D6.1 Project management strategy: Project Handbook

WP6. Project Management

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 31-OCT-2016

Actual submission date: 25-OCT-2016

© CIPSEC Consortium

HORIZON 2020. WORK PROGRAMME 2014 – 2015			Project No	700378
Call			Instrument	Innovation action
Digital Security: Cybersecurity, Privacy and Trust			Start date	May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens			Duration	36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection			Website	www.cipsec.eu
Public	Confidential	Classified	Lead contractor Atos SPAIN S.A.	

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The opinions expressed and arguments employed in this document do not necessarily reflect the official views of the Research Executive Agency (REA) nor the European Commission.

This deliverable has been endorsed by Security Advisory Board.

Document contributors

Editor	Fernando Carmona (Atos)	
Contributors		**Reviewers**
	AEGIS	
Elsa Prieto	ATOS	
	BD	
	COMSEC	Amir Atzmon
	CSI	
	DB	
	EMP	
	FORTH	Sotiris Ioannidis
	HCPB	
	TUD	
	UPC	
	UOP	
	WOS	

Document history

Version	Date	Author	Notes
0.1	01-08-2016	Fernando Carmona (ATOS)	First draft.
0.2	04-08-2016	Elsa Prieto (ATOS)	Sections introduction. Project roadmap. Specific decision making procedures.
0.3	08-08-2016	Sotiris Ioannidis (FORTH)	General review. Risk assessment.
0.4	10-10-2016	Amir Atzmon (COMSEC)	General approval.
0.5	25-10-2016	Fernando Carmona (ATOS)	Heraklion agreement and final check.

Index

1 Executive summary

CIPSEC is a complex project in terms of both the structure of the Consortium and the workflow between the partners. Because of that, management, coordination and quality assessment issues should be detailed as much as possible. This deliverable, D6.1 Project Handbook, describes CIPSEC approach of implementing an appropriate management and quality assessment framework, addressing general issues regarding project structure, organization, and control, partner responsibilities as well as specific guidelines about internal procedures, risk assessment and communication mechanisms.

- Describe the innovation framework.
- Monitor the progress of the work and overall project status on a regular basis.
- Facilitate decision-making and conflict resolution.
- Identify, assess, mitigate, and communicate potential risks and relevant issues during the project lifecycle.
- Detail how and when the documentation or software has to be exchanged by the Consortium partners.
- Set editorial standards for project document contents and guidelines to ensure the quality of the project outputs.

This document will function as a manual and reference document for the project partners to reach a common understanding of project procedures in order to efficiently execute it with the maximum quality, so that technical, societal and scientific project objectives can be achieved.

2 Introduction

2.1 Purpose of the document

This document stands for the overall Management Plan for CIPSEC. It defines procedures for ensuring that all project activities for planning, designing and implementing CIPSEC are effective and efficient with respect to the purpose of its objectives and its expected performance.

2.2 Relation to other project work

Project management is a continuous process through the whole project lifecycle, not just related to the schedule and delivery of project assets, but also about foreseeing, preventing, and avoiding contingencies by means of preparing actions to mitigate and counteract risks. Project management encompasses a set of activities related to:

- Progress / Completion. Progress and cost reporting for each activity and for the overall project.
- Communication procedures.
- Quality assurance / Validation plan.
- Risk assessment / Contingency plan.
- IPR management.

Management Plan is closely bond to other management deliverables and contractual documents:

- Consortium Agreement (CA).[i]
- Grant Agreement (GA) – Description of Action (DoA).[ii]
- D6.2 CIPSEC annual report on project management (Year 1) (expected Apr-2017).
- D6.3 CIPSEC annual report on project management (Year 2) (expected Apr-2018).
- D6.4 CIPSEC annual report on project management (Year 3) (expected Apr-2019).

2.3 Structure of the document

This deliverable consists of five main sections:

- Chapter 3 is comprehensive of CIPSEC project objectives and scope, showing out a quick reference of project work packages and deliverables and a brief introduction to CIPSEC Consortium.
- Chapter 4 describes the general management procedures that should be followed to ensure project objectives are met. These include the management structure and control, decision-making procedures, project monitoring, documentation guidelines, financial and administrative reporting, and intellectual property rights discussion.
- Chapter 5 focuses on the Quality Assurance activities, regarding both project assets: Documentation and Software. It includes all the planned and systematic activities implemented to provide confidence that the project will satisfy the relevant quality standards. Quality Assurance will be performed throughout the project as a continuous process.
- Chapter 6 defines the Risk Assessment process that will be followed in order to identify, communicate, and deal with events that could have a negative impact on the normal project course.
- Finally, chapter 7 introduces the innovation management process.

3 CIPSEC project

3.1 Introduction

The project CIPSEC (standing for "Enhancing Critical Infrastructure Protection with innovative SECurity framework") is a three-year multi-disciplinary, Innovation Action co-funded by the European Commission in the context of Horizon 2020, the EU Framework Programme for Research and Innovation, started on May 1st 2016 and will end on April 30st 2019.

CIPSEC is framed within Work Programme 2014 – 2015 and belongs to the DS-3-2015 call: The role of ICT in Critical Infrastructure Protection.

Specific challenge
Industrial and Automation Control Systems (IACS).They are no longer isolated siloes but are fully integrated with corporate IT infrastructures. An attack to IT assets can spread to the OT environment jumping to SCADA and Control Centres. Much vulnerability of critical infrastructures, including the communication networks, stems from the fact that ICT systems are deployed in an environment or for an application that was not designed with security in mind.
Scope
■ Investigate the dependencies on communication networks and ICT components (including SCADA and IACS systems) of critical infrastructures ■ Analyze and propose mitigation strategies and methodologies for assessing criticalities of services and detecting anomalies. ■ Developing tools and processes to simulate or monitor cascading effects due to ICT incidents. ■ Develop self-healing mechanisms. ■ Retrofit state-of-the-art security into networks.
Use cases
The investigated concepts have to be tested in a field trial (e.g. health, finance, energy, transport,…)
Participants
■ ICT operators (e.g. telecom operators) have experience in securing information networks and this competence can be applied to new types of networks such as smart grids linking communication, energy and transport networks. ■ In relation to the protection of legacy IACS, SMEs are particularly encouraged to provide specific and very focused security solutions adapting current ICT security technology to IACS environments on topics such as: • Early anomaly detection and compliance management. • Patching and updating equipment without disruption of service and tools. • Improved forensic techniques for supporting criminal law enforcement. • Anti-malware solutions with special focus on managing third-parties (e.g. maintenance and support service providers, IACS vendors, etc.) • Proactive Security Systems able to counteract Denial of Service attacks (distributed or not) and other type of attacks aimed to the IACS network disruption.

Expected Impact	
■ Resilient and robust communication networks offering a reduced attack surface to the supported critical infrastructures. ■ Reduced criticality of ICT components installed in critical infrastructures. ■ Increased preparedness, reduced response time and coordinated response in case of a cyber-incident affecting communication and information networks. ■ Reduced possibilities to misuse ICT as a vehicle to commit cybercrime or cyber-terrorism.	■ Where relevant, the supported activities should support the work of the European Program for Critical Infrastructure Protection (EPCIP). ■ The outcome of the proposal is expected to lead to developments up to Technology Readiness Level (TRL 7) or above; (Innovation Actions may include prototyping, testing, demonstrating, piloting, large-scale product validation and market replication).

3.2 Challenges

CI (Critical Infrastructures) networks nowadays have too many connections between their Information Technology (IT) and Operational Technology (OT) environments. While IT world has been gaining significant experience in protecting computer networks, OT departments have been traditionally focusing on lowering the cost and creating business opportunities, not realizing that the additional networking capabilities exposed them to a wide range of possible attacks.

Therefore, there is a double need for a flexible unified CI system able to collect and process data from diverse inputs and for a security ecosystem that goes beyond the borders of a single CI. Ability to easily integrate (i.e. plug n' play) heterogeneous security systems and components is also required.

To sum up, a CI security system must offer services (security studies and best practices, partnerships, cascading effect solutions, contingency plans, vulnerability tests, etc.), training courses and certification.

3.3 Objectives

Keeping this challenges in mind and considering that CI providers are general reluctant to cooperate on matters of sharing information about attacks on their systems, CIPSEC intends to create a unified security framework that orchestrates state-of-the-art heterogeneous security products and services to offer high levels of protection in IT and OT departments of CI. As part of this framework, CIPSEC will offer a complete security ecosystem of additional services: vulnerability tests and recommendations, CI technicians training courses, public-private partnerships (PPPs) for advanced contingency plan, forensic analysis, preliminary certification, and protection against cascading effects

3.3.1 Objective 1 (O1). Unified security framework for CI

There is a need for complete security solutions adjusted to the very specific requirements of CI environments. These solutions must be able to collect and process input and data from heterogeneous sources and allow easily integration of external market products that offer high-quality, specialized solutions.

- Allow easy integration of heterogeneous systems to the CIPSEC framework with minimum required modification.

  CIPSEC will handle CIs as comprehensive entities that require complete solutions but will create a flexible unified security framework that will be able to orchestrate diverse products of high quality created by different providers and experts on ICT security and network management. The goal is to create a system that provides robust security but, at the same time, it is easy to use. For the same objective, CIPSEC will also evolve market security products with innovative research enhancements and align CIPSEC products and services with current security standards and regulations.

- **Anomaly detection** and compliance management.

ATOS innovation factor	ATOS will connect XL-SIEM platform with a variety of systems, improving its detection capabilities and support for additional data formats.

- **Anti-malware**: URL filtering, firewalls, anti-spam, anti-phishing, online threat detection, etc.

Bitdefender Innovation factor	Within the CIPSEC project, Bitdefender cloud will be connected with diverse products and services to improve their detection rate, correlate some of the events with other ones identified from other sources and adapt their heuristics and whitelisting methods accordingly. Also, some of the Bitdefender Machine Learning technologies will be adjusted for a better detection rate and fewer false positives based on input received from CIPSEC. The network traffic analysis system will be improved and adjusted to various types of exploits or URL based malware such as botnets, ransomware etc.

- **Cyber-security**: firewalls with intrusion detection/prevention, data protection, etc.
- **Distributed Denial of Service**.
  - Honeypots sensors (defence against cyber-attacks).
  - PHY-layer to discard non-intended or malicious packets (defence against exhaustion attacks on M2M low-power networks).
  - Real-time signal detector to identify anomalies and location of wireless devices (defence against jamming attacks on the context of M2M low-power networks).

