timeline

Each project deliverable is assigned to one leading responsible partner. Therefore, the partner is responsible for the deliverable's quality and on time submission. The partner is responsible to ensure that the content of the deliverable is consistent with the team-workings of the deliverable and that the particular objectives related to the goals of the project are met. Any issues related to the deliverables, putting at risk the work package or the whole project must be reported immediately to the Project Coordinator and to the WP Leader.

Project deliverables will be reviewed against the below criteria:

- Clarity of the document analysis and conclusions.
- Overall suitability and originality of the document.
- Conflict of interests, suspicion of duplicate publication, fabrication of data or plagiarism.

In particular, a formal document "Review Form" as approval for the evaluation process has been used and attached in the Annex I.

The following Table 4-2 depicts all the steps involved in deliverable production.

Table 4-2 - ATLANTIS deliverable production steps

Steps	When (days to DE deadline)	Who	What
1	60	DE Leader	Publish ToC with assignments proposal

2	58	PC, TM	Review the ToC and Provide Comments and Suggestions
3	55	All DE partners	Final ToC with Chapter Editors
4	45	Chapter Editors	[Assign and collect sub-sections' input] (if needed) Send 1st integrated version to DE Leader
5	43	DE Leader	Integrate all chapter inputs and release new version
6	42	All	Agree on DE progress, input if needed, next steps
7-8-9	35-26-25		*Repeat 4 – 5 - 6 if needed*
10	26	DE Leader	Integrate and circulate pre-final version
11	23	Chapter Editors	Final input to DE Leader
12	15	DE Leader	Release pre-final to internal and security/ethics reviewers
13	12	Int./Sec/Eth. Reviewers	Provide review / security/ethics approval
14	7	PC and TM	Review, approval and release final version
15	1	PC	Approves, Final version freeze and submission to EC

4.1.2.2. Deliverables Review Checklist

Table 4-3 presents some of the main Aspects that each quality reviewer should check, beyond the provision of comments on the content of the deliverable and suggestions for improvement.

Table 4-3- ATLANTIS deliverable Quality Review Checklist

List of Quality Review Checks	Check
Deliverable follows the project's templates	☐
Headers and footers of the document are appropriately modified	☐
Contributing Partners are properly highlighted and in-line with the DoA	☐
A proper **Revision History** is included	☐
The list of Acronyms and **Abbreviations** is completed	☐
The Executive Summary provides a comprehensive summary of the document, while presenting the role of the document in the project's workplan	☐
The table of contents, the table of figures, the table of table and other references are properly updated	☐

The content of the document is in-line with the expectations described in DoA, as well as with the type of the deliverable (e.g., report, ethics, DMP)	☐
The document is properly structured and formatting i.e., it has a structured and no formatting flaws	☐
Tables, Figures and Codes contain properly numbered **captions** and apt descriptions	☐
The deliverable includes a "Conclusions" section	☐
In case the document is built incrementally over a previous version, it must clearly outline the changes, enhancements and improvements over the previous version	☐
References follow the same style and are properly cited in the text	☐
The **document follows** the **Naming Conventions of ATLANTIS**	☐
The PDF of the document is properly generated	☐

4.2 Project Monitoring and Reporting

The project will prepare periodic progress reports as required by the EC. As these documents may contain financial or other sensitive information, they as a whole will not be made public.

4.2.1 EC Reporting and Monitoring

Within ATLANTIS there are two reporting periods:

- Reporting Period 1 (RP1) from month 1 to month 18,
- Reporting Periods 2 (RP2) from month 19 to month 36.

These two periodic project reports M18 and M36 include both technical and financial reporting. Moreover, two technical Review Meetings will be scheduled after each reporting period (M18 and M36). The EC Project Officer, the EC appointed expert reviewers and all the partners will participate to these meetings. The EC will assess the project progress and results as well as the resource consumption.

The EC Reporting details are shown in Figure 4-1:

