Grant Agreement No.: 952697
Call: H2020-SU-ICT-2018-2020
Topic: SU-ICT-02-2020
Type of action: RIA

ASSURED

D8.4 RISK ASSESSMENT PLAN

Revision: v.1.0

Work package	WP 8
Task	Task 8.2
Due date	31/08/2021
Submission date	23/08/2021
Deliverable lead	Martel
Version	1.0
Authors	Jean-Baptiste Milon (Martel)
Reviewers	Thanassis Giannetsos (Ubitech)
Abstract	The purpose of the “Risk Assessment Plan” of the ASSURED project, is to provide a single point of reference on the risk approach that will be pursued throughout the course of the project. The deliverable at hand defines the project organisation, roles and responsibilities with emphasis on the risk assessment, risk monitoring and risk mitigation activities that will be carried out. It describes how the project will execute its day-to-day activities from a risk perspective, and ensures that standards, processes, and procedures are defined so that their execution is continuously monitored and improved. This deliverable defines all the necessary mechanisms and structures for the risk management and coordination of the project with emphasis on the assessment, risk communication, stages, milestones, reporting roles and responsibilities for all the partners on this aspect of the project is also made.

Keywords	Risk Management Plan, risk management, scope management, cost management, cost baseline, schedule baseline, schedule management, effort, budget, indicators, quality management, risk assessment, communication management, communication matrix, software management, guidance, administration

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	10/07/2021	Table of contents	Jean-Baptiste Milon (Martel)
V0.2	20/07/2021	First draft	Jean-Baptiste Milon (Martel)
V0.3	23/08/2021	Second draft	Thanassis Giannetsos (Ubitech)
V0.4	23/08/2021	Final review	Jean-Baptiste Milon (Martel)
V0.5	23/08/2021	Submission	Jean-Baptiste Milon (Martel)

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**to specify R, DEM, DEC, OTHER***	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ASSURED project and Commission Services	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Funded by the Horizon 2020 Framework Programme of the European Union

EXECUTIVE SUMMARY

The purpose of the “Risk Assessment Plan” of the ASSURED project, is to provide a single point of reference on the risk approach that will be pursued throughout the course of the project. The deliverable at hand defines the project organization, roles and responsibilities with emphasis on the risk assessment, risk monitoring and risk mitigation activities that will be carried out. It describes how the project will execute its day-to-day activities from a risk perspective, and ensures that standards, processes, and procedures are defined so that their execution is continuously monitored and improved. This deliverable defines all the necessary mechanisms and structures for the risk management and coordination of the project with emphasis on the assessment, risk communication, stages, milestones, reporting roles and responsibilities for all the partners on this aspect of the project is also made.

Funded by the Horizon 2020
Framework Programme of the European Union

TABLE OF CONTENTS

Funded by the Horizon 2020 Framework Programme of the European Union

LIST OF FIGURES

Funded by the Horizon 2020
Framework Programme of the European Union

LIST OF TABLES

Funded by the Horizon 2020
Framework Programme of the European Union

ABBREVIATIONS

CA	Consortium Agreement
CR	Change Request
DL	Deliverable Leader
DMS	Document Management System
DoA	Description of Action
Dx	Deliverable (where x defines the deliverable identification number e.g. D1.1.1)
EC	European Commission
ECAS	European Commission Authentication Service
EU	European Union
GA	General Assembly
GRA	Grant Agreement
KPI	Key Performance Indicator
MSx	project Milestone (where x defines a project milestone, e.g. MS3)
Mx	Month (where x defines a project month, e.g. M10)
MoM	Minutes of Meeting
O	Other
P	Prototype
PC	Project Coordinator partner (Martel)
PM	Person Month (a unit to count workload)
PMB	Project Management Board
PMCT	Project Management and Coordination Team
PO	Project Officer
PP	Restricted to other programme participants (including the Commission Services)
PPM	Partner Project Manager
PU	Public
QA	Quality Assurance
QAP	Quality Assurance Plan
R	Report
RE	Restricted to a group specified by the consortium (including Commission Services)
R&D&I	Research & Innovation & Development
SM	Scientific Manager
TL	Task Leader
WP	Work Package
WPL	Work Package Leader
WPS	Work Package Structure

Funded by the Horizon 2020 Framework Programme of the European Union

1 INTRODUCTION

1.1 DOCUMENT SCOPE

"Avoiding rocks on the road to success" [1] - following this guiding principle, the ASSURED consortium has established an effective project risk management strategy to avoid tripping over rocks on the road to successfully reach the planned project outcomes or go even beyond.

ASSURED is a unique, innovative H2020 project, which will **futureproof the next-generation smart connectivity "Systems-of-Systems" (SoS)**, comprising a multitude of heterogeneous embedded systems, running mixed-criticality services with different security, privacy and trust considerations. More specifically, the vision is to deploy a holistic trusted computing-enabled edge-cloud framework towards the provision of **enhanced, multi-tenant and perpetual protection** based on the convergence of the strict security, privacy, trust and functional requirements of innovative, mixed-criticality applications and silos running in highly complex and distributed (supply chain) ecosystems. Under the guiding principle "*Never Trust, Always Verify*", the goal of the envisioned ASSURED architecture is to enable the long term transformation of emerging supply chains in a distributed smart connectivity infrastructure with **embedded trust and high integration with edge computing** and processing while demonstrating the use of **trusted computing and Blockchain technologies** for addressing the pressing challenges of several vertical industry sectors in the context of **efficient, reliable and secure extraction and sharing of threat intelligence knowledge, perceived zero trust** in ecosystems with highly diverse device hardware densities and mobility requirements.

Developing and dealing with such an ambitious and highly innovative project, only *"innovation, fused with an agile, sophisticated approach to risk management, can create a powerful, value-driving partnership."* [2]

According to the ISO 31000 standard on risk management, a **risk** can be defined as an "*effect of uncertainty*" towards parts of objectives. An effect is described as a positive or negative deviation from the expected work-plan. Every step towards the project objectives has an element of risk that needs to be managed. [3]

In the context of risk management, **uncertainty** exists whenever the knowledge or understanding of an event, consequence, or likelihood is inadequate or incomplete. [3]

Risk management describes a coordinated set of activities and methods, which supports the control of risks that may affect the project's ability to achieve part of its objectives. The project risk management process is meant to form part of the project management routine at all stages of the project lifecycle. [3]

In order to raise awareness for the central project activities and as a starting point for risk management, a critical path has been defined, which is described in Chapter 3. Failing to follow a structured project risk management process for projects in a self-disciplined manner would quickly lead to project failure [3]. Therefore, within ASSURED a clear structured process of risk identification, risk monitoring & analysis and risk handling has been established (see Chapter 4). This process already started with the risk identification during the proposal preparation phase, continued in all process steps within the first year of the project and will accompany ASSURED throughout the project's lifetime. In order to settle this process as a vital one, communication as well as easy risk assessment tools turned out to be critical factors. Chapter 5 displays the practical risk assessment of ASSURED including an evaluation of probability and severity as well as mitigation plans for defined risks.

Funded by the Horizon 2020 Framework Programme of the European Union

1.2 DOCUMENT STRUCTURE

The purpose of the “Risk Assessment Plan” of the ASSURED project, is to provide a single point of reference on the risk approach that will be pursued throughout the course of the project. The deliverable at hand defines the project organization, roles and responsibilities with emphasis on the risk assessment, risk monitoring and risk mitigation activities that will be carried out. It describes how the project will execute its day-to-day activities from a risk perspective, and ensures that standards, processes, and procedures are defined so that their execution is continuously monitored and improved. This deliverable defines all the necessary mechanisms and structures for the risk management and coordination of the project with emphasis on the assessment, risk communication, stages, milestones, reporting roles and responsibilities for all the partners on this aspect of the project is also made.

This document is comprised of the following chapters:

Chapter 1 presents an introduction to the document.