FORTH Innovation factor	Providing an easily installed and maintained attack detection system to CIPSEC users/administrators. FORTH also plans to cross-check the results produced with other online external sources (online blacklists and whitelists) in a transparent way for the user/administrator of the system.
WOS Innovation factor	WOS will adapt a novel authentication scheme able to discard non-intended and/or non-legitimate packets just after the reception of the physical preamble, improving mitigation of exhaustion attacks, by including it in the communication protocol stack for the provided M2M devices. WOS will also add an adaptation upon Bitcarrier (jammer detector) for identifying possible DoS threats in a short range of time.

- **Hardware security**.

EMP Innovation factor	Based on Secocard, secure communication and authentication applications for a huge variety of purposes have been developed and more can be added. The device can be a smartcard and in parallel act as a smart card reader. Applications include Secure Cloud Sign-On, VPN Sign-On, Voice Encryption, Email Encryption, Secure Banking & Payment (online & mobile) etc.
UOP Innovation factor	The developed prototypes will be protected against hardware security attacks like side channel attacks and fault injection attacks in a holistic manner.

- Collect and process input from multiple sources and provide monitoring for the complete CI (i.e., cross-layer methods). CIPSEC will initially focus on the data collection and processing. It will then examine more complicated features: updating patching, communication between components, etc.

3.3.2 Objective 2 (O2). Security ecosystem

With the Internet enabling distribution of services and components, CIs are no longer isolated, independent entities, and their security is influenced by multiple factors which sometimes reside outside their borders. The absence of a general security ecosystem, which could provide means, tools, practices, etc. to enable stakeholders (from public and private sector) to coordinate and collaborate, leaves everyone vulnerable and alone against sophisticated attacks with cascading effect that can harm multiple CIs.

- Create industrial control **system vulnerability tests and recommendations** including studies for cascading effect attacks. Studies will examine a) how to protect CIs from an attack happening in an external CI, and b) how to isolate an attack within a CI before it is spread outside its borders
- Establish baseline requirements for the security and resilience for the proposed experiments within the three pilots.
- Define several **contingency plans based on PPPs**.
- Provide **training** courses for the critical infrastructure technicians and certification. Training will include courses on the CIPSEC framework operation and also the behavior of employees in case of an emergency.
- Continuous solutions **updating / patching** of adopted security solutions by using existing and implementing new updating mechanisms.
- Create innovative **forensic techniques** to reach the sources of the problems when dangerous situations are detected.

AEGIS innovation factor	AEGIS Visualization Toolkit was intended to augment and facilitate the “after the fact” analysis of digital forensic evidence, by providing different ways to visualize data collected by the forensics experts. AEGIS will adapt its visualization toolkit so that it can be integrated into the real-time analysis proposed by CIPSEC.

3.3.3 Objective 3 (O3). Real CIs (transportation, health and environment pilots)

CIs are complicated systems with multiple departments and components. Enforcing a complete security solution is not an easy task. Each CI has its specific requirements and any proposed solution must be adjusted to its very specific needs and systems. Especially when this solution combines diverse heterogeneous subsystems.

- Validate our proposed solution under real conditions and infrastructures, implementing three different pilots on three different CI sectors: transportation, health and environment monitoring
- Identify which of CIPSEC partial solutions and products and services match the very specific security requirements of each CI sector.
- Orchestrate CIPSEC products and services to produce unique overall solutions adjusted to transportation, health and environment sectors.
- Conduct an evaluation of the developed solution in the real-world environment to qualitatively and quantitatively assess the performance gains introduced by the solution.
  - System modules level (in each industrial section and security aspect).
  - System level (the complete framework).

Environment

CIPSEC will offer vulnerability tests including cascading effect studies, contingency plans and PPPs, forensics and personnel training. One of the major test will be to deploy a cascading effect scenario where a malicious attacker takes control of a component from the air-monitoring system and then tries to gain access to the rest of the services of the Piedmont Region.

Health

CIPSEC will provide solutions to secure the overall OT system, keeping in mind that the hospital has requested vulnerability tests (including cascading effect studies) and personnel training. CIPSEC will clarify that the aforementioned solutions may be modified based on the in-depth analysis on the hospital's CI environment. For instance Worldsensing's Bitcarrier solution for wireless monitoring and wireless DDoS protection requires the installation of wireless devices which may cause interference problems or affect patients. We shall implement privacy-enhancing countermeasures building upon the methodology of statistical disclosure control, specifically, via anonymous micro aggregation techniques if any sensitive data is gathered in the pilot.

Transportation

Communication monitoring between field elements and the core interlocking system.

3.3.4 Objective 4 (O4). Links and standardizations bodies

CI providers are reluctant to cooperate on matters of sharing information about attacks on their systems. However only a coordinated effort between governments and the private sector including the definition of national and international policies, security standards, and strategies will result in higher levels of CI protection. CIPSEC recognizes that the harmonization of CI security solutions with policies and standards will ensure the quality of the proposed products and services and will also promote collaboration and communication between stakeholders.

- CIPSEC will consolidate our proposed solutions for transportation, health and environment monitoring with distinguished European links to ensure higher levels of quality.
- CIPSEC will work together with standardization bodies through its Advisory Board.
  - EPCIP (European Program for Critical Infrastructure Protection).
  - ERNCIP (European Reference Network for Critical Infrastructure Protection): "Case Studies for the Cyber-Security of Industrial Automation and Control Systems" and "Industrial Automated Control Systems and Smart Grids".

3.3.5 Objective 5 (O5). Ready to market

Cybercrime and attacks against CIs affect economy and business growth in multiple ways. However, a solution towards CI security must not be defined only around the aspect of cost savings from attack prevention / tackling. A solution will be successful and has more chances to be adopted if it promotes business activities and alliances, collaborations, access to new markets, etc.

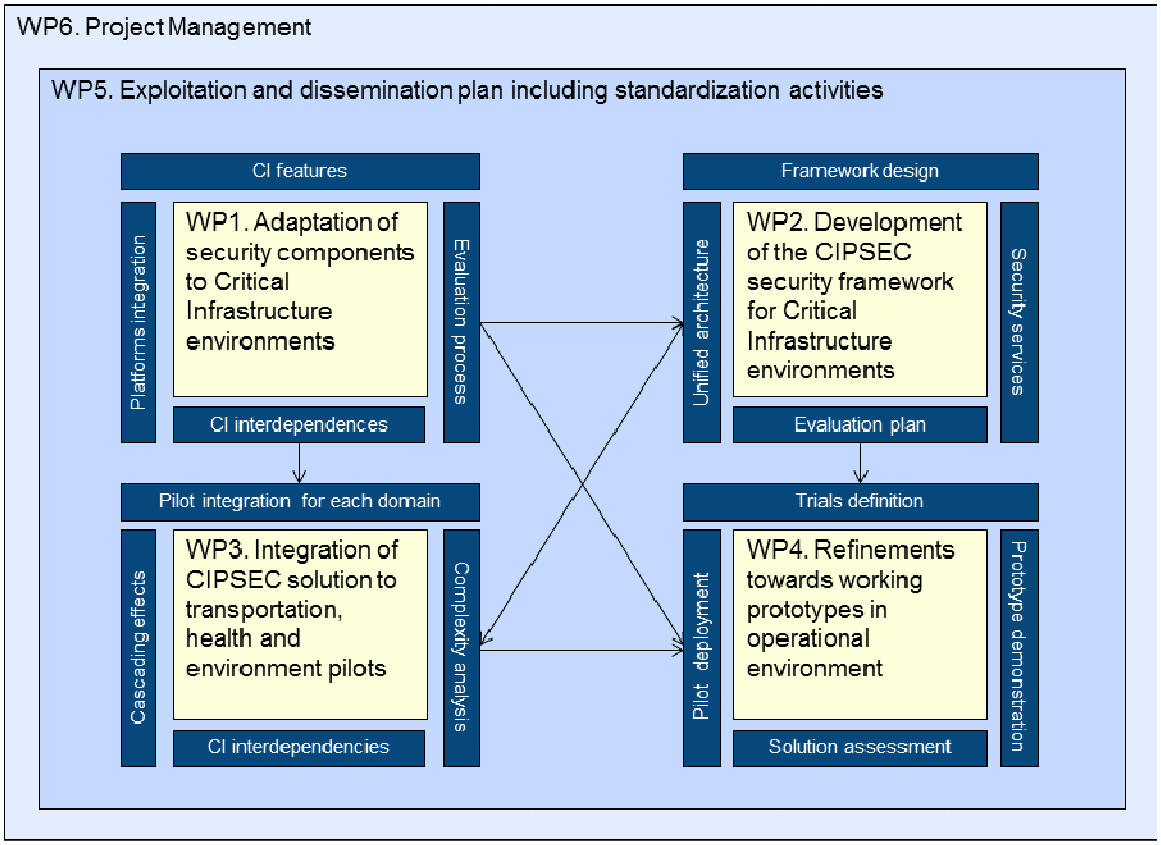
Investing in CI protection will not only support public safety and population welfare, but it will boost economy. CIPSEC will create positive business opportunities through its consortium and also through its proposed solution: The consortium brings together a large variety of diverse companies, enterprises and institutes promoting new collaborations, activities and innovation.

- Collaborations, activities and innovation within Consortium and with external companies, and research institutes.
- Security frameworks for transportation, health or environmental monitoring CIs TRL 7/8**.** Industrial partners will bring to the CIPSEC project their own market products services (up to TRL 8/9)
- Exploitation plan "after the project"-oriented. Key aspects: security system simplicity, threats identification, system downtime, cascading effect protection, orchestrated contingency plan, forensics analysis, and technician certification.

3.4 Roadmap

Work packages	Milestones (Month. Scope)
WP1. Adaptation of security components to Critical Infrastructure environments. WP2. Development of security framework for CI environments. WP3. Integration of CIPSEC solution to transportation, health and environment pilots. WP4. Refinements towards working prototypes in operational environment. WP5. Exploitation and dissemination plan including standardization activities. WP6. Project Management.	■ M3. Committees setting. ■ M6. Security analysis. Market review and analysis. Functionality building blocks. CI taxonomy. Exploitation and dissemination plan. Project management strategy. ■ M9. Architecture system design. ■ M12. Project report: First year. ■ M18. First release: preliminary version of the CIPSEC security platform. Preliminary report for pilots integration. Preliminary report on CI intra/inter- dependencies. ■ M24. Prototype ready for the operation environment tests. Adapted and optimized solution for the selected pilots. Final report on CIs intra/inter-dependencies analysis. List of policies for the CIPSEC prototype. Trials settings and configuration. Project report: Second year. ■ M27. System ready for the experimentation ■ M32. Prototype demonstration successfully conducted. ■ M34. The business model for impact creation and exploitation is ready. ■ M36. Final CIPSEC security framework. Final CIPSEC framework capabilities in TRL8: results evaluation. Final project quality demonstration: exploitation, dissemination and standardization report. Project report: Third year.