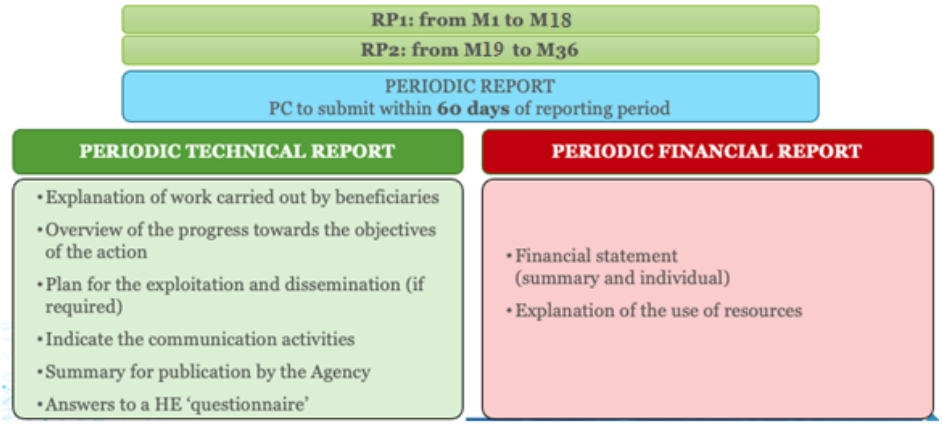


Figure 4-1 – ATLANTIS EC Reporting details

4.2.2 Internal Progress Reporting

In addition to the EC Reporting and Monitoring, an internal progress reporting mechanism will be set up.

This reporting mechanism is described below:

- Every six months, each WP Leader is responsible for writing an internal progress report and sending it to the PC and TM. In this report WP Leader will collect contributions from all the involved partners, describing the progress of activities per WP and effort spent per task in the reporting period. The template for internal progress report will be shared with all the partners.

4.1. Conflict Resolution and Issues Management

All ATLANTIS participants should be aware of their commitment. Nevertheless, unpredictable situations, possible conflicts or issues could occur and affect the project activities and as consequence delay the submission of deliverables. Conflicts will be resolved by a procedure detailed in the Consortium Agreement.

Potential conflicts will be identified and brought to the immediate attention of the PC by the appropriate Local Project Manager or WP leader. The PC will attempt to resolve this by discussion or by calling an ad-hoc meeting. In this situation, it is recommended to try to resolve at lowest level and ease agile resolution according to this flow: **TL → WPL → PC → GENERAL ASSEMBLY → CA**. An escalation has to be executed only if needed (better to make use of negotiation skills).

If that fails, the PC can organise extraordinary General Assembly meetings and seek a decision by majority vote of the General Assembly. These meetings can be organised also remotely (e.g., audio conference) and an email voting is allowed (according to CA rules).

In case of non-performance of any of the partners, the PC shall have the power to exclude the offending partner by a vote of unanimity minus one. In such circumstances, the provisions of the Grant Agreement guidelines will apply as well as relevant non-conflicting provisions. Any conflicts that cannot be resolved through the principles above will be handled according to the dispute resolution provisions made in the CA. However, before using these procedures, the ATLANTIS beneficiaries will make the largest possible use of their proven negotiation skills.

5 Procedures for Project Meeting

The ATLANTIS project kick-off meeting represented the effective start of the project operations in which presentations for each WP and each tool has been made followed by discussions between end-users and technical partners. The meeting has been the first opportunity to focus in detail on the work plan, to refine the common understanding of tasks and to build up an operational team spirit among partners.

5.2 Project Meeting

Project meetings are set periodically, or exceptionally at different levels if it is needed. The different types of meetings that have been foreseen for ATLANTIS follow:

1. **General Assembly meetings**: one representative per partner and relevant people needed are expected to participate in the periodic General Assembly meetings alongside key members of the consortium (PC, Quality & Risk Manager + Ethical & Legal Manager + Dissemination & Communication Manager). General Assembly meetings are generally planned every 6 months, in person or remotely.
2. **PSC meetings**: The PC could arrange remote meetings (focused in- person only if really needed) every month for the efficient coordination of the project. PC, TM and WP leaders are expected to participate. These are regular meetings, and a fixed date will be chosen by all the participants. PC is responsible for notifying the participants the meeting and report meeting minutes. PSC meetings are generally planned every month and whenever required.
3. **Review meetings**: review meetings will be scheduled in correspondence of the EC's review process. Review meetings have been scheduled to occur for the Mid-review and the Final review in month 19 and in month 36 respectively. Albeit they can be changed in accordance with EC Project Officer. Project Officer (PO), EC's nominated expert reviewers and all partners (at least one representative per partner mandatory) are expected to participate. Such meetings could include some additional preparation days before the review day for finalising demonstrations preparation, the agenda and presentations. These meetings are in person or remote ones.