Chapter 2 offers information related to the project objectives, workplan and outputs, to provide the context for this document.

Chapter 3 explains the overall strategy and approach towards Risk Management

Funded by the Horizon 2020 Framework Programme of the European Union

2 ASSURED CONTEXT

2.1 PROJECT SCOPE AND OBJECTIVES

The ASSURED vision is rooted in the fact that CPS (e.g., manufacturing, aerospace, satellite and smart cities systems) are made up of components supplied by multiple vendors, often also because of the legal obligation not to lock suppliers out of the supply chain. Furthermore, these systems are increasingly integrated with global information and management networks.

Therefore, they **constitute ever more complex SoS with no single tenant or provider**. In the face of an increasing landscape of cyber-attacks, it must be possible to understand how remediation must be applied rapidly, otherwise we risk major disasters caused by malicious failures of our IT infrastructure. Consequently, we must understand CPS inherently and increasingly as **Federated Safety Critical Systems designed, implemented, operated, and owned by multiple tenants with different security goals, requirements, and priorities**.

Furthermore, **security cannot be seen in an isolated way**, but must be considered also in the face of the safety of the overall system. Simply disabling some communication for security reasons may leave the system in an unsafe state and lead to further damage. It is necessary to understand what is semantically sensible for a component of a certain type to do and from this microscopic view expand to overall system analysis.

ASSURED relies on three core pillars:

- **Remote attestation of Properties**
- **Dynamic real-time risk assessment**
- **Enforcement of self-learning adaptable policies and enhanced secure data sharing**

ASSURED has laid out Seven core objectives:

- **Objective I:** The design and development of a novel, highly-usable, and resilient cybersecurity, privacy and data protection management framework, targeted at “Systems-of-Systems” (SoS) enabled ecosystems
- **Objective II:** The construction of a highly automated middleware for the secure configuration, deployment, operation, management and maintenance of edge devices, processes and safety-critical software components
- **Objective III:** The identification and implementation of a reactive, runtime risk assessment model, facilitating the real-time handling of threats and identified risks, for enhancing the security- and privacy-by-design features of the entire ASSURED security assurance and data sharing framework through a holistic threat assessment against aspects of such hyper-connected SoS.
- **Objective IV:** The leverage of the ASSURED Framework to automatically infer optimal software deployment plans, for the safe implementation of mixed-criticality applications in CPSs and support their correct execution and verification through an incremental adoption and deployment of (on-demand) capability-oriented security attestation controls.
- **Objective V:** The provision of a secure, trusted and audible data sharing environment (for threat intelligence data and beyond) by designing and implementing advanced Blockchain operation and control services through leveraging distributed ledgers infrastructure and

Funded by the Horizon 2020 Framework Programme of the European Union

specifying novel Trusted Component (TC)-enabled security and privacy-preserving protocols

- **Objective VI:** The delivery of the applicability, usability, effectiveness and value of the ASSURED concepts, models and identified security, privacy, trust and operational assurance enablers in real-world industries, safety critical infrastructures and applications
- **Objective VII:** The insurance of wide communication and scientific dissemination of the innovative ASSURED results to the research, academic, and international community, the efficient exploitation and business planning of the ASSURED concepts and tools to SoS and ICT supply chains

2.2 PROJECT WORKPLAN

The ASSURED work plan is organized in eight work packages whose relations are shown in the PERT chart below.

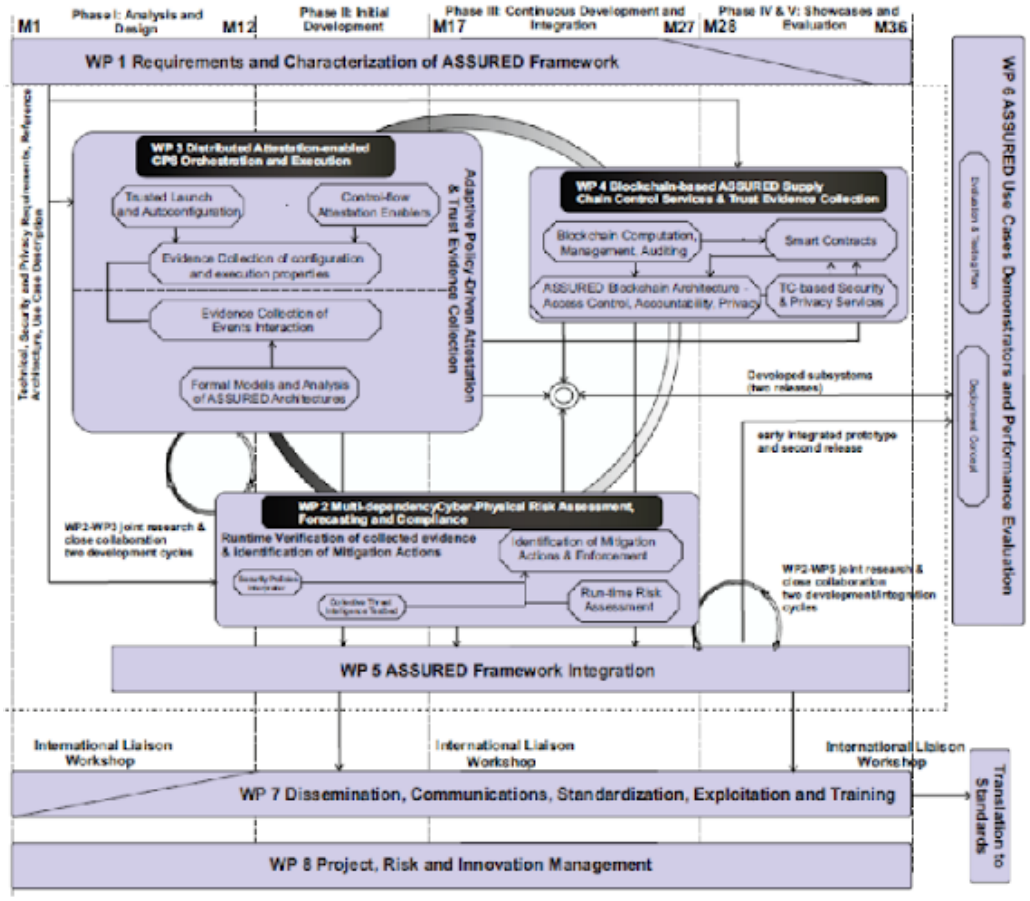

FIGURE 1: ASSURED WP STRUCTURE AND RELATIONS

- **WP1**, Requirements and Characterization of ASSURED Framework
- **WP2**, Multi-dependency Cyber-Physical Risk Assessment, Forecasting and Compliance
- **WP3**, Distributed Attestation-enabled CPS Orchestration and Execution
- **WP4**, Blockchain-based ASSURED Supply Chain Control Services and Trust Evidence Collection
- **WP5**, ASSURED Framework Integration

Funded by the Horizon 2020 Framework Programme of the European Union

- **WP6**, ASSURED Use Cases Demonstrators & Performance Evaluation
- **WP7**, Dissemination, Communications, Standardization, Exploitation and Training
- **WP8**, Project Risk and Innovation Management

2.3 MILESTONES

Project milestones are presented in **Annex 1 of the Grant Agreement**, in the **Description of the Action (DoA).** The complete milestone table is provided within Section **1.3.4 WT4: 'List of milestones'** of the DoA, but also in the following table.