3.5 Quick reference



WP1	**Adaptation of security components to Critical Infrastructure environments** **FOR** CIPSEC will perform an in depth analysis into the CI environments of the pilots and also the characteristics of CIs in general. This process will identify the critical assets and components and also their vulnerabilities, interdependencies, configurations, etc.			
	D1.3 Report on taxonomy of the CI environments			M6
T1.1 In depth security analysis for CIPSEC pilot's CIs	M1-M6	BD AEGIS, ATOS, CSI, DB, EMP, FORTH, HCPB, TUD, UPC, UOP, WOS		
Basic characteristics of the various CI environments: Three CI environments that are related to the pilots & alternative domains.				
T1.2 Evaluation of CIPSEC market products in relation to CIs and pilots needs	M1-M6	COMSEC AEGIS, ATOS, BD, FORTH, TUD, UOP, WOS	D1.1 CI base security characteristics and market analysis report	M6
Evaluation process will consider robustness, availability, reliability, usability, effectiveness, privacy, cost, timely responsiveness and other aspects.				
T1.3 Requirements of integrating heterogeneous products into unified solutions	M1-M6	UPC ATOS, CSI, FORTH, TUD, UOP	D1.2 Report on functionality building blocks	M6
Analyzing the pilots: individual unique characteristics or overlapping. Classes of common features for creating functionality basic blocks capable for different CI domains.				
T1.4 Interdependences of CIs	M1-M6	CSI ATOS, BD, FORTH, TUD, UPC, UOP		
Taxonomy of different CI environments: differences and common aspects. Functional prerequisites for collaboration between different CIs and CI domains.				

<table>
<tr><td>WP2</td><td colspan="5">Development of the CIPSEC security framework for Critical Infrastructure environments ATOS
In WP2 the academic & industrial partners will work together to provide research innovations to some of the product solutions and market products.</td></tr>
<tr><td colspan="2" rowspan="3">T2.1 CIPSEC security framework design, integration and optimization – prototype</td><td rowspan="3">M1-M24</td><td rowspan="3">ATOS
AEGIS, COMSEC, CSI, DB, FORTH, HCPB, TUD, UPC, UOP</td><td>D2.1 CIPSEC System design</td><td>M9</td></tr>
<tr><td>D2.2 CIPSEC Unified Architecture – First Internal Release</td><td>M18</td></tr>
<tr><td>D2.5 Final Version of the CIPSEC Unified Architecture and Initial Version of the CIPSEC Framework Prototype.</td><td>M24</td></tr>
<tr><td colspan="6">Design driving factors will be identified based on WP1 and translated into functional and non-functional features. Requirements for the different usage scenarios, such as security capabilities, scalability, latency and others will be documented.
Agile development principles. In-lab tests, including reliability and vulnerability tests.
Interfaces. Investigation on how external tools can interoperate with the CIPSEC framework where applicable.
Preliminary business study, conducted in WP5, will influence this architecture design.</td></tr>
<tr><td colspan="2">T2.2 Enhancing CIPSEC market products with the latest research innovations</td><td>M7-M18</td><td>UOP
AEGIS, ATOS, EMP, FORTH, TUD, WOS</td><td>D2.3 CIPSEC products integration on the Unified Architecture</td><td>M18</td></tr>
<tr><td colspan="6">Road-map of the innovations to be included in the existing assets to cover the requirements identified in WP1 and WP5.
The definition of these enhanced assets will serve as a basis to define the first release of the unified architecture in T2.1 and the final complete and optimized security framework in T2.5.
Commercial products that will be evaluated are:
■ Cyber-security (networks firewalls, DDoS, etc.).
■ Early anomaly detection and compliance management (data aggregation, filtering, etc.).
■ Anti-malware (antispam, anti-phishing, etc.).
■ Hardware security (trusted arbiter for CIS nodes, etc.).
■ Denial of Service detector (Super-node, communication protocols, etc.).</td></tr>
<tr><td colspan="2">T2.3 CIPSEC security services</td><td>M7-M18</td><td>WOS
AEGIS, ATOS, CSI, FORTH, TUD, UPC, UOP</td><td>D2.4 CIPSEC services integration on the Unified Architecture</td><td>M18</td></tr>
<tr><td colspan="6">■ Industrial control system vulnerability tests and recommendations including studies for cascading effect attacks.
■ Ad-hoc contingency plan definition in partnership between public and private entities:
■ Training courses for the critical infrastructure technicians and certification:
■ Easy-friendly updating for the adopted security solutions by implementing patching mechanisms.</td></tr>
</table>

T2.4 Derivation and evaluation of default settings	M10-M24	COMSEC ATOS, BD, FORTH, TUD, UPC, UOP	D2.6 CIPSEC Evaluation Plan	M24
Fully operational CIPSEC. ■ Compliant with requirements (WP1). ■ Basis for the pilot preparation (WP3). ■ Demonstration activities during the real-life implementation (WP4). ■ Compliant with standards, and end-users and business requirements (WP5).				
T2.5 From the prototype to the final CIPSEC security framework	M22-M36	FORTH AEGIS, ATOS, BD, CSI, TUD, UPC, UOP	D2.7 CIPSEC Framework Final version	M36
Optimization of the prototype through the validation activities of WP4.				

WP3	**Integration of CIPSEC solution to transportation, health and environment pilots** **CSI** WP3 and WP4 will enable the validation of any prototype in operational environment for these products, ensuring that modified products are at least at TRL7			
T3.1 Security framework for transportation CIs	M10-M24	DB AEGIS, ATOS, COMSEC, CSI, EMP, FORTH, TUD, UPC, UOP, WOS	D3.1 Preliminary Pilot I Integration: Incident Discovery and Response for Railway use case	M18
			D3.5 Pilot I Integration: Incident Discovery and Response for Railway use case	M24
CIPSEC accommodation to the specificities and requirements for Pilot I, "German Transport" (Incident Discovery and Response for Railway).				
T3.2 Security framework for health CIs	M10-M24	HCPB AEGIS, ATOS, COMSEC, CSI, EMP, FORTH, UPC, UOP, WOS	D3.2 Preliminary Pilot II Integration: Hospital's Operational Technology Management System use case.	M18
			D3.6 Pilot II Integration: Hospital's Operational Technology Management System use case.	M24
CIPSEC accommodation to the specificities and requirements for Pilot II, "Spanish Health" (Hospital Operational Technology Management System).				
T3.3 Security solution for environmental monitoring CIs	M10-M24	CSI AEGIS, ATOS, COMSEC, EMP, UPC, UOP, WOS	D3.3 Preliminary Pilot III Integration: Air quality Monitoring System use case.	M18
			D3.7 Pilot III Integration: Air quality Monitoring System use case	M24
CIPSEC accommodation to the specificities and requirements for Pilot III, "Italian Environment Monitoring" (Air quality Monitoring System).				
T3.4 CIs intra- and inter-dependencies including cascading effects	M13-M24	CSI FORTH, TUD, UPC, UOP	D3.4 CIPSEC Intra/ Inter-dependencies Analysis Preliminary Report	M18
			D3.8 CIPSEC Intra/ Inter-dependencies Analysis Report	M24
■ How possible security breaches in the air quality monitoring network might affect other parts of the Public Administration regional network (Italian Pilot) ■ How industrial systems may effect on medical systems in an hospital environment (Spanish Pilot). Helping on the definition of the second release for the CIPSEC platform.				
T3.5 Complexity analysis and policies definition	M19-M24	COMSEC AEGIS, CSI, EMP, FORTH, TUD	D3.9 Complete Complexity Analysis	M24
Pros and cons of general solutions vs particular solutions for CI scenarios. Set of policies and rules to assess individual scenarios where general solutions might be not suitable.				

WP4	**Refinements towards working prototypes in operational environment** **WOS** Especially in WP4 CIPSEC will work on aspects like field configuration and solutions assessment to take CIPSEC overall framework to higher TRLs (7, 8 or even 9)			
T4.1 Setup and configuration of the trials	M19-M24	EMP AEGIS, ATOS, BD, CSI, DB, HCPB, TUD, UPC, UOP, WOS	D4.1 Trial scenario definitions and evaluation methodology specification	M24
Trial of the system framework. ■ Definition of experiments to evaluate the performance of the individual modules in controlled environments. ■ Definition of the proof of concept scenarios in three pilots (and its adaptability to multiple scenarios). ■ Definition of an evaluation methodology for the technical aspects of individual technologies. ■ Transition from lab testing system to demonstrator system for the three pilots. ■ Set trial goals according project objectives and KPIs. Planning for trial (timing, procedures, people, and equipment).				
T4.2 Field configuration for pilot deployment	M21-M27	TUD ATOS, BD, CSI, DB, HCPB, UPC, UOP, WOS	D4.2 System ready for validation activities DB	M27
Preparatory actions for the field trial. ■ Configuration of the several experimentations for TRL 8 including the selection of industrial control sub-systems and hardware components. ■ Execution of sanity checks.				
T4.3 System Prototype Demonstration (TRL 8)	M25-M32	WOS AEGIS, BD, CSI, DB, EMP, HCPB, TUD, UPC, UOP	D4.3 Prototype Demonstration: Field trial results	M32
Conduct trials based on defined scenarios: intra-domain as well as inter-domain (cascading effects).				
T4.4 Solution assessment	M26-M36	COMSEC AEGIS, CSI, DB, HCPB, UPC, UOP, WOS	D4.4 Use-case evaluation and recommendations	M36
■ Qualitative and quantitative assessment of the performance. Evaluate both, the performance of the individual system modules, and the integrated system. Analyse results against WP2 requirements and performance indicators. Lessons learned and recommendations. ■ Total Cost of Ownership (TCO) to evaluate the expected savings of the deployed solution. • Scalability. • Cost differences and benefits between applications domains. • Optimal location and configuration of the security framework and components. Due to the uncertainty and country dependence of some input parameters (regulations, configurations, etc.) a sensitivity analysis will be performed related to specific cases and general harmonization.				