5.3 Meeting Procedures

The meeting's organiser that could be PC, TM or WP Leader, depending on the specific meeting, is responsible for:

- Creating the new event for the meeting and invite the involved people at least 40 calendar days before for in-person meetings and at least 10 calendar days before for remote meetings.
- Providing the agenda of the meeting as well as documents that may be required for partners to prepare for the meeting, uploading them in the project internal portal and linked in invitation at least 18 days before for in-person meetings and at least 5 days before for remote meetings. The agenda editing is allowed to any invited participant at least 14 days before for in-person meetings and at least 2 days before for remote meetings.
- Once the meeting is finished, the organiser should take the meeting minute providing information about the participants, action points and topics discussed. The document should be circulated to partners and be uploaded to ATLANTIS repository within 10 calendar days from the meeting end. The minutes shall be considered as accepted if,

within 15 calendar days from sending, no Member has sent an objection with respect to the accuracy of the draft of the minutes.

On the other hand, each partner of ATLANTIS:

- Should be present at any meeting with at least one representative.
- May appoint a substitute to attend and vote at the meeting.
- Should actively participate in a cooperative and fruitful manner in the meetings.

The template for the meeting minutes is available in project's repository.

6 Quality and Risks Management

As a fundamental part of the project management activities, the Quality Management provides the basis for successful, timely and quality implementation of the project activities. It is in line with common standards to be applied and followed throughout the entire project lifetime, as compliance with all relevant rules and provisions is very complex and comprehensive task.

Taken together, Risk Management and Quality Management have interdependencies necessary to guarantee successful project results. Defining risks and establishing policies and procedures to address risks are therefore necessary to proactively respond to any challenge that could negatively impact the overall quality of the project. Risks are defined as potential variations which would have a negative impact on the project, be it a decrease in quality, increase in cost, delay in completion or even a failure of the project.

The quality methodologies and procedures applied will be in line with ISO 9001 requirements. The ISO 9001 requirements provide a set of standard elements that guide the implementation of a Quality Management System (QMS). The requirements are designed to be generally applicable and as such they identify which elements are mandatory in a QMS, but not how these are implemented. The ISO 9001 requirements are broadly separated into eight sections (called ISO 9001 clauses), five of which contain mandatory requirements for a QMS: general Quality Management System requirements (clause 4), Management Responsibility (clause 5), Resource Management (clause 6), Product Realisation (clause 7), and Measurement, Analysis and Improvement (clause 8). All elements of these five clauses are mandatory, with the exception of the Product Realisation part.

6.2 Quality Management System

The project quality management system aims to ensure that ATLANTIS will achieve the expected results in the most efficient way and that the deliverables will be accepted by the EC. Towards this end, quality methodologies and procedures are established giving guidelines to be adopted by project partners on preparation and validation of the deliverables, internal peer reviewing, preparation of financial statements, periodic reporting and risk management. To guarantee a high quality of all activities carried out in the context of a project of the scale and complexity of ATLANTIS, quality management procedures are essential. Quality management procedures will be applied to all activities and will be the joint responsibility of all partners until complete discharge of their obligations under the EC contract. The main goals of the Quality Management procedures are:

- The establishment of documentation, reporting and communication procedures;
- The production of high-quality deliverables on time and according to specifications;
- The identification of technical and commercial risks, or deviations at an early stage;
- The realisation of any necessary remedial actions as soon as possible.

The PC and the PMT will be responsible for the Quality Management applied in daily and overall project management and quality control by all project partners, responsible for preparing and producing deliverables. Quality Management documentation will be maintained during the project lifetime and will be accessible for the partners through the ATLANTIS operational environment (§3.1.2.3). Quality in an EC-funded project, such as ATLANTIS, should be addressed not only in deliverables and reporting but also in prototypes, demonstrations and for the project process itself.

The Quality Management is fundamental for all work undertaken by ATLANTIS project and should be implemented by all partners in their work. To that effect, ATLANTIS will:

- Maintain consistency in work method throughout in accordance with set policies, procedures, regulations and codes of practice and without significant deviation.
- Ensure that all policies, procedures, relevant regulations and codes of practice are implemented and systematically reviewed to reflect quality's values.
- Regularly monitor and measure the quality of its work methods, outputs and outcomes with a view to ensuring high quality standards, best value and continuous improvement.

The Quality Management is based on the following main objectives:

- Process quality assurance: this type of quality assurance activities aims to ensure that all processes and related tasks defined in project plans are performed as described.
- Product quality assurance: This type of quality assurance activities is carried out in order to assure that all project's deliverables are drafted, verified, approved and issued following the process described in the section 4 and, at the same time, that the content of the deliverables are aligned with expected outputs and requirements as defined in Section 4.1.

6.3 Process Quality Assurance

These activities are carried out by the PC and aim to ensure that project activities are carried out in line with processes defined for the overall project lifetime and to identify any deviation between what is implemented and what has been agreed. In case of discrepancies from the defined processes, it will be evaluated if process improvement opportunities are possible.