TABLE 1: LIST OF MILESTONES

No	Milestone title	WP	Date
MS1	Availability of the technical, security, privacy and functional safety requirements to be met by the ASSURED Framework and the use cases	WP1	M06
MS2	Availability of the ASSURED Reference Architecture	WP1	M09
MS3	Availability of the ASSURED conceptual models designing the integral security, privacy, operational assurance and data sharing services	WP1	M12
MS4	Availability of ASSURED's collaborative risk assessment methodology, the design of the operational assurance attestation enablers, the Blockchain architecture and the ASSURED Framework integration plan	WP2 WP3 WP4 WP5	M15
MS5	Availability of the ASSURED Framework Components and Mechanisms – Early Release	WP2 WP3 WP4 WP5 WP6	M18
MS6	Availability of the ASSURED Integrate Framework – First Release	WP2 WP5	M30
MS7	Readiness of the ASSURED Demonstrators & Early Performance Evaluation (1st Demonstration Phase)	WP6	M24
MS8	Availability of the ASSURED Framework, Components and Mechanisms – Final Release	WP2 WP3 WP4 WP5	M30
MS9	Readiness of the ASSURED Demonstrators (2nd Phase)	WP6	M33

Funded by the Horizon 2020 Framework Programme of the European Union

MS10	Availability of ASSURED Evaluation, Validation, Lessons Learnt and Adoption Guidelines	WP5 WP6	M36

2.4 DELIVERABLES

A detailed deliverable list is presented in **Annex 1 of the Grant Agreement** within Section **1.3.2 WT2: 'List of Deliverables'** of the DoA, but also here:

TABLE 2: LIST OF DELIVERABLES

No	Deliverable title	Delivery Date	Lead Beneficiary	Nature
D1.1	ASSURED Use Cases and System Requirements	M06	UTRCI	R
D1.2	ASSURED Reference Architecture	M09	DTU	R
D1.3	Operational SoS Process Models & Specification of Properties	M12	TUDA	R
D1.4	Report on Security, Privacy and Accountability Models for Dynamic Trusted Consent and Data Sharing	M12	TUE	R
D2.1	Risk Assessment Methodology and Threat Modelling	M15	DTU	R
D2.2	Policy Modelling & Cybersecurity, Privacy and Trust Policy Constraints	M15	MLNX	R
D2.3	ASSURED Runtime Risk Assessment Framework - version 1	M18	UBITECH	O
D2.4	ASSURED Runtime Risk Assessment Framework - version 2	M30	UBITECH	O
D2.5	Security Context Broker Specification and Smart Contract Definition & Implementation for Policy Enforcement - version 1	M18	TUE	R
D2.6	Security Context Broker Specification and Smart Contract Definition & Implementation for Policy Enforcement - version 2	M30	TUE	O
D2.7	ASSURED Collective Threat Intelligence Analysis & Forecasting Framework - version 1	M18	UTRCI	O
D2.8	ASSURED Collective Threat Intelligence Analysis & Forecasting Framework - version 2	M30	UTRCI	O
D3.1	ASSURED Attestation Model and Specification	M15	UBITECH	R

Funded by the Horizon 2020 Framework Programme of the European Union

D3.2	ASSURED Layered Attestation and Runtime Verification Enablers Design & Implementation - version 1	M15	TUDA	R
D3.3	ASSURED Layered Attestation and Runtime Verification Enablers Design & Implementation - version 2	M30	TUDA	O
D3.4	ASSURED Real-time Monitoring and Tracing Functionalities - version 1	M18	MLNX	R
D3.5	ASSURED Real-time Monitoring and Tracing Functionalities - version 2	M30	MLNX	O
D3.6	ASSURED Secure and Scalable Aggregate Network Attestation - version 1	M18	TUDA	R
D3.7	ASSURED Secure and Scalable Aggregate Network Attestation - version 2	M30	TUDA	O
D4.1	ASSURED Blockchain Architecture	M15	SUITE5	R
D4.2	ASSURED Secure Distributed Ledger Maintenance & Data Management	M18	SURREY	R
D4.3	ASSURED Blockchain-based Control Services and Crypto functions for Decentralized Data Storage, Sharing and Access Control - version 1	M18	TUE	R
D4.4	ASSURED Blockchain-based Control Services and Crypto functions for Decentralized Data Storage, Sharing and Access Control - version 2	M30	TUE	R
D4.5	ASSURED TC-based Functionalities - version 1	M18	SURREY	R
D4.6	ASSURED TC-based Functionalities - version 2	M30	SURREY	O
D5.1	Technical Integration Points, APIs Specification and Testing Plan	M15	INTRA	R
D5.2	ASSURED Blockchain and Data Storage Environment	M18	UNIS	O
D5.3	ASSURED Secure Information & Attestation Data Exchange Services Implementation - version 1	M21	SUITE5	O
D5.4	ASSURED Secure Information & Attestation Data Exchange Services Implementation - version 2	M30	SUITE5	O
D5.5	ASSURED Integrated Framework, Testing and Refinement - version 1	M21	INTRA	O

Funded by the Horizon 2020 Framework Programme of the European Union

D5.6	ASSURED Integrated Framework, Testing and Refinement - version 2	M30	INTRA	O
D6.1	Evaluation Framework and Demonstrators Planning	M18	UTRCI	R
D6.2	First Demonstrators Implementation Report	M24	BIBA	R
D6.3	Final Demonstrators Implementation Reports	M33	UTRCI	R
D6.4	Performance Evaluation and Adoption Guidelines	M36	SUITE5	R
D7.1	Internal and External IT Communication infrastructure and project website	M03	MARTEL	W
D7.2	Exploitation, Standardisation, Dissemination and Communication Activities Report - version 1	M18	TUE	R
D7.3	Exploitation, Standardisation, Dissemination and Communication Activities Report - version 2	M36	TUE	R
D7.4	Market Analysis, Business and Sustainability Plan - version 1	M21	SPACE	R
D7.5	Market Analysis, Business and Sustainability Plan - version 2	M36	SPACE	R
D7.6	Project's Impact Assessment - version 1	M21	DAEM	R
D7.7	Project's Impact Assessment - version 2	M36	DAEM	R
D8.1	Project Quality Plan	M03	MARTEL	R
D8.2	Data Management Plan (DMP) - version 1	M6	MARTEL	R
D8.3	Data Management Plan (DMP) - version 2	M24	MARTEL	R
D8.4	Risk assessment plan	M24	MARTEL	R

Funded by the Horizon 2020 Framework Programme of the European Union

3 CRITICAL PATH OF THE PROJECT

As a starting point for risk management, the critical path of ASSURED has been defined in order to be aware of the central project activities. The critical path determines the targeted time to complete the project and the critical activities that might be able to threaten the project objectives. **The items of the critical path are mostly reflected by project milestones, presenting central and critical achievements during the project lifetime**.

Towards this direction, the ASSURED consortium had identified a list of risks – during the proposal preparation phase – that could be materialized during the project lifecycle and, thus, continuous monitoring is needed. Table 3 provides a summary of such identified risks.

Figure 2 below indicates the key activities of ASSURED that must be performed in order to meet the planned objectives successfully and on time. The items of the critical path are mostly reflected by project milestones, presenting central and critical achievements during the project lifetime. The timeline indicates that the key topics of the project differ during the project duration. The critical path analysis helps the consortium to predict whether the project can be completed on time and as it progresses, to keep the project's completion on track. It also helps to ensure that deliverables are ready as scheduled. Besides the critical path, which the consortium is challenged to pass, risks will occur in different work packages and might influence the projects´ development if not handled carefully and timely. Therefore, the critical observation and examination of risks has a central role during the project lifetime. The following chapters focus on the risk management process established within ASSURED.

After a successful project kick-off in September 2020, the ASSURED partners mainly focused on WP1 which defines the **security and privacy requirements of the supply chain ecosystems** that must be met by the ASSURED framework as well as the definition of the **data sharing behaviors**, between all involved actors in such environments (that need to be secured by leveraging advanced crypto primitives in conjunction with the underlying Blockchain infrastructures) and the **operational assurance models** (per use case) by fleshing out the system properties that need to be secured throughout the entire lifecycle of the deployed devices. The first milestone "Use Cases Definition and System Requirements" was achieved in M06 of the project, after submitting D1.1. The second milestone "Availability of the ASSURED Reference Architecture" was achieved in M09 of the project, after submitting D1.2. With reaching MS3 in M12, the "Data Sharing Behaviors and Operational Assurance Models" will be available (D1.3 and D1.4, respectively). In addition to that the project consortium has been working in parallel on all the three core technical work packages: Risk Assessment and Policy Generation (WP2); Remote Attestation (WP3); Blockchain Architecture and Secure Data Sharing (WP4).