WP5	Exploitation and dissemination plan including standardization activities			COM
T5.1 Exploitation activities	M6-M36	WOS AEGIS, ATOS, BD, COMSEC, CSI, DB, EMP, TUD	D5.1 Dissemination plan and market analysis	M6
			D5.5 Business model definition ATOS	M34

- Preliminary market analysis.
  - Definition of a methodology to identify major market segments, analysis of Unique Selling Points, and competitors' strengths and weaknesses.
  - Analysing existing technologies, current trends and market barriers.
  - Assessing selected business and technology transfer models in the different EU countries and defining a deployment strategy for CIPSEC partners.
- Industrial roadmap: individual exploitation plans for each industrial partner, including a forecast for 3 year period after project completion and business models based on a thorough risk analysis.
- Business model: framework for analysis of value creation and business models for deployment of security-based applications, including metrics for cost-effectiveness, organisational adaptation and sustainable cost-benefit analysis.
  - Development of a suitable business model at European level.
  - Define the socio-economic foundation for sustainable implementation of the proposed security products and services across multiple application domains.
  - Created value and deriving sustainable business models to support deployment of the proposed CIPSEC framework.
  - Identifying actors and roles.
- IPR management: rules for managing project results after the project life. (Consortium Agreement compliant)

T5.2 Dissemination activities	M1-M36	UPC AEGIS, ATOS, COMSEC, CSI, DB, EMP, FORTH, HCPB, TUD, UOP, WOS	D5.2 CIPSEC annual report on exploitation, dissemination and standardization (Year 1)	M12
			D5.3 CIPSEC annual report on exploitation, dissemination and standardization (Year 2)	M24
			D5.4 CIPSEC annual report on exploitation, dissemination and standardization (Year 3)	M36

- Web portal.
- Dissemination material: leaflet, poster and presentation slides will be created and updated upon major developments in the course of the project. Publications in major European and Non-European technical conferences as well as in specialised journals and magazines.
- Project blog / Social media strategy (including Twitter, Facebook, LinkedIn and the likes) / Newsletter.
- Workshops. The Consortium will organize three workshops between M18 and M36. CIPSEC is not organizing standalone workshops but rather co-locate our workshops with international events (EU meeting, conferences).
- Training. The Consortium will organize three training between M18 and M36. Educational material, on-line courses related to project outcomes, key factors and best practices learnt during project development.

T5.3 Standardization activities	M6-M36	TUD FORTH, UOP		
■ Disseminate first take of ICT standards related to Digital Security and CI management within the project. ■ Provide feedback to the standardization bodies: tools and methods to evaluate implementation (conformity, etc.). ■ Participate in the evolution of standards for their second take pushing the results of our innovation activity.				
T5.4 Preliminary certification activities	M25-M36	COMSEC EMP	D5.6 Preliminary certification activities	M36
Certification of the CIPSEC solution platform: security elements will be carefully inspected for potential and actual security flaws.				

WP6	**Project Management**	**ATOS**
T6.1. Project Coordination including operational management		M1-M36
D6.1 Project management strategy: project handbook	M6	■ Validation Plan. ■ Risk Management Plan. ■ Project's Contingency Plan ■ Progress and cost reporting (costs reports for each activity cost reports and for the overall project), ■ Progress, Communication and IPR Management plan.
D6.2 CIPSEC annual report on project management (Year 1)	M12	This deliverable contain an overview of the activities carried out during the reporting period, describe the progress in relation to the project objectives, the progress towards the milestones and deliverables set for the period, any problems encountered and corrective actions taken, etc. Deliverable also includes a detailed justification of the costs incurred and of the resources deployed by each contractor linking them to activities implemented and justifying their necessity, the financial statements from each contractor and a summary financial report consolidating the costs of the contractors, etc.
D6.3 CIPSEC annual report on project management (Year 2)	M24	
D6.4 CIPSEC annual report on project management (Year 3)	M36	

3.6 Consortium

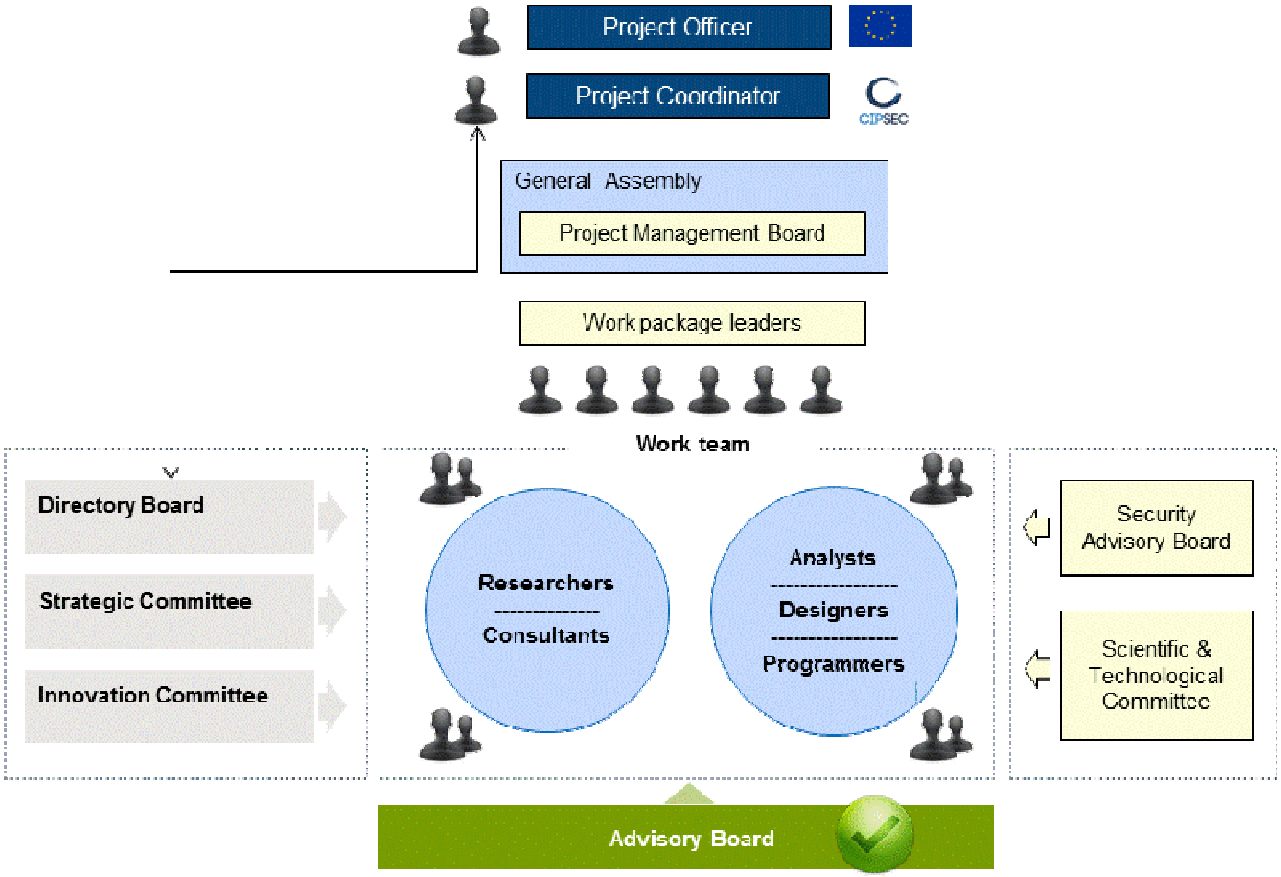
Name	Comments	WP1 Critical Infrastructure environments	WP2 Development of security framework	WP3 Pilots	WP4 Working prototypes in operational environment
AEGIS IT RESEARCH LTD AEGIS / UK / SME	AEGIS Visualization Toolkit allow datasets to be viewed graphically and combined with other datasets to improve the understanding of the investigator and identify possible problems in many scenario including industrial operations. (TRL 5)	Data collection requirements for the forensics analysis and the visualization tool.	Visualization component of the CIPSEC platform. Coordination with the developers of the anomaly detection system.	Requirements of each pilot and specify rules regarding the highlighting of parameters.	Forensics analysis and visualization system adjustment for the pilots.
ATOS SPAIN SA ATOS / Spain / Enterprise	**XL-SIEM Cross-Level Cybersecurity Event and Information Management** (TRL 8/9) has the ability to integrate under the same framework different kinds of security systems and can correlate/process events across multiple layers, identify anomalies, provide improved detection capabilities like near real-time aggregation, disseminate events etc., with small overhead upon CIs resilience.	Analysis for Financial Services (CI other domains). Functionality building blocks according participants provided platforms.	CIPSEC security framework.	Pilot integration support.	Trial scenarios and platform readiness for validation support.
BITDEFENDER SRL BD / Romania / Enterprise	**CIPSEC will use Bitdefender products of Cyber-security and Anti-virus/malware.** ■ TotalSecurity 2015, GravityZone (TRL 8/9)	Requirements for cybersecurity, antimalware and antivirus protection.	CIPSEC security framework: products for security solutions integration.		Trial tests of the CIPSEC framework adjusting its contributed products in the three pilots.
COMSEC LIMITED COMSEC / Israel / Consultant	Solid background and great expertise in the evaluation of cyber security solutions and compliance with standards and certification. Tools, technology, services for evaluation, certification, and standardization alignment of CIPSEC solutions (TRL 7).	Building security development life cycle from the prototype to the final framework.	Security design supporting the sw/hw security: anomaly detection and compliance management, Denial of Service detector.	Deploying policies, regulations and standardizations.	Support the trial setup and deployment.
CONSORZIO PER IL SISTEMA INFORMATIVO (CSI PIEMONTE) CSI / Italy / Provider Communication	Public entity responsible for managing the underlying IT and communication infrastructure of the Piedmont region, also handling all data management and OT of multiple public CI services.	Security aspects of the Piedmont pilot and discover interdependencies among different networks and domains.	To develop the security framework according to its own specific requirements.	To integrate the CIPSEC solution on the environment monitoring system.	Environment monitoring pilot coordination.

Name	Comments	WP1 Critical Infrastructure environments	WP2 Development of security framework	WP3 Pilots	WP4 Working prototypes in operational environment
DEUTSCHE BAHN NETZ AG DB / Germany/ Provider Transportation	The biggest company for railway transportation in Germany.	Providing information about the specific requirements of transportation domain.	To review proposed solutions and innovations and advising on the applicability on transportation CI.	Integration of the security platform into their railway pilot.	Developing a solid configuration for the transportation domain.
EMPELOR GMBH EMP / Switzerland / SME	**CIPSEC will use EMPELOR modules for hardware protection.** ■ Secocard (mobile security computing and communication platform) TRL 7	Analyzing security issues, with particular focus on the e-health and transportation.	2 PMs supposedly for T2.1	e-health and transportation pilots. CI intra & inter-dependencies and CI policies definition.	Trials configuration preparatory activities and demonstration of the prototype.
FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS FORTH / Greece / Research	FORTH is member of FORWARD and the coordinator of SysSec. Solid background and great expertise in the evaluation of cyber security solutions and compliance with standards and certification. **CIPSEC will use FORTH DDoS solutions.** ■ DDoS detection system (TRL 7)	All tasks.	All tasks.	e-health and transportation pilots. CI inter-dependencies. CI complexity analysis.	
HOSPITAL CLINIC I PROVINCIAL DE BARCELONA HCPB / Spain / Provider Hospital	One of the largest public hospitals in EU	Analyzing security issues and existing market products, e-health pilot- oriented.	To provide advice on the CIPSEC platform design to meet specific e-health pilot's needs and requirements.	Adapting proposed architecture to the specific requirements of the health scenario	Contributing to pilot and trial settings as well as to the validation and demonstration activities.