The quality surveillance is a continuous activity performed by monitoring the project's process workflow in terms of:

- Internal team communication
- Deliverables and Documentation handling
- Project progress review

These types of controls are performed through witnessing and observation of project milestones and project meetings. For each of them, different quality controls are applicable as presented in the following sections.

6.3.1 Project Milestones and Quality Controls

Exhaustive quality assessment of the work in progress will be undertaken upon completion of the Milestones MS1-MS13. The *Means of Verification* are presented in Table 6-1 for each type of milestone:

Table 6-1 – ATLANTIS Milestones Quality Controls

Milestone	Name	Due Date (months)	Means of Verification
MS1	Project Web site & Social Channels establishment	2	D6.1
MS2	1st Advisory Board meeting organized	6	D6.2, D6.5
MS3	ATLANTIS Components (Alpha Version)	14	D1.1, D1.2, D2.1, D2.3, D3.1

MS4	ATLANTIS Integrated (Alpha Version)	17	D4.1, D4.4
MS5	ATLANTIS Initial Validation @ LSPs	18	D5.2
MS6	ATLANTIS Components (Beta Version)	24	D1.3, D2.4, D3.2
MS7	ATLANTIS Integrated (Beta Version)	28	D4.2, D4.5
MS8	ATLANTIS Intermediate Validation @ LSPs	30	D5.3
MS9	ATLANTIS Components (Version 1.0)	31	D2.4, D3.6
MS10	ATLANTIS Integrated (Version 1.0)	33	D4.3, D4.6
MS11	ATLANTIS Final Validation	36	D5.4
MS12	First project Review	18	Review Report
MS13	Final project Review	36	Review Report

The results of the assessment and any necessary actions that need to be taken will be outlined in the corresponding evaluation reports. In between project milestones, dedicated progress meeting and/or mid-term checkpoints will be identified and reported in the project management documentation.

6.3.2 Project Reporting and Quality Controls

Within ATLANTIS the project reporting is related to EC Reporting and Monitoring and Internal Progress Report as shown in Figure 6-1:

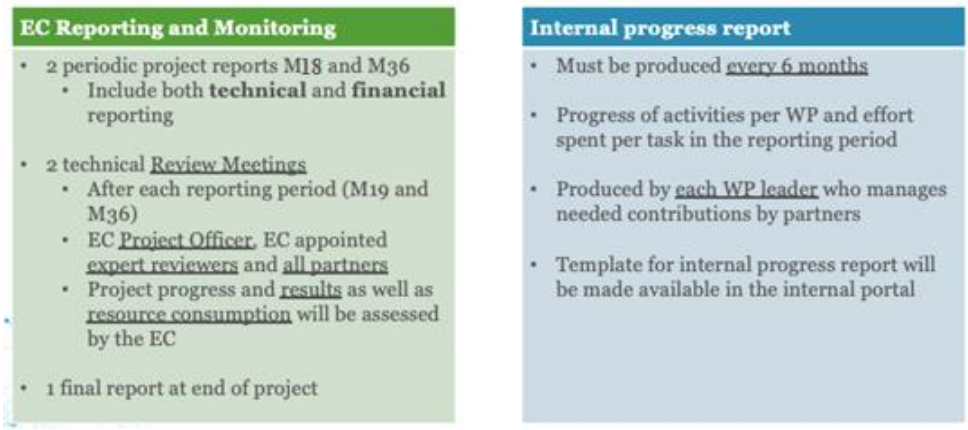


Figure 6-1 – ATLANTIS Project Reporting

The quality controls for each type of project reporting are illustrated in Table 6-2:

Table 6-2 – ATLANTIS Project Reporting Quality Control

Project Progress	Cycling Period	Description	Quality Controls
Two times a year	Every Six Months	An internal progress reporting mechanism. Every six months, each WP Leader is responsible for writing	Ensure that all partners have sent

		an internal progress report (collect contributions from all the involved partners, describing the progress of activities per WP and effort spent per task in the reporting period) and send it to the PC.	the requested input on time.
Periodic Project Reports to Commission	Every year and half	Periodic Project Reports are extended reports that will form the basis for the editing of the periodic progress reports to be forwarded to the Commission reporting the progress of the project during each period of the project.	Ensure that all inputs are present, and all action and meeting outcomes are taken in charge by the responsible person and configured.