In M16, the goal is to also hold the 1st ASSURED Workshop on Secure Systems. The workshop's goal will be to foster collaboration between different key players in the secure system and trusted computing communities and others involved in similar projects.

The next big project milestone is MS4 "Availability of the ASSURED Risk Assessment, Remote Attestation Data Sharing Models and Crypto Primitives", which is due in M15 (November 2021). To reach MS4 an early release of the designs and models of the components and mechanisms of the ASSURED Framework is needed.

As soon as results can be made publicly available, the project consortium will publish scientific articles and present the project to external stakeholders. To conclude, it can be said that the analysis of the critical path helped to identify critical items and allows us to put necessary measures into place.

Funded by the Horizon 2020 Framework Programme of the European Union

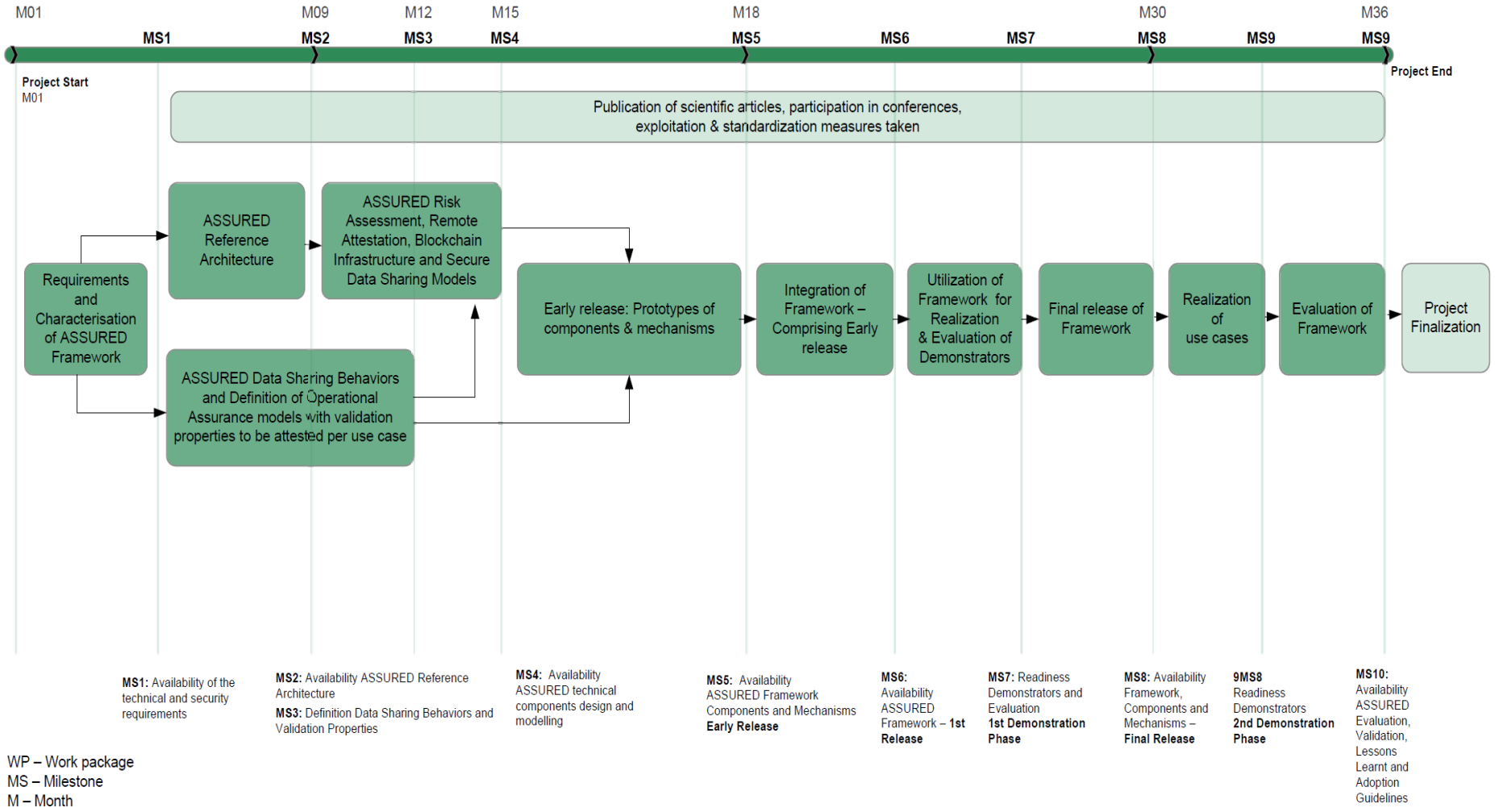

FIGURE 2: CRITICAL PATH

Funded by the Horizon 2020 Framework Programme of the European Union

3.1 LIST OF IDENTIFIED RISKS

A detailed Risk list is presented in **Annex 1 of the Grant Agreement** within Section **1.3.5 WT5: "Critical Implementation risks and mitigation actions"** of the DoA, but also here:

TABLE 3: LIST OF IDENTIFIED RISKS

RISK REGISTER					
#	**WP**	**WP Start**	**WP End**	**Descrition**	**Mitigation**
1	8	M1	M36	AFR1: Insufficient consortium coordination	The effective management of the consortium will be assured with the appropriate Project Management described in WP8. The roles & responsibilities of each partner are already identified and will be continuously reviewed to mitigate the risk of overlapping and implementation of the same activities from two or more partners.
2	8	M1	M36	AFR2: Budget issues due to complexity	The project baseline has been defined, utilizing existing assets. Budget carefully allocated; resources will be monitored during the project.
3	8	M1	M36	AFR3: Insufficient consortium competence / effectiveness	The project team is highly complementary and gathers together the requested skills for the main streams of research and technology development. Moreover, all the technologies that are going to be used in the implementation of the project will be carefully selected to minimize potential risks on these technologies. If a consortium incompetence is identified, the consortium partners will try to fill this gap either through the own pools of resources, or through subcontracting.
4	7	M1	M36	AFR4: Conflicts over ownership	Disagreements in the consortium over ownership may result in non-agreement on IPR. The principles and the existing assets included in the Consortium Agreement, the continuous activity in T7.3 on IPR handling, and the creation of an ongoing IPR inventory will ensure protection of generated and prior IPR.
5	8	M1	M36	AFR5: Shortage of resources and/or change of personnel	Problems with personnel relate to lack of competencies and withdrawals. However, all the partners have assured that they will choose their best personnel to implement the relevant activities. All partners could change a member of their team with another person with comparable competencies, in case of inability to continue. Keep close contact with all partners. Early communication of budget and personnel problems.