Name	Comments	WP1 Critical Infrastructure environments	WP2 Development of security framework	WP3 Pilots	WP4 Working prototypes in operational environment
TECHNISCHE UNIVERSITÄT DARMSTADT TUD / Germany / University	■ Safety processes and requirements for critical railway systems. (TRL 8) ■ Hardware and specification for object controllers (OC) of field elements. (TRL 5)	Requirements of railway transportation CIs.	Designing and developing anomaly detection and incident response solutions for CIs. To assist in developing the architecture of the CIPSEC framework.	Developing solutions to apply the CIPSEC security framework to the railway transportation domain.	Providing pilot setups for anomaly detection and incident response solutions. Transportation pilot setup.
UNIVERSITAT POLITECNICA DE CATALUNYA UPC / Spain / University	■ Data Privacy Tool. (TRL 5)	Analyzing and reviewing security solutions specially in the areas of data privacy and interdependencies of Cis. Integration requirements and functional definition.	Architectural prototype, and final CIPSEC framework. To define security services and the evaluation plan.	Data privacy security for the pilots. Potential CI inter-dependencies and cascading effects.	Testing regarding data privacy security aspects on pilots validation. Define trials and the evaluation roadmap.
UNIVERSITY OF PATRAS UOP / Greece / University	**CIPSEC will use modules for hardware protection enhanced with additional cryptographic modules designed and implemented by UOP.** ■ Add-on Cryptographic Hardware and Software toolset (TRL 5).	Requirements and interdependencies on hardware security and identity management.	Hardware security element innovation integration.	Innovative hardware means to each pilot.	Trial setup and deployment regarding hardware security design.
WORLDSENSING LIMITED WOS / UK / SME	**CIPSEC will use Worldsensing DDoS solutions.** ■ Enriching Bitcarrier product (owned by WOS) with a jammer detector. (TRL 7) ■ PHY-layer Authentication Preamble against exhaustion attacks (DDoS exhaustion). Adapting a novel authentication scheme, able to discard non-intended and/or non-legitimate packets just after the reception of the physical preamble, to include it in the communication protocol stack for the provided M2M devices (WOS will explore several standards for implementing this solution, for example, IEEE 802.15.4e). (TRL 5)	For each pilot: to design configuration of the proposed security product and to evaluate configuration for the DoS detector	To design and integrate components of the jamming detector into Bitcarrier. To coordinate CIPSEC in the definition of the proposed services.	Integration and optimization of the CIPSEC security framework taking into account the specific requirement within the proposed pilots.	To lead the operational demonstration tests: coordination with involved entities and definition and applications of the best configuration for each pilot.

4 Project management

4.1 Organization



Project officer (PO)	Cristina Longo.
Project coordinator (PC)	Fernando Carmona. (ATOS) PC acts as an intermediary between the consortium and the European Commission, and is responsible for ensuring that both financial and contractual obligations defined in the GA are met. PC provides strategic leadership for the project; coordinates and controls its major activities; supervises the project's progress against the planned schedule in budget and manpower; is responsible for monitoring resource usage, budget allocation, project cash flow and also managing conflicts by application of the foreseen procedures and const as well as for the project's overall scientific vision and steers the research, technical, training and dissemination activities of the project. PC's main responsibilities are summarized in next page.

Management

- Bringing up the proper governance structure for an effective project direction and management.
- Facilitating a smooth project operation and an effective collaboration among partners, the European Commission and other external bodies as required.
- Establishing measures for avoiding risks related to financial, legal, administrative and technical coordination as well as contingency plans ready to be launched, when necessary.
- Work plan: formulating propositions for modifications, processing and coordinating any amendment on behalf of the Consortium, and transferring any contractual change to the project plan.
- Verifying progress of work according to the project time schedule.
- Monitoring resource usage, budget allocation, project cash flow.
- Managing conflicts by application of the foreseen procedures.
- Manage and coordinate the activities of the strategic, scientific and technological, and innovation committees as well as the relationship with the advisory board.
- Supervising contacts with all external organisations.

Communication & Reporting

- Contacting the Project Officer.
- Legal entity acting as the intermediary between Parties and the Funding Authority.
- Delivering all types of reports and deliverables.
- Setting up the communication procedures and methods for reporting, monitoring, and quality assurance.
- Performing the financial, legal, administrative and technical coordination within the given budget and time limits, according to the formal requirements and guidelines of the European Commission.
- Keeping the address list of members and other contact persons updated and available.

IPR

- Proper management of foreground, knowledge and intellectual property.
- Overseeing the process and advice the project on all aspects of Knowledge Management and patent filing. PC is also in charge of maintaining a schedule of knowledge produced during the project and, in conjunction with the partners involved, assessing the opportunities to apply for patents or declare copyrights.
  - Description of the innovative elements of the work conducted in the technological work packages.
  - Review of existing patents databases and other scientific databases for similar developments.
- Reporting to the Project Board and to the technical teams about the innovation status of the project results and proposing registration of patents where appropriate.

Gender issues

- Enforcing gender equality in all aspects of the project and non-discrimination based on able-ness or origin.

General Assembly	Chaired by the Project Coordinator, the General Assembly is the main decision making body of the project and is established to define and review the overall progress of the project, acting as the common forum for discussion and high-level decisions. ■ Ordinary meeting: at least once a year. ■ Extraordinary meeting: at any time upon written request of the PMB or 1/3 of the Members of the General Assembly, or at the request in writing of the PC. Meeting minutes will always be submitted to the partners' representatives for acceptance.

	Project Management Board (PMB)	**Security Advisory Board[1] (SAB)**
	Chaired by PC	
	Working committee of the General Assembly to actively control the overall success of the project and to support the Project Coordinator in the strategic management, ensuring thereby that all partners can meet their individual responsibilities. PMB is on charge of contractual management[2] (except in the case of coordinator replacement), to ensure its compliance to GA. Any changes to the project scope and plan must be reviewed and approved by all levels of project management, before proposing these changes to the PMB; any modification will be considered rejected, if so on any of these involved levels. ■ Ordinary meeting: at least quarterly. ■ Extraordinary meeting: at any time upon written request of any Member of the PMB, or at the request in writing of the PC.	Assessing the sensitivity of deliverables prior to their publication. Silence will be taken as approval, as agreed at Kick-Off meeting. All deliverables will explicitly declare that have been endorsed by SAB.
AEGIS	Ilias Spais	Vassilis Prevelakis
ATOS	Fernando Carmona	Fernando Carmona
BD	Ovidiu Mihăilă	Dragoș Gavriluţ
COMSEC	Amir Atzmon	Gil Cohen
CSI	Vittorio Vallero	Barbara Lunel
DB	Christian Schlehuber	Christian Schlehuber
EMP	Pascal Papagrigoriou	Pascal Papagrigoriou
FORTH	Sotiris Ioannidis	Sotiris Ioannidis
HCPB	Ferrán Rodriguez	Ferran Rodríguez
TUD	Neeraj Suri	Neeraj Suri
UPC	Xavi Masip	Jordi Forne
UOP	Kostas Lampropoulos	Apostolos Fournaris
WOS	Francisco Hernández	Francisco Hernández

[1] As appointed at project Kick-off in Barcelona. June, 6,7.

[2] Changes in the Consortium configuration (e.g. addition or withdrawal of beneficiaries or third parties) or CA. Contract closing.

	Work package leaders	Scientific & Technological Committee
	WP leaders are responsible for setting up technical meetings, preparing and distributing minutes within affected WP.	Implementation of strategies as defined by the Project Management Board and synergetic communication between the different activities and work packages. On charge of monitoring the research and technical activities, is led by WP1 leader, FORTH. It consists of the Project Coordinator and all Work Package Leaders plus one representative for each academic partner (KO meeting agreement). Usually meets during the GA or upon request.
WP1 – FORTH	Sotiris Ioannidis	**Leader: Sotiris Ioannidis**
WP2 – ATOS	Rodrigo Díaz	Rodrigo Díaz, Joaquín Rodríguez
WP3 – CSI	Barbara Lunel	Barbara Lunel
WP4 – WOS	Carlos Valderrama	Carlos Valderrama
WP5 – COMSEC	Amir Atzmon	Amir Atzmon
WP6 – ATOS	Fernando Carmona	Fernando Carmona
Academic partner - TUD		Neeraj Suri, Markus Heinrich.
Academic partner - UPC		Xavi Masip, Jordi Forné
Academic partner - UOP		Apostolos Fournaris
BD		Ciprian Oprisa
DB		Christian Schlehuber

Directory Board	The Directory Board is chaired by the Project Coordinator and composed by several experts from ATOS. It is offered to provide support to the Project Coordinator. Elsa Prieto: Management. Rodrigo Díaz: Head of CyberSecurity Lab. Aljosa Pasic: Technology Transfer Director.

Strategic Committee	Its leadership is established on a yearly basis. COMSEC leads SC in the first year. Monitoring the project activities, especially the plan of use, exploitation and dissemination. It will ensure not only a maximum synergy between work packages, but also an adequate and updated validation of milestones and deliverables. SC is responsible for the strategic evolution of the CIPSEC proposal, through a continuous monitoring of the different project activities to guarantee alignment with external project efforts and initiatives as well as the right matching with CIs needs and evolution.		
	Year 1	**Year 2**	**Year 3**
	■ Project visibility and awareness. ■ Strategic networks of the partners. ■ Powerful standing in CIP clusters.	■ Continue to build awareness of CIPSEC results in CIP and within smart cities communities. ■ Verify opportunities to apply CIPSEC in public events and involve other stakeholders.	■ Prepare to integrate CIPSEC pilots and liaise with prominent CIP clusters for future exploitation. ■ Promote the uptake of specific methods, technologies & tools in selected domains. ■ Prepare for exploitation of all CIPSEC knowledge components, products and services.

Innovation Committee	Its leadership is established on a yearly basis. WOS leads SC in the first year. A close relationship with exploitation activities is needed in order to monitor the project alignment with the technological and market trends in terms of: ■ Meeting the needs of European and global markets. ■ Delivering such innovations to the markets. ■ Enhancing innovation capacity and integration of acquired knowledge. In addition, there are some technological factors that might create a sense of urgency around the need to generate new ideas for meeting these goals. These drivers can be summarized as follows: ■ Emerging technologies. ■ Competitor actions (especially other research initiatives). ■ Emerging changes in the external environment. Decisions taken from this Committee will strongly impact on the implementation of successful innovative ideas. By studying the technical and strategic reports/deliverables and interacting with project's external entities, such as advisory board's members, Innovation Committee allows responding promptly to external or internal opportunities.