6.4 Product Quality Assurance

In the case of deliverables, the first level of quality will be exercised by the responsible Task Leader who will establish a deliverable development plan identifying the deliverable coordinator, contributors, the development procedure and the evaluation process. The task leader and PC will identify two internal reviewers (IR) appointed by the General Assembly, not involved in the preparation of the deliverable (external to the WP or at least not initially involved in the writing process), to peer review the deliverable once the preliminary version is finished. The two revisers will provide in the shortest period of time, comments and proposed corrections to the document authors, in order to ensure high quality of the final document. The deliverable will also be circulated among partners for review and comments in case of serious doubts or disagreements about the quality of the deliverable. A Security and Ethical Review will be performed by the SAB and the DC. At the end, the PC will monitor the quality of work and deliverables and will report to the General Assembly on quality progress and resolution of issues. The deliverable quality assurance process is related to deliverables' quality and the procedure that should be followed as already been described. The product quality assurance is related to deliverables' quality and the procedure that should be followed as already been described in Section 4.1.

6.5 Management Responsibilities

Top management (i.e., PC, TM, WPLs) will provide evidence of its commitment to the development and implementation of the Quality Management and continually improving its effectiveness by establishing the quality policy and ensuring that the quality objectives are established. Review reports and meetings at specific time intervals will be conducted. The Quality Assurance monitoring will be ensured by PC, TM and WPLs. The members' task is to:

- Make sure the partners comply with the Quality Management procedures.
- Help measure and record the achievement of the project objectives.
- Make sure that usability and technical evaluation tests are properly carried out, and results reported back.

They are responsible for the coordination and supervision, regarding the implementation of the measures for the quality assurance.

In addition, the Quality Management responsibilities are to make sure that end users' requirements are taken into account to enhance their satisfaction. Moreover, that responsibilities and authorities are clearly defined and communicated with the consortium as already defined in DoA and in section 2 of this deliverable.

Other important aspect in terms of responsibility is to ensure that the internal communication processes are established within the consortium and that communication takes places regarding the effectiveness of Quality Management procedures as defined in this section.

6.6 Resources Management

In order to achieve the project objectives, ATLANTIS consortium has already made provision of resources and personnel needed for each work package as already defined in DoA. In addition, there is dedicated budget for the various needs of the project including equipment in terms of both hardware and software, travel, event organisation, open access dissemination and other goods and services costs (other direct costs). Financial reports will be made available by each partner in order to closely monitor the budget allocation through the lifetime of the project. Any deviations in costs, resources or schedules will be identified, recorded and used as input for continuous improvement. Possible impacts on the schedule, changes on the budget and resources of the project and on the quality of the product should be determined.

6.7 Risk Management

Quality and Risk Management are considered two key tools that contribute to the success of the project. Regular internal project reporting and a transparent communication approach will ensure that eventual problems or delays in project progress will be detected early and that corrective actions can be taken if necessary. Special attention will be paid to keeping the partners informed of the project status, planning and other important issues. In the lifetime of the project, potential risks will be ensured through self-assessment. The management process will identify and monitor, during project implementation, internal and external risks as well as any other issues that might affect the project progress towards its objectives, in order to carry out mitigation actions as early as possible. Risks can arise from:

- Unexpected technical difficulties or unexpected scientific findings.
- Poor communication or co-operation between the partners.
- Resource shortage by the partners
- Human operational errors: planning errors, poor quality, incomplete tasks, etc.

Risk Management is a process which enables the analysis and management of risks associated with the project. It is expected to increase the likelihood of successful completion of the project to cost, time and performance objectives. By nature, innovation projects should be effectively organised in order to handle change since their future is less predictable than other activities. To this end, the objective of risk management is to provide the process and techniques for the evaluation and control of potential project risks, focusing on their precautionary diagnosis and handling.

Responsibility for risk management is carried by many contributors within the project and each contributor must be aware of risk warning signs throughout the project's lifetime. In ATLANTIS, the General Assembly has the responsibility to identify on time any upcoming risks of a delay or deviation from the Work Plan or resource allocation and requesting all

necessary corrective actions from WP leaders. Moreover, the General Assembly will provide also a mechanism for the prevention and resolution of disputes. The PC will be the key person in the assessment of the achievement of the objectives and risks within the project throughout its complete duration and in the implementation of contingency plans. While, the SM will be responsible for monitoring risks and adjusting manpower assignment, together with the PC and the WP leaders and facilitating the information flow, collaboration effects between partners of the consortium. The management structure as outlined in Section 2 ensures that risks are reported promptly to the Coordinator via the WP leaders.