Funded by the Horizon 2020 Framework Programme of the European Union

6	8	M1	M36	AFR6: Lack of communication among the partners	Keep close contact with all partners by regular teleconferences and virtual meetings. Organise regular plenary and technical meetings at different partners' sites. Consider reworking the exploitation plans. Detailed project plan that clearly states goals and responsibilities of the partners.
7	8	M1	M36	AFR7: Partner withdrawal	Immediate substitution by another partner, from existing partnerships, through dissemination activities or from interaction with cybersecurity industry.
8	6	M10	M36	TIR1: CubeSat compute resources are insufficient to host the surveillance application plus the remote attestation functions	The satellite-based surveillance application to be implemented on-board will be implemented taking into account the resource constraints. If necessary, part of the functions (e.g. image processing) will be off-loaded to the ground station, at the expense of increased communication overhead.
9	3	M7	M30	TIR2: High performance Overhead of Control-flow attestation	Providing trade-offs between performance and security assurance, deployment of hardware accelerators to offload the computation-intensive tasks.
10	1	M1	M12	TIR3: Requirements and architectures do not produce workable security services, mechanisms or implementations	While the changing field of security and threat intelligence based on the use of advanced attestation and deep learning mechanisms inserts an unknown factor, the researchers in the consortium are at the leading edge of the field and will adapt to any major developments. It is still possible that no solutions are possible for the requirements set out. In this case the requirements can be revisited at a later stage and adapted to meet the practicalities of network security and operational assurance and/or real-world implementation.
11	1	M1	M12	TIR4: Proposed operational models too ambitious to be implemented and work properly	The project will make careful steps towards the realization of its objectives. If needed, the consortium has the experience to adjust these objectives so that they can be achievable and still yield the anticipated results. The project will follow the motto "think big, act small" in order to produce results that could realistically become exploitable and useful after its completion.
12	2	M7	M30	TIR5: Multi Dependency Cyber Threats modelling not completed	Close collaboration with WP3 activities for better understanding low-level network and device threats and vulnerabilities. Incorporation of widely known vulnerabilities and threats repositories (e.g. US NIST CPE/CVE).
13	2	M7	M30	TIR6: Risk Assessment methodology not completed	Joint research activities with WP3 & WP4 for better incorporating the specificities of the ASSURED integral components.

Funded by the Horizon 2020 Framework Programme of the European Union

14	2	M7	M30	TIR7: Some SDKs not completed	WP1 task's input will allow the realization of SoS assets enumeration and criticality quantification. WP2, WP3 and WP4 will provide SDKs, services and tools for SoS for cybersecurity services deployment.
	3	M7	M30		
	4	M7	M30		
15	2	M7	M30	TIR8: Limited functionality or inadequate integration of ASSURED Framework	The workplan includes two tight cycles of development, integration and demonstration of the components (WP2-WP5). The successful integration of these components into the ASSURED Framework (WP5) represents a critical chapter in the workplan. An overlap is in place between implementation and integration, as well as continuous participation of the same partners and strong horizontal technical coordination of WP2-WP5.
	3	M7	M30		
	4	M7	M30		
16	2	M7	M30	TIR9: Project propositions too ambitious to work properly in project runtime	The project will make careful steps towards the realisation of its objectives. If needed, the consortium has the experience to adjust these objectives so that they can be achievable and still yield the anticipated results. The project will follow the motto "think big, act small" to produce results that could realistically become exploitable and useful after its completion.
	3	M7	M30		
	4	M7	M30		
17	2	M7	M30	TIR10: Project facing technology replacement issues	ICT technologies continue to be developed at rocket speed, and it is difficult to foresee their evolution. Thus, the project will be engaged in a continual technology watch effort, which will last till the very end of the project. The technical management of the project will always be in touch with the scientific community for learning about possible future disruptive technologies relevant to the project activities. The consortium will deliver concepts that are going to be built on existing standards to effectively face potential technology replacement issues.
	3	M7	M30		
	4	M7	M30		
18	7	M1	M36	TIR11: Insufficient Project Impact, Community Building, Stakeholders Engagement	The consortium consists of a number of technology providers, cybersecurity experts, IT service providers, end users, indicating the interest of industry in ASSURED. The extended community and business network of these industrial partners (SPH, DAEM, BIBA, UTRCI) and cybersecurity (MARTEL, TUE, SURR) will reassure the reach out of a critical mass of stakeholders, service providers, vendors and verticals.
19	3	M7	M30	TIR12: Insufficient cybersecurity services and systems support for the Demonstrators	The workplan has already foreseen the involvement of the demonstration partners early in the project's lifecycle, imposing the detailed definition of the demonstrators' scenarios at M06. Moreover, there will be two releases of the ASSURED Framework and its components reassuring their efficiency.
	4	M7	M30		
	6	M10	M36		

Funded by the Horizon 2020 Framework Programme of the European Union

20	3	M7	M30	TIR13: Algorithms will not fit on current resource constrained devices	Using a reconfigurable and big enough System on Chip device, where resource constraints can be preselected and changed.
21	5	M7	M30	TIR14: Insufficient data availability	The demonstration partners SPH, BIBA, DAEM and UTRCI have already committed themselves to provide already available datasets, in accordance to the National Laws and EC Regulations. As a matter of fact, the companies work already internally to have everything ready at the project's kick off date.
	6	M10	M36		
22	5	M7	M30	TIR15: User friendliness issue on the adoption of ASSURED Framework	Close collaboration with supply chains and SoS during the design, specification, development and implementation of several components (WP2-WP4), to ensure that all these services integrated into the ASSURED Framework meet the needs of end users. Moreover, there will be two releases of the ASSURED Framework to ensure that the feedback from end users at the first evaluation phase is considered.
	6	M10	M36		
23	1	M1	M12	TIR16: Failure to provide comprehensive use cases and elicit solid requirements	At the beginning of the project, the consortium will try to aggregate and analyse all functional and non-functional, generic and demonstrator-specific requirements. These requirements will be translated into technical requirements, and in turn into technical components. Should additional requirements be identified in the future, because of the agile development process, the consortium will try to integrate the new functionalities in the platform to the extent possible.
24	7	M1	M35	TIR17: Business plan failing to exploit market opportunities	The development of the ASSURED business plan will be led by an experienced and professional team. Nevertheless, opportunities may be identified by other partners in the domain, or later in the project, but within its lifecycle. Should this happen, the business plan development leaders will evaluate the opportunities, and modify the business plan accordingly in its final iteration to facilitate the exploitation of these opportunities.

Funded by the Horizon 2020 Framework Programme of the European Union

4 RISK MANAGEMENT PLAN

INTRODUCTION

Risk is an “event/issue” that may happen and have an impact on our project. The purpose of the **Risk Management Plan** is to prevent those events from happening or minimize their impact in case they happen.

ASSURED is a complicated and demanding project and its success highly depends on the effectiveness of the **risk management process**. The objective of the risk management procedure is to provide the processes and techniques for the evaluation & control of potential project risks, focusing on their precautionary diagnosis & handling. The **Project Coordinator** with the cooperation of the **Technical Coordinator** and the rest of the project management roles (WP and Task Leaders) will be mainly responsible to handle risks and inform all partners when necessary.

4.1 RISK METHODOLOGY

Risk management is as an overarching process that encompasses **risk planning** (identification, assessment, analysis, mitigation planning) and **risk abatement** (mitigation plan implementation, tracking, risk reassessment), in an **iterative cycle** until the end of the project, to ensure that risks are identified in a timely manner and handled proactively.

In more detail, this involves the **identification** of a risk, the **assessment** of its importance and the **evaluation** of whether the risk level is higher than the risk that could be accepted for the project. In case that a risk exceeds the acceptable levels, a risk **analysis** activity will be instantiated that will define the required actions, in order to set the risk within acceptable levels. In addition, the management of risks also involves the planning of the required activities to handle the risk, the redistribution of resources, the evaluation of the results, as well as ensuring the stability of the new status.

FIGURE 3: RISK MANAGEMENT PROCESS

Timely awareness and reaction to potential problems are crucial to effective risk management. That is why it is essential for ASSURED to effectively manage changes. Changes may arise in **project scope, project cost, time-schedule or techniques employed**. In ASSURED, change management will be realized with standard activities (as described in D8.1 Chapter 5) ensuring that potential changes will happen only if necessary, and that they will be reported appropriately. This involves the **evaluation** of the **necessity** of a change and the assessment of its **consequences**. The primary objective is to avoid reasonless project breaks, budget excess and uncontrolled time-schedule extensions, and for that purpose a number of internal

Funded by the Horizon 2020 Framework Programme of the European Union

and external risks were identified even from the beginning of the project and will be constantly be updated (See section 2.5 “List of Identified Risks”); these are described in the following subsections.