	Strategic Committee	**Innovation Committee**
AEGIS	Vassilis Prevelakis	Ilias Spais
ATOS	Fernando Carmona	Rodrigo Díaz
BD		
COMSEC	**Leader: Gil Cohen**	
CSI	Vittorio Vallero	
DB	Ralph Müller	
EMP		Panagiotis Sifniadis Nikos Papadakis
FORTH		Christos Papachristos
HCPB	Ferrán Rodriguez	Manel Sanz
TUD		
UPC	Eva Marín Tordera	Ahmad Mezher
UOP		Kostas Lampropoulos
WOS		**Leader: Carlos Valderrama**

<table>
<tr><td rowspan="11">Advisory Board</td><td colspan="3">Chaired by Project Coordinator</td></tr>
<tr><td colspan="3">Independent group composed by external experts in security and privacy that will give guidelines and provide expert advice to the project in order to maximize the impact of the project results. PAB responsibilities include:
■ To provide expert advice and feedback on selected CIPSEC developments or innovations
■ To assist the Consortium with communication and dissemination activities, including the uptake and understanding of CIPSEC research and national and pan-European dimensions.</td></tr>
<tr><td>Centro Nacional de Excelencia en Ciberseguridad (Spain)</td><td>Enrique Avila.</td><td>Assisting the project Consortium in providing guidance, advice, specs and requirements, feedback as well as promoting CIPSEC results on its contacts network.</td></tr>
<tr><td colspan="2">Katholieke Universiteit Leuven (ICRI[1]) (Belgium)</td><td>Legal requirements: advices to define appropriate solutions in each case/country/region.</td></tr>
<tr><td>Thales (France)</td><td>Paulitsch Michael.</td><td rowspan="2">Managing and contributing to several standardizations groups: EPCIP and ERNCIP, such as Industrial Automated Control Systems and Smart Grid.</td></tr>
<tr><td>TNO (Netherlands)</td><td>Frank Fransen.</td></tr>
<tr><td>SIEMENS (Germany)</td><td>Michael Munzert.</td><td rowspan="3">Connection chain with main stakeholders, OEMs, SMEs and consumers in the field of digital security and critical infrastructure protection.</td></tr>
<tr><td colspan="2">CISCO</td></tr>
<tr><td colspan="2">INFINEON</td></tr>
<tr><td>PESI Plataforma Tecnológica Española de Seguridad Industrial (Spain)</td><td>Javier Larrañeta.</td><td>Assisting the project Consortium in providing guidance, advice, specs and requirements, feedback as well as promoting CIPSEC results on its contacts network.</td></tr>
<tr><td>Technische Universität Berlin (Germany)</td><td colspan="2">Robert Pelzer.</td></tr>
<tr><td>Piedmont Region (Italy)</td><td>Stefano Rigatelli.</td><td>The region is willing to study and test CIPSEC solution in the Air Quality Monitoring system and to understand and analyze impacts and potential cascading effects to provide requirements and feedback, and promote CIPSEC results.</td></tr>
<tr><td>SP Technical Research Institute of Sweden</td><td>Anders Lönnermark.</td><td>Assisting the project Consortium in providing guidance, advice, specs and requirements, feedback as well as promoting CIPSEC results on its contacts network.</td></tr>
</table>

[1] Interdisciplinary Center for Law and ICT.

Grant administration

Each beneficiary must immediately inform the PC — which must immediately inform the Agency and the other beneficiaries — of any of the following:

- Events which are likely to affect significantly or delay the implementation of the action or the EU's financial interests, in particular:
  - Changes in its legal, financial, technical, organisational or ownership situation or those of its linked third parties.
  - Changes in the name, address, legal form, organisation type of its linked third parties;
- Circumstances affecting the decision to award the grant or compliance with requirements under the Agreement.

Mailing lists

Atos is responsible for managing and maintaining the mailing list service. There are two mailing lists in CIPSEC:

- The address cipsec@lists.atosresearch.eu will be used as the common point for communication among all project members. All technical project staff from all project partners must be subscribed. It must be used by partners to communicate project results, organize meetings and common activities, and all activities that require coordination and synchronization among members.
- The address cipsec-mgmt@lists.atosresearch.eu will be used just for administration-related issues. Each partner will appoint the appropriate people to be part of this list. At least one person from each partner dealing with financial, contractual and legal issues must be subscribed to this list. No issues other than administrative ones can be addressed by using this list.

Users of the mailing lists should refrain from an improper usage of the list. Mail intended for specific purposes or restricted groups communications should not be sent to the list but only to interested parties.

The email subject must contain all the useful information to allow an easy and rapid classification of the messages received. Specifically the subject must start with “[CIPSEC]” (this string is already appended at the beginning of the subject by the mailing system). In addition, if related to a specific work package, it should be evidenced (for instance, “[CIPSEC][WP1]”). If it is related to a specific task, it must be also notices (for instance, “[CIPSEC][WP6][T6.1]”). An explicit title is requested in the case of meeting announcements, agendas, deliverable draft, etc.

An “URGENT” label in the email subject should identify any deliverable and decision deadline as well as urgent information by the Commission.

The word “REMINDER” will be used by PC for reminders about open actions. If a file has to be attached, please use.zip files to compress the information. However, and as a general rule, if the file may be of interest for several people in the project, it is always preferable to upload the file to the SVN repository for CIPSEC and inform concerned people of the location of the file.

Mailing lists have a limit on the size of messages, so attachments should be avoided, in favour of document storage on the CIPSEC repository.

Electronic exchange system

- Each beneficiary must keep information stored in the 'Beneficiary Register' up to date, in particular, its name, address, legal representatives, legal form and organisation type.

  https://ec.europa.eu/research/participants/portal/desktop/en/projects/

4.2 Monitoring

The project monitoring oversees all the tasks and metrics necessary to ensure that the project is within scope, on time, and on budget, so that the project proceeds with minimal risk. PC is on charge of project monitoring, with the support of the PMB.

Qualitative measures and key performance indicators (KPIs) have been defined in order to control the project execution and its compliance with the three project areas: scope, schedule and budget.

Project objectives

Objective	Measure
Unified security framework for CI	■ Orchestration through the XL-SIEM – Cross-Level Cybersecurity Information and Event Management. ■ Collection of data, provided as input to XL-SIEM, for monitoring and anomaly detection from multiple sources.
Security ecosystem	■ Setup and execution of an incident causing cascading effect between two CI providers. Analysis report on cascading effect protection. ■ Promotion of PPPs, definition of contingency plans, means for advancing collaboration and data sharing ■ Training courses. ■ Updating and patching mechanisms. ■ Enhanced forensics methods. Digital forensics analysis visualization toolkit
Real CIs (transportation, health and environment pilots)	■ Security framework for transportation, health and environment monitoring sector. ■ Successful validation of proposed products and services
Links and standardizations bodies	■ Harmonization of CIPSEC proposed solutions with EU standards. ■ Successful alignment of CIPSEC with EPCIP.
Ready to market	■ Ready to market solutions for the overall framework and independent security solutions. ■ Collaborations between partners and external stakeholders

Project management

KPI		Target
Technical team members joined up in less than two weeks.		>=90%
Milestones timely fulfilled (milestones achieved / total milestones).		>=90%
Task undergoing diverted schedule (delayed tasks / total tasks).		<=10%
Task undergoing diverted effort (delayed tasks / total tasks).		<=5%
Project handbook fulfilment (achieved guidelines / total guidelines).		>=80%
Risk assessment fulfilment (achieved guidelines / total guidelines).		>=80%
Meeting agendas are forwarded in advance.	General Assembly	30 calendar days (7 calendar days for an extraordinary meeting)
	Project Management Board	10 calendar days
Period for issuing meeting minutes.		<=10 calendar days
Period for reviewing deliverables.		<=15 calendar days

KPI	Target
Deliverables schedule fulfilment (timely deliverables / total deliverables).	=100%
Meeting attendances under PC request (attendances / total requests).	>=80%

Requirements elicitation

KPI	Target
Identified requirements (requirements in catalogue / total final requirements).	>=80%
Requirements traceability (traceable requirements / total final requirements).	>=80%

Implementation

KPI	Target
Number of decisions for reversing during the implementation process.	<=3

Testing

KPI	Target
Test plan fulfilment (achieved milestones / total milestones)	>=80%
Test sessions attendances (attendances / total requests).	=100%
Number of severe faults / setbacks not detected during configuration and deployment but arisen during prototypes demonstration.	<=5
Number of minor faults / setbacks not detected during configuration and deployment but arisen during prototypes demonstration.	<=10

Data sources

KPI	Target
Average period to carry out data extraction requests.	<=10 calendar days

Training

KPI	Target
Fulfilling surveys / total surveys	>=90%

4.3 Meetings

4.3.1 Plenary meetings

The Plenary meetings are held physically in a venue previously chosen by consensus within the Consortium. Each partner is requested to provide at least one representative to these meetings. There will be 4 different kinds of Plenary Meetings,

- Kick-off. It happens just once and is the first meeting of the project. Its agenda comprised the following slots:
  - Presentation of Consortium partners.
  - Project overview, chaired by PC. It offers an overview of the project and all its related aspects.
  - One slot per work package, chaired by WP leaders. In these slots, all the issues related to each work package are addressed.
  - Presentation of the H2020 Administrative Framework: chaired by the European Commission.
  - Wrap-up and next steps: to recap all the agreements and actions, outcomes of the meeting.
- Internal monitoring (Consortium) scheduled in order to check the completion of milestones and the status of the tasks. These meetings will comprise the following slots:
  - One slot to describe briefly the general status of the project, as an introduction to the rest of specific work package slots. Chaired by the PC.
  - One slot per work package to follow up the progress of work, analyse risks and plan the next actions. Chaired by the WP leaders.
  - Wrap-up and next steps: to recap all the agreements and actions, outcomes of the meeting.
  - Specific slot will be saved in General Assemblys agenda for Committees meeting proposal (Scientific & Technological Committee, Strategic Committee, and Innovation Committee).
  - Optional slots to discuss specific cross-issues affecting the whole project.
- Rehearsal meetings. They are scheduled to prepare a Technical Review Meeting. The goal is to rehearse the presentations and live demos (if any) that will be showed out in front of the Project Officer and reviewers. Besides, a slot devoted to deal with last minute problems will be foreseen in the agenda. Likely issues coming from the Project Officer and the reviewers should be anticipated during this meeting.
- Technical review meeting. It takes place once per reporting period. The date and place for the meeting is previously agreed with the Project Officer. Each partner must provide the needed staff to give the presentations, set up the live demos and contribute with the discussions. The Project Officer will appoint some people to act as reviewers during the meeting. As a result of the meeting, a report assessing the progression of the project is sent to the PC by the EC.