ATLANTIS will use **risk management procedures** based on the use of Risk Issue Logs identifying tolerances and thresholds and preparing contingencies. We will make an initial Quality and Risk Management (Task 1.2) at the outset of the project (updating and if necessary, adding to the risks identified below), which will feed into the Project Manual – Risk and Quality Management Plan (D1.1). A risk table associated to each WP has been established and will be progressively maintained throughout the project lifecycle. Table 6-3 summarises the critical risks for the project in its entirety and their mitigation measures. The table constitutes the 1st version of the risk registry of the project. The registry will be updated regularly (i.e., every six months) to include new risks, updated risks, as well as risks that have been cleared. Moreover, any risks that have materialized will be presented, along with the applied/activated mitigation actions and their outcomes.

Table 6-3 – Risk Registry Critical risks

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	A partner is not respecting the hierarchy and does not fulfil its obligations (Likelihood: Low, Severity: High)	ALL	As most partners have collaborated in the past, we consider that as very small probability. Yet, a clear decision-making process is agreed, and all measures will be taken to avoid any abnormal co-operation.
2	Agreement between partners is not achieved (Likelihood: Medium, Severity: Low)	ALL	In the project consortium agreement, we will define a clear structure and project management foresees clear conflict resolution and decision procedures to resolve any disagreement quickly.
3	A partner bankrupts, does not have sufficient financial viability or withdraws (Likelihood: Low, Severity: High)	ALL	If not possible to be replaced by an existing partner, a new partner will be sought via a transparent process. If it is a living lab owner, we may still produce excellent results utilising the remaining labs and trials.
4	High complexity and under estimation of project effort (Likelihood: Low, Severity: High)	ALL	The project will use an agile CI/DC/CP methodology and short work cycles which give detailed planning and early working versions of components minimizing the risk that results are not achieved.
5	Consensus on APIs/ interoperability with existing CI systems is not achieved (Likelihood: Medium, Severity: High)	WP2, WP3, WP4, WP5	Preliminary analysis has shown that interfacing existing CI system will be feasible. In case a CI security system is not possible to be interfaced the project will continue with the remaining systems.

6	Research concepts turn out to be harder than initially anticipated. (Likelihood: Medium, Severity: Medium)	WP2, WP3, WP4, WP5	ATLANTIS has an excellent consortium and is expected to create significant impact. If necessary, in co-operation with the Advisory Board, we will try to make more significant impact in a subset.
7	Living labs do not expose the necessary functionality or open APIs to integrate (High impact, low probability) (Likelihood: Low, Severity: High)	WP5	Preliminary analysis of all the living labs shows that exposing of APIs will be feasible. Moreover, ATLANTIS adopts a modular framework, thus if interfacing a legacy system is not achieved in a trial the use case will be slightly modified and tested in another trial.
8	Performance and behaviour of the system depends on the characteristics of the evaluation environment and how close it is to realistic conditions (Likelihood: Low, Severity: High)	WP5	An accurate assessment will be obtained by jointly analysing the lab and living labs results. Lab testing will be based on parameterizable models, which can capture various aspects of the real environment. The quantitative evaluation will consider various workload values, to assess the sensitivity and robustness, along with end-user behaviour.
9	During pilots, ATLANTIS might have access to sensitive data which could, in principle, constitute a risk to privacy. (Likelihood: Low, Severity: High)	ALL	We will establish guidelines at the beginning of the project on data handling based on applicable laws and regulations and will monitor their implementation. CRI will ensure legal compliance with EU data protection legislation as well as frameworks on data privacy
10	A new EU Policy comes into force (Likelihood: Medium, Severity: Medium)	ALL	In case a new EU Security policy or Data Protection Regulation comes into force, LSPs will be modified if needed.
11	A new security policy turns a trial inaccessible to the consortium (Likelihood: Low, Severity: High)	WP5	All trials have been committed and a consortium agreement will be signed before the project start. Yet, in case this risk takes place the project use cases will be executed only by the responsible.
12	Technology is not accepted by edge, cloud or IoT Stakeholders (Likelihood: Low, Severity: High)	ALL	The consortium will push towards commercialisation via continuous market analysis, events, Advisory Board feedback and overall, via a pan-European stakeholders group roadmap.
13	Technology is not accepted by decision makers or open source communities (Likelihood: Low, Severity: High)	ALL	Our use cases and trials are defined based on a research and commercial viewpoint and user centred design will make sure that every solution developed will actually fit business needs.
14	Impact on standards is not achieved (Likelihood: Low, Severity: Medium)	WP6	The ATLANTIS partners are actively participating in industry-standardization, thus at least ATLANTIS will be standards compliant.