Internal risks will be minimized and managed by using well-established methodologies for project planning and project control. The splitting of project work into individual packages also minimizes internal risks. The Project Coordinator in cooperation with the Technical Coordinator and other project management roles will be mainly responsible to handle internal risks and inform all partners when necessary. The management of external risks lays primarily on the hands of the PCT. External risks will be minimized by following closely on technological and business development in the field as well as on pertinent regulatory issues.

4.2 RISK IDENTIFICATION

Risk Identification is the first key activity that examines each element of the program to identify associated risks and set the stage for their successful management. The risks that will be documented in the context of ASSURED will be classified according to their probability and severity following the below **three axes**:

- **administrative and organization risks**: including lack or shortage of availability of key resources, withdrawal of the participation of a partner having a key role, lack of communication;
- **technical implementation risks**: including methodologies and tools replacement issues, inadequate tools integration and collaboration, inadequate project results; and
- **communication and business risks**: like low interest of the targeted community / stakeholders, insufficient impact in standards liquidation of a partner business during the course of the project.

A baseline set of risks shall be identified and entered as risk statement through a Risk Information Form. Each risk is identified by number (for configuration control) and have a responsible partner/person (s) assigned as risk owner which is primarily the related WP Leader uness indicated otherwise. The risk owner has the overall responsibility for risk management activities until final closure of the risk.

4.3 RISK ASSESSMENT AND ANALYSIS

Once the Risks have been identified they should be analysed and assessed as to the likelihood (what’s the “chance” it will go wrong) and consequence of occurrence (what’s the “effect” on the project if it does go wrong).

The level of likelihood of each risk is established utilizing the following specific criteria.

TABLE 4: LEVEL OF RISK LIKELIHOOD

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low likelihood	~30%

Funded by the Horizon 2020 Framework Programme of the European Union

3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

The level of consequence of each risk is established utilizing a number of criteria related to a concrete situation or a recognized hazard. Finally, the overall impact is assessed, and the level of consequence is calculated as follows:

TABLE 5: LEVEL OF RISK CONSEQUENCE

Level	Impact of occurrence
1	Negligible
2	Minor
3	Moderate
4	Significant
5	Severe

Each partner should contribute to the risk assessment process by the definition and the identification of the different kind of risks. The collection and classification of the risks needs specific description and formulation in a unique matrix for each subsystem/module, in order to make feasible their systematic analysis. The following matrix calculates quantitatively the risk "score" as illustrated in the matrix below. The matrix is not symmetric as consequence values are weighted more than likelihood values.

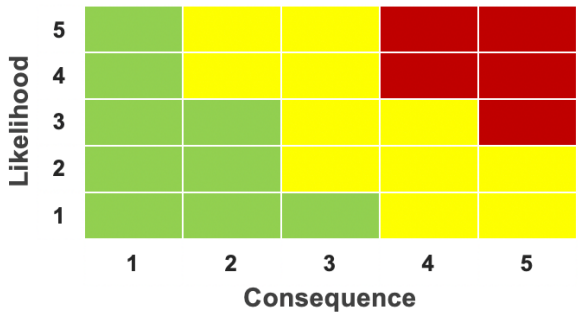

FIGURE 4: ASSESSMENT OF THE IDENTIFIED RISK ACCORDING TO ITS LIKELIHOOD AND CONSEQUENCE LEVELS

The following table converts the score to a qualitative risk assessment.

Funded by the Horizon 2020 Framework Programme of the European Union

TABLE 6: RISK SCORE ASSESSMENT

Risk level	Definition
LOW	Has little potential to cause disruption of schedule, increase in cost, or disruption of performance. Normal company effort will probably be able to overcome difficulties
MODERATE	Can potentially cause some disruption of schedule, increase in cost, or disruption of performance. However, special effort will probably be able to overcome difficulties.
HIGH	Likely to cause significant serious disruption of schedule, increase in cost, or degradation of performance even with special effort and close monitoring of the contracting activity.

Severity defines the effects and consequences; a project may face in case of risk occurrence. The severity may be influenced by various risk triggers arising from the project environment, consortium characteristics, external effects, technological breakthroughs etc. and may affect the technological and financial performance as well as the schedule of the project. [3]

- **Marginal** – Risk has relatively little impact on the project's technological and financial performance as well as the schedule
- **Critical -** Risk has the potential to impact the project's technological and financial performance as well as the schedule
- **Catastrophic –** Risk has the potential to greatly impact the project's technological and financial performance as well as the schedule

Classifying risks with the indicated scale, allows the appraisal of any action that might be needed. The qualitative analysis further includes the assessment if the risk is (still) relevant (yes/no), if the risk did materialise as well an as update of the risk. This is needed as basis for the decision if any measures need to be taken in a further step. The description of the current risk status also supports the deeper understanding and specification of the risk. At this point quantitative elements step into. The detailed assessment of the risk may include explanations of further effort requests, additional expenses, etc. needed to deal with the risk consequences, which makes it quantitatively measurable.

The practical implementation of the qualitative and quantitative analysis within the ASSURED project can be found in Chapter 5.

4.4 RISK MITIGATION

Risk mitigation planning identifies, evaluates, and selects options to lower risk at acceptable levels given program constrains and objectives.

This can be accomplished through reduction in likelihood, reduction in consequences, or a combination of both. It includes the specifics of **what** should be done, **when** it should be accomplished, **who** is responsible, and the **resources** required to implement the risk mitigation plan.

Funded by the Horizon 2020 Framework Programme of the European Union

4.5 RISK MITIGATION PLAN IMPLEMENTATION

The next key activity is the Risk Mitigation Plan Implementation which ensures successful risk mitigations occurs. It:

- Directs the teams to execute the defined and approved risk mitigations plans,
- Outlines the risk reporting requirements for on-going monitoring and
- Documents the change history.

Implementing risk mitigation should be accomplished by risk category (technical performance, schedule, cost) and it's important for this process to be worked through the Work-Breakdown Structure (WBS) level to scrub and endorse the risk mitigations of lower levels. It is important to mitigate risk where possible before passing it up to the next WBS level.

4.6 RISK TRACKING

The final key activity is risk tracking which is the activity of systematically tracking and evaluating the performance of risk mitigation actions. The PCT monitors progress and regularly updates risk status and information. Risk tracking is actually a feedback procedure where risk abetment plans may be revised or updated based on risk status update. If the plan is not effective, alternative plans must be put in place to ensure that risk is appropriately handled.

A project **Risk Register** is to be kept and reviewed at the Consortium meetings. For each identified risk the Risk Register shall detail at least:

- Risk title;
- Risk description;
- Description of the risk impact;
- Log date;
- Likelihood;
- Its potential consequence on the project;
- Work package in which the risk is managed;
- Risk owner;
- Risk status (Open / Occurred / Not occurred / Cancelled);
- A list of envisaged solutions / mitigation plan
  - action number
  - action description
  - target date for action
  - current action status
- The deadline for decision;
- Progress / comments.

Funded by the Horizon 2020 Framework Programme of the European Union

4.7 RISK BASELINE

The ASSURED consortium partners have realized that they take the responsibility of an ambitious, innovative project with major strategic impact. As a result, a preliminary list of identified risks along with their contingency planning is presented in Section **1.3.5 *WT5: Critical Implementation risks and mitigation actions*** *of* ***Part A of the GA*** **(See section 2.5 page 15)**.

4.8 INTERIM MANAGEMENT REPORTS

Interim Management Reports (IMR) serve as continuous internal quality control and risk monitoring and assessment tool. IMRs have been established by the coordinator MARTEL, in order to ensure that the work progress and the efforts spent are reasonable and in line with the expectations. It also supports the early recognition of deviations and potential risks for the project. In order to use the IMRs also as preparation for the Periodic Reports, the partners update dissemination and exploitation activities as well, which also implies the continuous update of the project website and social media accounts. The structure of the IMR includes reports on the following key points:

- Explanation of the work carried out by the beneficiaries and overview of the progress including use of resources and deviations;
- Dissemination, Exploitation, Standardization and Cooperation activities;
- Risk Assessment;

The structure proved to be effective in various projects and turned out as an easy management tool accepted by all project partners. The IMR requests partner inputs after each 6 months. It is collected and compiled by MARTEL. The cumulative outcome gives an overview to all partners about ongoing project issues and makes them aware of potential upcoming challenges.