  PC, with the support of WP Leaders and all Consortium members, will organise and prepare the review meetings in advance, following these guidelines:
  - Preparing the agenda for review preparation and for the review meeting.
  - Liaising with management participants and making sure that advance registration for the review is complete.
  - Presiding over all review presentations.
  - Presenting an overview of the project/activity in the beginning of the review.
  - Ensuring the taking of minutes and providing the final version of minutes.
  - Sending all partners the review report from the EU.
  - Following up all comments and recommendations from the reviewers and EU Project Officer.

4.3.2 General follow-up calls

As agreed at General Assembly in Heraklion, a general monthly telco will be hold for the overall follow-up of the project. This telcos will be leaded by Project Coordinator and leaders of WP in progress. For the work in progress, WP leaders and Deliverable leaders attendance is mandatory; each WP leader will nominate mandatory attendees related with tasks and deliverables under their responsibility. Duration for this telcos will be one hour. Telcos will take place last Thursday of each month, 10:00 – 11:00.

4.3.3 WP / Task follow-up calls

Regular WP and Task conference calls must be set up to track progress of the activities of participants and report on the work carried out towards achieving the WP/Task objectives. Periodicity should be, at least, one per month. If needed, they can be scheduled more frequently.

The WP/Task leader must organise progress calls taking into account the constraints of the majority of the required participants (e.g. by using a voting poll facility such as http://doodle.com).

The WP/Task leader should decide the telephone system for hosting conference calls, prioritizing as much as possible the availability of local numbers for participants. Specific conference calls and meetings are expected to be organised when preparing deliverables or other intermediate milestones.

4.3.4 WP / Task specific workshops (face-to-face)

Phone conferences are always the preferred means over face-to-face meetings, in order to minimize travelling within the project. When a WP/Task leader considers necessary to call for a face-to-face meeting, it should be notified to the PC formally by email, and at least 1 month in advance.

PC will consult PMB to evaluate possibilities of collocation with other face-to-face meetings (plenary or other WP / Task workshops). Each partner will appoint the staff who will take care of attending the meeting.

4.3.5 PAB meetings

Project Advisory Board members will be invited to attend the Project internal monitoring (Consortium) sessions at their discretion and will be supplied with a roster of proposed subjects to address their advice, without refraining them in regard to any other support they might consider.

If PAB meeting could not be conducted because of the lack of quorum, separate telcos will be set up according PAB members availability.

4.3.6 Face to face meetings (scheduled)

Face to face meetings	Month		Organize	GA	PMB	STC
Project Kick-Off	M1	May 2016	ATOS	☑	☑	([1])
Project internal monitoring	M5	Sep 2016	FORTH		☑	
I Technical Workshop – Critical Infrastructure Protection and Industrial Control System management	M7	Nov 2016	UPC			
Project internal monitoring	M9	Feb 2017	EMP		☑	

[1] Scientific and Technological Committee set up.

Face to face meetings	Month		Organize	GA	PMB	STC
Project internal monitoring	M13	May 2017	WOS	☑	☑	☑
II Technical Workshop – Critical Infrastructure Protection and Industrial Control System management	M15	Jul 2017	TUD			
Project internal monitoring	M17	Sep 2017	EMP		☑	
Project internal monitoring	M21	Jan 2018	AEGIS		☑	
Stage 1 - Field Trial configuration	M24	Apr 2018	CSI / DB / HCPB			
Project internal monitoring	M25	May 2018	WOS	☑	☑	☑
III Technical Workshop – Critical Infrastructure Protection and Industrial Control System management	M26	Jun 2018	UOP			
Project internal monitoring	M29	Sep 2018	DB		☑	
I – Training courses for CI staff: how to use CIPSEC framework and react to emergency situation	M30	Oct 2018	TUD			
II – Training courses for CI staff: how to use CIPSEC framework and react to emergency situation	M30	Oct 2018	COMSEC			
III – Training courses for CI staff: how to use CIPSEC framework and react to emergency situation	M30	Oct 2018	FORTH			
Stage 2 – Prototype Demonstration	M32	Dec 2018	CSI / DB / HCPB			
Final project internal monitoring	M35	Mar 2019	ATOS	☑	☑	☑

4.3.7 Decision making

Decision making process is closely related to (and comes from) the project overall plan. Hence, it is depicted in next page, followed by project milestones.

Project plan

Internal review / Reporting period						IR						IR						RP1			IR						IR						RP1
						MS22												IR			MS24												IR
						MS18															MS14												
						MS4															MS13												MS25
						MS3												MS10			MS12												MS20
						MS2												MS9			MS11												MS17
			MS21			MS1			MS5			MS23						MS6			MS7			MS15					MS16			MS19		MS8
	2016								2017												2018										2019			
	may	jun	jul	aug	sep	oct	nov	dec	jan	feb	mar	apr	may	jun	jul	aug	sep	oct	nov	dec	jan	feb	mar	apr	may	jun	jul	aug	sep	oct	nov	dec	jan	feb	mar	apr
Work package	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP1. Adaptation of security components to Critical Infrastructure environments						**D1.3**																														
1.1 In depth security analysis for CIPSEC pilot's CIs																																				
1.2 Evaluation of CIPSEC market products in relation to CIs and pilots needs						**D1.1**																														
1.3 Requirements of integrating heterogeneous products into unified solutions						**D1.2**																														
1.4 Interdependences of CIs																																				
WP2. Development of the CIPSEC security framework for Critical Infrastructure environments																																				
2.1 CIPSEC security framework design, integration and optimization – prototype									**D2.1**									**D2.2**						**D2.5**												
2.2 Enhancing CIPSEC market products with the latest research innovations																		**D2.3**																		
2.3 CIPSEC security services																		**D2.4**																		
2.4 Derivation and evaluation of default settings																								**D2.6**												
2.5 From the prototype to the final CIPSEC security framework																																				**D2.7**
WP3. Integration of CIPSEC solution to transportation, health and environment pilots																																				
3.1 Security framework for transportation CIs																		**D3.1**						**D3.5**												
3.2 Security framework for health CIs																		**D3.2**						**D3.6**												
3.3 Security solution for environmental monitoring CIs																		**D3.3**						**D3.7**												
3.4 CIs intra- and inter-dependencies including cascading effects																		**D3.4**						**D3.8**												
3.5 Complexity analysis and policies definition																								**D3.9**												
WP4. Refinements towards working prototypes in operational environment																																				
4.1 Setup and configuration of the trials																								**D4.1**												
4.2 Field configuration for pilot deployment																											**D4.2**									
4.3 System Prototype Demonstration (TRL 8)																															**D4.3**					
4.4 Solution assessment																																				**D4.4**
WP5. Exploitation and dissemination plan including standardization activities																																				
5.1 Exploitation activities						**D5.1**																												**D5.5**		
5.2 Dissemination activities												**D5.2**												**D5.3**												**D5.4**
5.3 Standardization activities																																				
5.4 Preliminary certification activities																																				**D5.6**
WP6. Project Management																																				
6.1. Project Coordination including operational management						**D6.1**						**D6.2**												**D6.3**												**D6.4**

Project milestones

Milestone ID	Month	Scope	Internal monitoring	Project review
MS21	M3 – JUL 2016	Committees setting		
MS1	M6 – OCT 2016	Security analysis	☑	
MS2		Market review and analysis		
MS3		Functionality building blocks		
MS4		CI taxonomy		
MS18		The exploitation and dissemination plan is ready		
MS22		Project management strategy		
MS5	M9 – JAN 2017	Architecture system design		
MS23	M12 – APR 2017	Project report: First year	☑	
MS6	M18 – OCT 2017	First release: preliminary version of the CIPSEC security platform	☑	☑
MS9		Preliminary report for pilots integration		
MS10		Preliminary report on CI intra/inter-dependencies		
MS7	M24 – APR 2018	Prototype ready for the operation environment tests	☑	
MS11		Adapted and optimized solution for the selected pilots		
MS12		Final report on CIs intra/inter-dependencies analysis		
MS13		List of policies for the CIPSEC prototype		
MS14		Trials settings and configuration		
MS24		Project report: Second year		
MS15	M27 – JUL 2018	System ready for the experimentation		
	M30 – OCT 2018		☑	
MS16	M32 – DEC 2018	Prototype demonstration successfully conducted		
MS19	M34 – FEB 2019	The business model for impact creation and exploitation is ready		
MS8	M36 – APR 2019	Final CIPSEC security framework	☑	☑
MS17		Final CIPSEC framework capabilities in TRL8: results evaluation		
MS20		Final project quality demonstration: exploitation, dissemination and standardization report		
MS25		Project report: Third year		

Approach

There are a number of ways the Consortium can arrive at a decision, frequently due to trade-offs of time-cost-quality, or around the emergence of a risk. Decisions are reached within the project meetings. The decision making process comprises five steps.

- Identification. This step determines that a decision is needed and requires identifying alternatives or possible paths of action and gathering relevant information or provisions to support the analysis step, such as associated risks, costs implications, scope or quality implications, or even regulatory and contractual provisions.
- Analysis of the decision. Based on the available information, the decision team evaluates and discusses the alternatives, and reaches a decision.
- Render the decision. This phase implement the agreed actions.
- Decision tracking. During this phase the decision team assesses how well the selected actions delivered the desired (or expected) positive outcomes.
- Communication. All the previous steps are supported by the communication process, so that information is spread throughout all the decision-making groups and involved stakeholders.

The basic approach for the decision-making process is to locate the decision as close as possible to the level responsible for the execution. PC will aim at consensus building, promoting mediation over voting in order to ensure a maximum degree of cooperation within the Consortium. Attempts will be made to solve conflicts as close as possible to their source. This is, conflicts within a WP will be managed by the WP leader. If the conflict cannot be solved at that level, the PMB will be asked to intervene. PC assumes the role of arbitrator / facilitator.

Major decisions on different issues, technical or otherwise, pertaining to the overall project will be reached by consensus decision-making in the PMB, if necessary by asking for the advice of external experts.

Rules

- Each Consortium Body shall not deliberate and decide validly unless two-thirds (2/3) of its members are present or represented.
- If voting is expected, meeting agenda will clearly indicate it.
- Decisions are binding once the relevant part of the meeting minutes has been accepted.