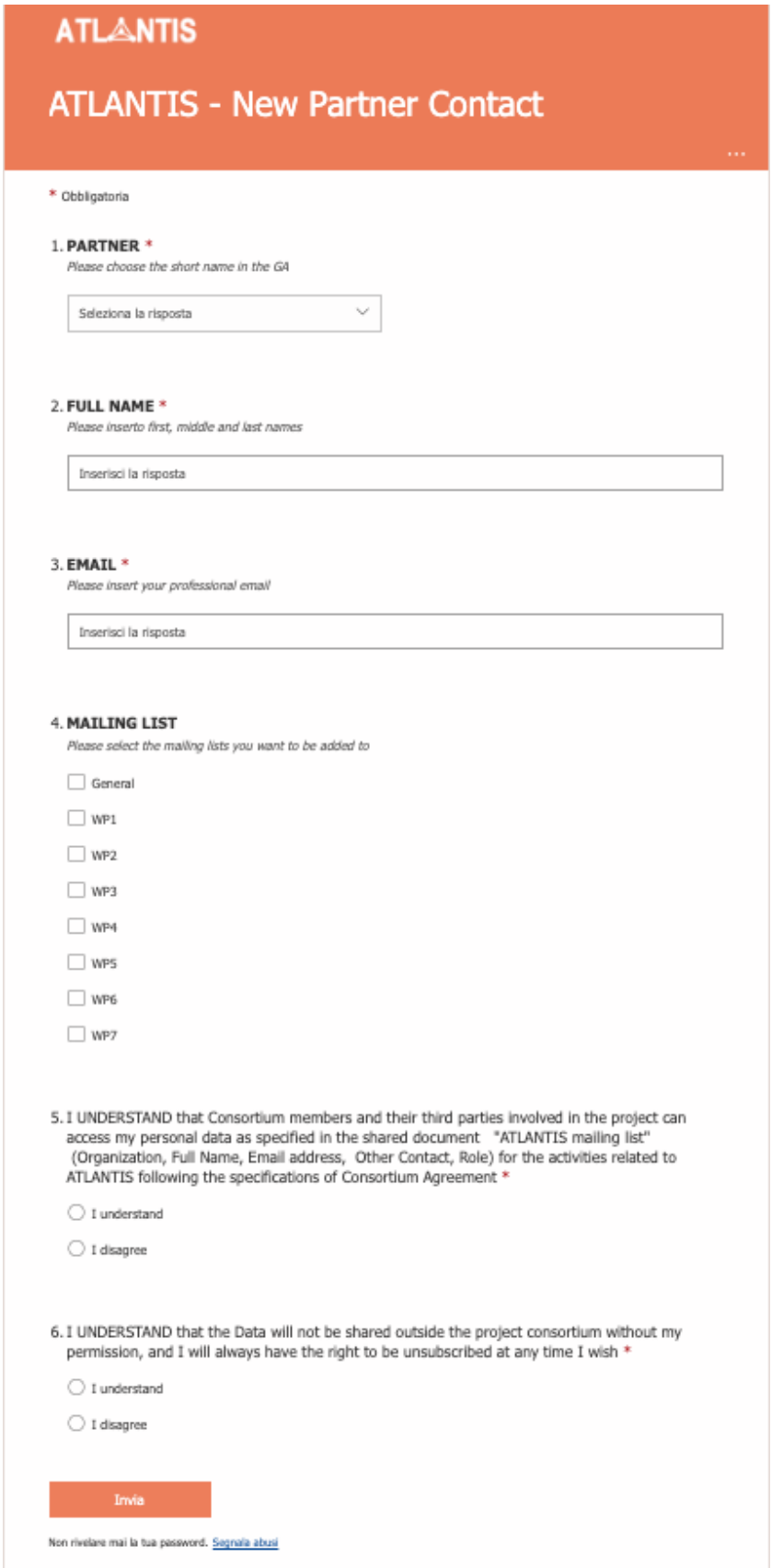
15	An IPR conflict arises among the consortium partners (Likelihood: Low, Severity: Low)	WP8	The ATLANTIS partners have already agreed on the common exploitation plan outlined in §2.2.2.1. The role distribution among the partners also ensures that no overlap of interest exists.

7 Conclusions and Future Outlook

This deliverable report defines rules, procedures and establishes a quality and risk management plan that should be followed within ATLANTIS project for achieving high quality results. All the project bodies were defined and explained on the basis what was already established in the proposal and accepted by all the participants by signing the Consortium Agreement. This report acts as a reference manual for all project partners and defines procedures that need to be respected by all members.