Further, the IMR allows a check if the partners' work is performed as planned in the DoA. This also minimizes the risk of underperforming partners, deviations in terms of efforts and allows early detection of potential delays. Furthermore, regular progress telephone conferences give an update on the WP status and the partners' work, which allows the assessment and identification of further risks and timely corrective actions if needed.

The effort reported (PMs/partner/WP) in the IMR is collected in a cumulative table over the quarters, which generates diagrams for a swift and easy understanding of over- and under spending of resources per partner as well as on WP level. In this way the critical key indicators in terms of efforts are presented at one glance and possible actions can be taken in due course.

Risk assessment includes the evaluation of the already stated risks according to the current status of the project by the WP leaders as well as the additions of unforeseen or potentially upcoming risks. Those inputs were included into the overall risk map and due to the evaluation, it will then be decided if it is necessary to request measures (risk handling) or to iteratively continue with the analysis and monitoring process.

Funded by the Horizon 2020 Framework Programme of the European Union

5 MANAGING ASSURED RISKS

This chapter illustrates the implementation of the previously described risk tools into the ASSURED project structure. It presents the defined risks, shows the development of the risks based on probability & severity/impact estimations at several evaluations and tries to assess the current status of the risk. As the WP leaders are the main responsible persons for the risks of their WPs, this section is built up on WP level.

As described in detail in Chapter 4, a probability/severity analysis is used to qualitatively evaluate the risk status. The scale for probability has been defined as low, moderate or high. The scale for severity/impact has been defined as marginal, critical and catastrophic. The scale for probability and severity/impact is described in the table below.

TABLE 7: PROBABILITY/SEVERITY MATRIX

	Low	**Medium**	**High**
Probability	Less than *<30%>* probability of occurrence	Between *<30%>* and *<70%>* probability of occurrence	More than *<70%>* probability of occurrence
	Marginal	**Critical**	**Catastrophic**
Severity/Impact	Risk has relatively little impact the projects technological and financial performance as well as the schedule	Risk has the potential to impact the projects technological and financial performance as well as the schedule	Risk has the potential to greatly impact the projects technological and financial performance as well as the schedule

Risks with a high level of probability and/or severity are monitored very closely. They are subject to review within monthly progress telcos. Furthermore, the project management team is in contact with the WP leader in order to monitor the development of such risks.

The detailed risk assessment on WP level was performed two times during the first project year, in June 2021 there was the most recent assessment. **So far two risks identified prior to the project start materialised and one new risk has been identified during the first project year.** The detailed risk assessment will be available in the first periodic report after M18, due to the fact that this deliverable is public.

In the future the risk assessment on WP level will be performed on a quarterly basis. In order to support the WP leaders to perform the risk assessment and to help them fill in the complex risk assessment template, MARTEL illustrated the risk assessment process shown in Figure 5. According to the given answers the WP leads have to fill in different questions.

For example:

- If the risk materialised the WP leads have to fill in also the questions: **h)** Explain the reason why it materialised? & **i)** What are the consequences? & **j)** What are the corrective actions & updated mitigation measures?

If the risk did not materialise the WP leads do not have to fill in these further questions.

Funded by the Horizon 2020 Framework Programme of the European Union

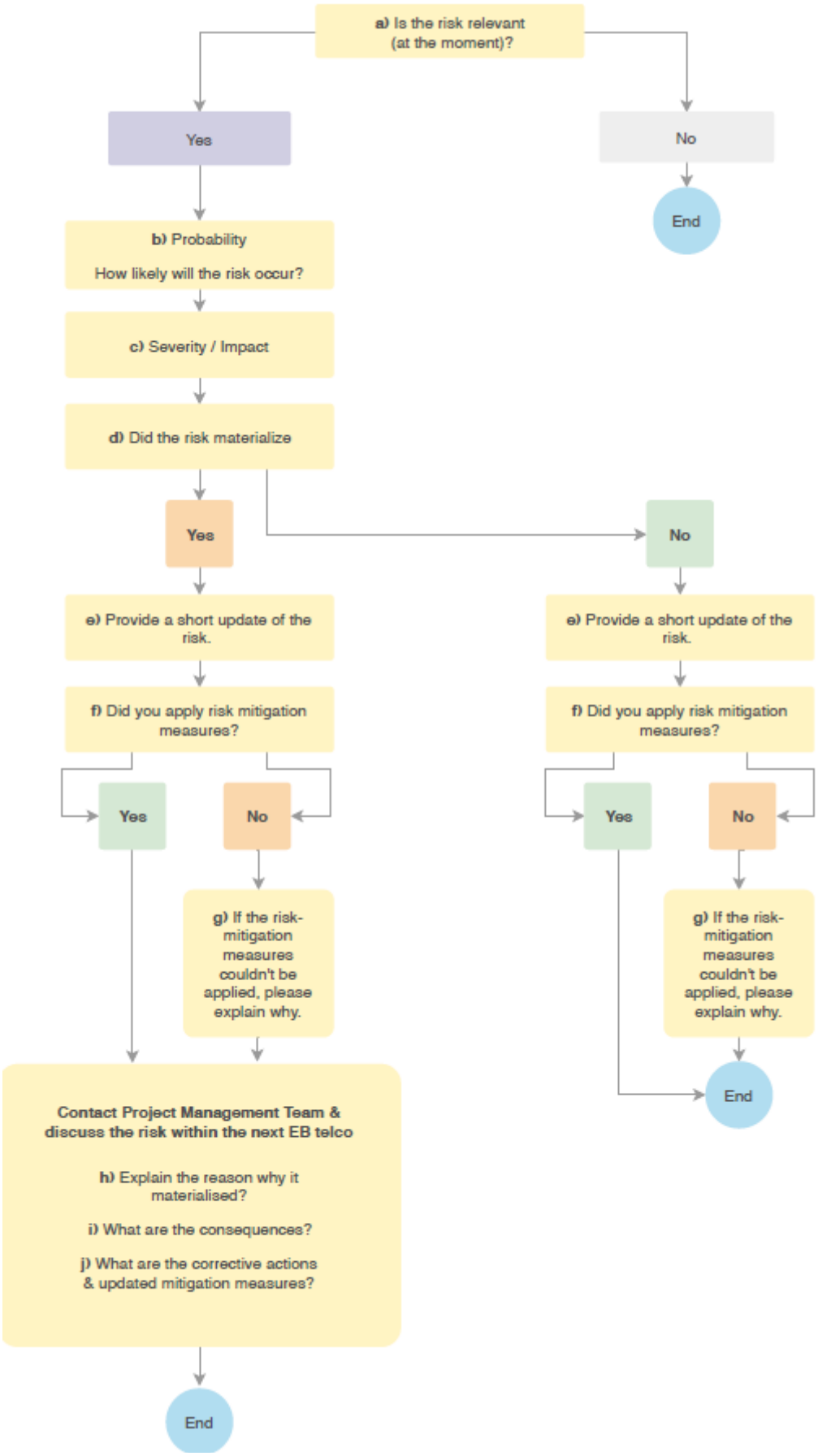

FIGURE 5: ASSURED RISK ASSESSMENT PROCESS

Funded by the Horizon 2020 Framework Programme of the European Union

In the following sub-chapters, the risk assessment of each WP will be described shortly. As mentioned before due to the fact that this deliverable is a public report, a detailed risk assessment report will be available in the first periodic report of the ASSURED project (after M18).

5.1 WP1 REQUIREMENTS AND CHARACTERIZATION OF ASSURED FRAMEWORK

Duration: M01-M12; WP Lead: UBITECH

Within WP1, which is led by partner UBITECH, there were three risks identified prior to the project start. None of the risks has materialized since the beginning of the project and no new risk has been identified so far. The probability of occurrence has been assessed as medium for two of the identified risks, for one it was assessed to be low. The level of severity is medium for all three risks and all three risks are still relevant although WP1 ends in M12 of the project. For all of the risks appropriate mitigation measures have been developed, so that none of the risks will materialize in the future.

5.2 WP2 MULTI-DEPENDENCY CYBER-PHYSICAL RISK ASSESSMENT, FORECASTING AND COMPLIANCE

Duration: M07-M30; WP Lead: UBITECH

WP2 has six pre-defined risks that were assessed by the WP lead UBITECH. The probability to occur has been assessed as low for four of the six risks. For one risk the probability to occurrence has been assessed as medium. Also, the level of severity was assesed in the last evaluation for two risks as marginal, for the risk "*RA methodology not completed*" (Risk # 13 in Table 3) it is critical. For all of the risks appropriate mitigation measures have been developed and actions are being taken in order to minimise the risks.

5.3 WP3 DISTRIBUTED ATTESTATION-ENABLED CPS ORCHESTRATION AND EXECUTION

Duration: M07-M30; WP Lead: TUDA

WP3 has seven pre-defined risks that were assessed by the WP lead TUDA. The probability for five of those to occur has been assessed as low. For one risk (Risk #9 in Table 3) the probability for occurence has been assesed as moderate depending on the type of attestation scheme/service for which system data needs to be traced. For instance, regarding Configuration Integrity Verification (CIV) and in general the attestation of static properties [6], the probability of this risk to materialize is low. In the case of control-flow attestation, since the goal of the ASSURED tracer component is to be purely sw-based, this might incur additional overhead. However, the ASSURED consortium has already identified possible mitigation actions (as described in D1.2 [7]) towards the usage of a "hybrid" tracing mechanism which will sit in the interesection of sw- and hw-based solutions.

Another risk (Risk #20 in Table 3), the probability for occurence has been assessed as moderate especially for two of the use case, namely the "Public Safety" and "Secure Aerospace" use cases. However, the mitigation plan of the consortium is to leverage Rapsebrry Pis – as program Logic Controllers (PLCs) – attached to the deployed edge devices for being

Funded by the Horizon 2020 Framework Programme of the European Union

able to execute the ASSURED services. This will also be part of the overall evaluation of the ASSURED framework and remote attestation services.

5.4 WP4 BLOCKCHAIN-BASED ASSURED SUPPLY CHAIN CONTROL SERVICES AND TRUST EVIDENCE COLLECTION

Duration: M07-M30; WP Lead: TUDE

Within WP4, which is led by partner TUDE, there were five risks identified prior to the project commencement. None of the risks has materialized since the beginning of the project and no new risk has been identified so far. The probability for all risks was assessed as low and the level of the severity was assessed as marginal.

5.5 WP5 ASSURED FRAMEWORK INTEGRATION

Duration: M07-M30; WP Lead: INTRASOFT

Risks within WP5 are being evaluated by the WP leader INTRASOFT. During the creation of the proposal, there was only one risk identified for WP5. The probability for this risk was assessed as low and the level of the severity was assessed as marginal. Due to appropriate risk mitigation measures the risk did not materialize and no new risk has been identified within WP5.

5.6 WP6 ASSURED USE CASES DEMONSTRATORS & PERFORMANCE EVALUATION

Duration: M01-M36; WP Lead: SPH

Within WP6, which is led by partner SPH, there were four risks identified prior to the project start. None of the risks materialized since the beginning of the project and one additional risk has been identified so far. Essentially, this is a specific instantiaion of Risk #19 (Table 3) that is related with the system support from the demonstrators: Dure to the complexity of the remote attestation enablers to be tested, in the context of ASSURED, that require the presence of a specific trusted computing base ([5]) at each host device, there have been discussions within the consortium on what would be the best camera platform/device to be procurred in the context of the “Public Safety” use case and whether this could support the execution of the envisioned remote attestation services. There have been identified adequate options (e.g., cameras equipped with Jetson, connection of existing cameras by the leading use partners – DAEM – to Rapsberry Pis for executing the ASSYRED services) but a separate riks has been added so as to better monitor its progress. The probability to occur has been currently assessed as mediocre and the level of severity is marginal. For all of the risks appropriate mitigation measures have been developed and actions are being taken in order to minimise the risks.

5.7 WP7 DISSEMINATION, COMMUNICATIONS, STANDARDIZATION, EXPLOITATION AND TRAINING

Duration: M01-M36; WP Lead: MARTEL

Funded by the Horizon 2020 Framework Programme of the European Union

Within WP7 led by the partner MARTEL, there were three pre-defined risks that are specifically applicable to this WP. Generally, most of the risks were evaluated as low or medium in probability and negligible to marginal in severity level. None of the risks has materialized, mainly because of continuous excellent cooperation and open communication among partners. No new risks have been identified by the WP leader. The defined risk mitigation measures were not needed yet.

5.8 WP8 PROJECT RISK AND INNOVATION MANAGEMENT

Duration: M01-M36; WP Lead: MARTEL

There are six pre-defined risks within WP8 that were already identified during the proposal phase. Later on, during the first few months of the project, a new risk has been identified and allocated to the WP. At the same time however, a mitigation measure was proposed and implemented in order to prevent the risk from occurring. All risks are on low probability and marginal to critical severity.

At the beginning of the project, two risks materialized: Risk #7 (Table 3) “Partner Withdrawal” where the partner Technical University of Eindhoven (TUE) withdrew from the project. TUE’s main expertise was on the design of cryptographic algorithms and security mechanisms to work on top of the Blockchain infrastructure towards the secure data sharing of information in the context of supply chains (WP4). After following all of the steps identified in the Project Handbook, the consortium agreed to onboard the Technical University of Delft (TUDE) where Dr. Kaitai Liang (prior member of University of Surrey) had recently moved. SURREY, and more specifically Dr. Kaitai Liang, was the other core partner to lead the Blockchain-related research activities in the context of WP4, thus, the transition of WP4 leadership (from TUE to TUDE) was smooth and did not affect the project progress.

Finally, Risk #5 (Table 3) on “Change of Personnel” materialized where on top of Dr. Liang’s transition to TUDE, the Scientific Coordinator of the project moved from Technical University of Denmark (DTU) to UBITECH. Since UBITECH was already a member of the consortium, this switch did not affect the project operation since the technical coordination of the overall project was shifted from DTU to UBITECH.

Funded by the Horizon 2020
Framework Programme of the European Union

6 CONCLUSIONS

This report consists of the ASSURED “Risk Assessment Plan” and is the single point of reference on the risk approach that will be governed during the course of the project. It covers all aspects related to; the overall risk management strategy and approach; the risk management, reporting, monitoring and mitigations that will be implemented throughout the course of the project.

This report is a live document that will be updated as necessary during the lifetime of the project.

Funded by the Horizon 2020
Framework Programme of the European Union

REFERENCES

[1] Holland & Holland Enterprises Ltd. (2013): Project Risk Management, online: http://www.successful-project-management.com/project-risk-management.html

[2] Alon, Adi/Koetzier, Wouter/Culp, Steve (2013): The art of managing innovation risk, online: https://www.accenture.com/us-en/insight-outlook-art-of-managing-innovation-risk.aspx

[3] ISO 31000 (2009): Risk management, online: http://www.iso.org/iso/home/standards/iso31000.htm

[4] PMBOK (2004): A Guide to the Project Management Body of Knowledge, published by Project Management Institute; Newton Square, Pennsylvania (USA)

[5] The ASSURED Consortium, “ASSURED Attestation Model and Specification”, September 2021.

[6] The ASSURED Consortium, “Operational SoS Process Models & Specification of Properties”, September 2021.

[7] The ASSURED Consortium, “ASSURED Reference Architecture”, March 2021.

Funded by the Horizon 2020 Framework Programme of the European Union