Annex I

Teams Data Policy



ATLANTIS

ATLANTIS - New Partner Contact

* Obbligatoria

1. **PARTNER** *
Please choose the short name in the GA

Seleziona la risposta

2. **FULL NAME** *
Please inserto first, middle and last names

Inserisci la risposta

3. **EMAIL** *
Please insert your professional email

Inserisci la risposta

4. **MAILING LIST**
Please select the mailing lists you want to be added to

- [ ] General
- [ ] WP1
- [ ] WP2
- [ ] WP3
- [ ] WP4
- [ ] WP5
- [ ] WP6
- [ ] WP7

5. I UNDERSTAND that Consortium members and their third parties involved in the project can access my personal data as specified in the shared document "ATLANTIS mailing list" (Organization, Full Name, Email address, Other Contact, Role) for the activities related to ATLANTIS following the specifications of Consortium Agreement *

- ( ) I understand
- ( ) I disagree

6. I UNDERSTAND that the Data will not be shared outside the project consortium without my permission, and I will always have the right to be unsubscribed at any time I wish *

- ( ) I understand
- ( ) I disagree

Invia

Non rivelare mai la tua password. Segnala abusi

EU RESTRICTED Deliverables Cover Page

RESTREINT UE/EU RESTRICTED

Dx.y <Deliverable full name (from DoA) here>

Work Package:	<WP here>
Lead partner:	<Lead Partner name and short code (from DoA) here>
Author(s):	<Authors name and surname (PARTNER_SHORTNAME)>
Due date:	<due date as per DoA>
Version number:	0.1 **Status:** Draft

Project Number:	101073909	**Project Acronym:**	ATLANTIS
Project Title:	European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection		
Start date:	October 1st, 2022		
Duration:	36 months		
Call identifier:	HORIZON-CL3-2021-INFRA-01		
Topic:	HORIZON-CL3-2021-INFRA-01-01		
	European infrastructures and their autonomy safeguarded against systemic risks		
Instrument:	IA		

Dissemination Level	
EU-RES: Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	✓

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909

RESTREINT UE/EU RESTRICTED

SENSITIVE and PUBLIC Deliverables Cover Page

Dx.y <Deliverable full name (from DoA) here>

Work Package:	<WP here>
Lead partner:	<Lead Partner name and short code (from DoA) here>
Author(s):	<Authors name and surname (PARTNER_SHORTNAME)>
Due date:	<due date as per DoA>
Version number:	0.1 **Status:** Draft

Project Number:	**101073909**	**Project Acronym:**	ATLANTIS
Project Title:	European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection		
Start date:	October 1st, 2022		
Duration:	36 months		
Call identifier:	HORIZON-CL3-2021-INFRA-01		
Topic:	HORIZON-CL3-2021-INFRA-01-01		
	European infrastructures and their autonomy safeguarded against systemic risks		
Instrument:	IA		

Dissemination Level	
PU: Public	✓
SEN: Sensitive	✓

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909

Meeting Minutes Cover Page

Meeting Minutes – <meeting name>, <meeting date>			
Work Package:	<WP here>		
Lead partner:	<Lead Partner name and short code (from DoA) here>		
Author(s):	<Authors name and surname (PARTNER_SHORTNAME)>		
Version number:	0.1	**Status:**	Draft

Project Number:	**101073909**	**Project Acronym:**	ATLANTIS
Project Title:	European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection		
Start date:	October 1st, 2022		
Duration:	36 months		
Call identifier:	HORIZON-CL3-2021-INFRA-01		
Topic:	HORIZON-CL3-2021-INFRA-01-01 European infrastructures and their autonomy safeguarded against systemic risks		
Instrument:	IA		

Template for Meeting Agenda

< Meeting name >
<Type of meeting (e.g. physical, virtual, hybrid)>
<Meeting venue>
<Meeting date>

Day 1 – meeting date
<< DAY 1 conference call link>>

Time (CEST)	Topic	Presenter
Time slot (hh:mm – hh-mm) (mins)	Topic name	e.g. ALL or speakers' names (Beneficiaries Short Name)
Time slot	**Break (mins)**	
Time slot (hh:mm – hh-mm) (mins)	Topic name	e.g. ALL or speakers' names (Beneficiaries Short Name)
Time slot	**Lunch (mins)**	
Time slot (hh:mm – hh-mm) (mins)	Topic name	e.g. ALL or speakers' names (Beneficiaries Short Name)
Time slot	**Break (mins)**	
Time slot (hh:mm – hh-mm) (mins)	Topic name	e.g. ALL or speakers' names (Beneficiaries Short Name)
Time	**End of DAY 1**	

Template for Attendees List

<Meeting name>
<Meeting venue>

List of attendees for <meeting data>

	Participant name	Partner short name	Country	Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Funded by the
European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909