Level	Decision		Escalate if
Work package	Verbal consensus.		No consensus. Appeal to PMB.
Scientific & Technological Committee	Verbal consensus. Vote if necessary. Majority of 51%.	PC holds the casting vote.	No consensus. Appeal to PMB.
Project Management Board	Voting mandatory. Majority of 51%.	PC holds the casting vote.	No consensus. Appeal to GA
General Assembly	Majority of 51% with the exception section 6.3.1.2, Bulletpoint 2, of CA which shall be agreed by 75% of the votes.	PC holds the casting vote.	Intervention by the EC or legal action.

4.4 Documentation

4.4.1 Language

English is the official language in CIPSEC. All relevant documents will be written in English. All communication between CIPSEC and the Project Advisory Board is done in English as lingua franca.

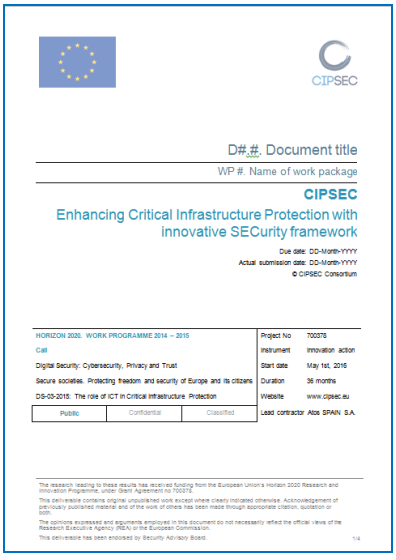
Nevertheless there can be exceptions with regard to dissemination materials, such as press releases or technical publications, which can be translated to other languages (mainly the Consortium languages: German, Greek, Hebrew, Italian, Romanian, Spanish, and French). In this scenario, each partner is responsible for translation of official CIPSEC documents to its language of interest.

4.4.2 Development

- Each partner is responsible for the quality of their contribution.
- The deliverable editor and the contributors must agree the table of contents, the work each contributor has to provide, and a tentative schedule for closure.
- The deliverable editor is responsible for the overall quality of the deliverable, including the appropriate issue of the document and communication management procedures: coordinating, requesting and collecting contributions, as well as integrating them in the different releases.
- WP leader will support the deliverable editor by checking the alignment of the deliverable with the following features:
  - Section assignment is consistent with the roles of the partners in the work package.
  - Proposed timetable is realistic according the expected deadline.
  - Proposed contents are compliant with objectives stated in the work plan.

4.4.3 Template

CIPSEC deliverables are produced by using a template which has been agreed within the Consortium. The general structure the deliverables will follow is the following.


D#.#. Document title

WP #. Name of work package

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: DD-Month-YYYY

Actual submission date: DD-Month-YYYY

© CIPSEC Consortium

HORIZON 2020. WORK PROGRAMME 2014 – 2015	Project No 700378
Call	Instrument Innovation action
Digital Security: Cybersecurity, Privacy and Trust	Start date May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens	Duration 36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection	Website www.cipsec.eu
Public / Confidential / Classified	Lead contractor Atos SPAIN S.A.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The opinions expressed and arguments employed in this document do not necessarily reflect the official views of the Research Executive Agency (REA) or the European Commission.

This deliverable has been endorsed by Security Advisory Board.

1/4

- Executive summary.
- Introduction.
  - Introductory explanation of the deliverable.
  - Purpose and scope.
  - Structure of the document.
  - Relationship to other project outcomes.
- Development of the content of the deliverable, structured as needed.
- Conclusions.
- Appendix (if needed).
- References.

4.4.4 Repository

All project-related documentation will be stored in the CIPSEC repository that has been set up upon Apache™ Subversion ® (SVN), an open source version control system[1]. CIPSEC SVN is maintained by Atos.

SVN is organized by the six work packages of the project. Each folder will contain a subfolder structure, comprehensive of WP meetings and one subfolder per deliverable. Other required folders are possible, always with a descriptive name of the content.

- Advisory Board. PAB meetings.
- Contract.
  - CA.
  - GA.
- Deliverables.
  - Final.
  - Submitted to EC.
- Events (F2F meetings): Plenary meetings & WP / Task specific workshops.
- WP1, WP2, WP3, WP4, WP5.
  - Conference calls.
    - YYYYMMDD.
  - DX.Y (one folder for deliverable)
- WP6.
  - DX.Y (one folder for deliverable).
  - Templates.

Work package leaders are in charge of the documents organisation related to their WP. Deliverable editors are responsible for keeping updated versions of the corresponding deliverable. All partners are responsible for supporting the documentation management process.

4.4.5 Notation

Each document will be identified with a unique coded name, regardless filenames and referencing conventions each partner is free to use in local archives. Document coded names are structured into the following fields:

Date DX.Y Name vX.Y (Status)

Where:

- Date. YYYYMMDD, following ISO 8601[3] standard notation (four digit year, two digit month and two digit day of the month; 20150331 for March 31st 2015).
- DX.Y stands for Deliverable, Work Package(X), Deliverable number (Y).
- Name: deliverable name according DoA.

[1] CIPSEC SVN installation and configuration has been delivered and distributed to Consortium members.

- vX.Y stands for Version X.Y.
  - X. Major release
    - 0 for draft versions.
    - 1+ for delivered versions.
  - Y. Minor release. It is a progressive number >0.
- Status.
  - Draft, refers to intermediate versions of the document.
  - Review refers to the version for internal review.
  - Final refers to the version for official delivery.

Example: 20160930 D6.1 Project management strategy. Project handbook v0.1 (Draft)

4.5 Reporting (Consortium)

According to CA, parties shall provide to PC periodical reports on partners' activity in each active work package for every six month period, containing:

- Summary of the resource consumption for project monitoring purposes, consisting of an estimate of efforts spent per task and major eligible cost items incurred in the interval.
- Any foreseen deviation of the effort or costs foreseen for the next six-month interval.

PC shall provide a template for collection of this six-monthly report to monitor actual effort deviation from internal resources planning.

PC will compile all inputs and generate reports per WP that will be verified with the WP leaders. This control action will help understand the project status and apply corrective measures when necessary. The information received within this internal reporting will be used by the PC as input for the production of a periodical report on the progress of the project to the entire Consortium.

4.6 Reporting (European Commission)

CIPSEC action is divided into the following reporting periods: RP1: from month 1 to month 18, RP2: from month 19 to month 36 in which the PC must submit to the Agency the technical and financial reports as set out in Article 20 of GA. These reports include requests for payment and will be drawn up using the forms and templates provided in the electronic exchange system.

4.6.1 Periodic reports

PC must submit a periodic report within 60 days following the end of each reporting period. The periodic report will include the following:

Technical report

- Explanation of the work carried out by the beneficiaries.
- Overview of the progress towards the objectives of the action, including milestones and deliverables identified in Annex 1, Description of the action. GA 700378.

This report must include explanations justifying the differences between work expected to be carried out in accordance with Annex 1 and that actually carried out. The report must also detail the exploitation and dissemination of the results.

- Summary for publication by the Agency.
- Answers to the 'questionnaire', covering issues related to the action implementation and the economic and societal impact, notably in the context of the Horizon 2020 key performance indicators and the Horizon 2020 monitoring requirements.

Financial report

- Individual financial statement from each beneficiary and from each linked third party, for the reporting period concerned, detailing the eligible costs for each budget category according Annex 2, Estimated budget for the action. GA 700378.

  The beneficiaries and linked third parties must declare all eligible costs, even if they exceed the amounts indicated in the estimated budget. Amounts which are not declared in the individual financial statement will not be taken into account by the Agency.

  If an individual financial statement is not submitted for a reporting period, it may be included in the periodic financial report for the next reporting period.

  The individual financial statements of the last reporting period must also detail the receipts of the action.

  Each beneficiary and each linked third party must certify that:

  - The information provided is full, reliable and true.
  - The costs declared are eligible.
  - The costs can be substantiated by adequate records and supporting documentation that will be produced upon request or in the context of checks, reviews, audits and investigations, and
  - for the last reporting period: that all the receipts have been declared.
- Explanation of the use of resources and the information on subcontracting and in-kind contributions provided by third parties from each beneficiary and from each linked third party, for the reporting period concerned.
- Periodic summary financial statement, created automatically by the electronic exchange system, consolidating the individual financial statements for the reporting period concerned and including the request for interim payment.

4.6.2 Final report

Final technical report

- Overview of the results and their exploitation and dissemination.
- Conclusions on the action.
- Socio-economic impact of the action.

Final financial report

PC must submit to the Commission the final report within 60 days following the end of the last reporting period which should include, amongst other documents:

- Final summary financial statement, created automatically by the electronic exchange system, consolidating the individual financial statements for all reporting periods and including the request for payment of the balance.

- Certificate on the financial statements for each beneficiary and for each linked third party that requests a total contribution of EUR 325 000 or more, as reimbursement of actual costs and unit costs calculated on the basis of its usual cost accounting practices. The CFS must cover all reporting periods of the beneficiary or linked third party indicated above.
- The CFS is composed of two separate documents:
  - The Terms of Reference to be signed by the Beneficiary / Linked Third Party and the Auditor.
  - The Auditor's Independent Report of Factual Findings to be issued on the Auditor's letterhead, dated, stamped and signed by the Auditor (or the competent public officer) which includes the agreed-upon procedures to be performed by the Auditor, and the standard factual findings to be confirmed by the Auditor.

4.7 Payments

PC is responsible for payments to partners according CA agreed procedures.

- The following payments will be made to the coordinator:
  - One pre-financing payment.
  - One interim payment. RP1: from month 1 to month 18.
  - One payment of the balance. RP2: from month 19 to month 36.
- The estimated budget breakdown may be adjusted by transfers of amounts between beneficiaries or between budget categories (or both).
- Beneficiaries may not add costs relating to subcontracts not provided for in Annex 1 of GA, unless such additional subcontracts are approved by an amendment or in accordance with Article 13 of GA.
- Evaluations may be started during implementation of the action and up to five years after the payment of the balance.

4.8 Intellectual property rights

IPR overall approach and detailed issues has been agreed and signed in CA. PC will oversee the process and advice the project on all aspects of Knowledge Management and patent filing. PC will also be in charge of maintaining a schedule of knowledge produced during the project and, in conjunction with the partners involved, assessing the opportunities to apply for patents or declare copyrights.

- Results are owned by the beneficiary that generates them.
- Two or more beneficiaries own results jointly if they have jointly generated them and it is not possible to establish the respective contribution of each beneficiary, or separate them for the purpose of applying for, obtaining or maintaining their protection.

Documentation

Previous to any publication, the author of the communication will inform other partners about the intention to publish and will circulate an abstract of the publication one week in advance, so that other partners can detect any potential conflict and reach consensus on the content to be communicated.

Partners are given one week for reaction to the abstract. Silence will be taken as approval.

5 Quality assurance

5.1 Documentation

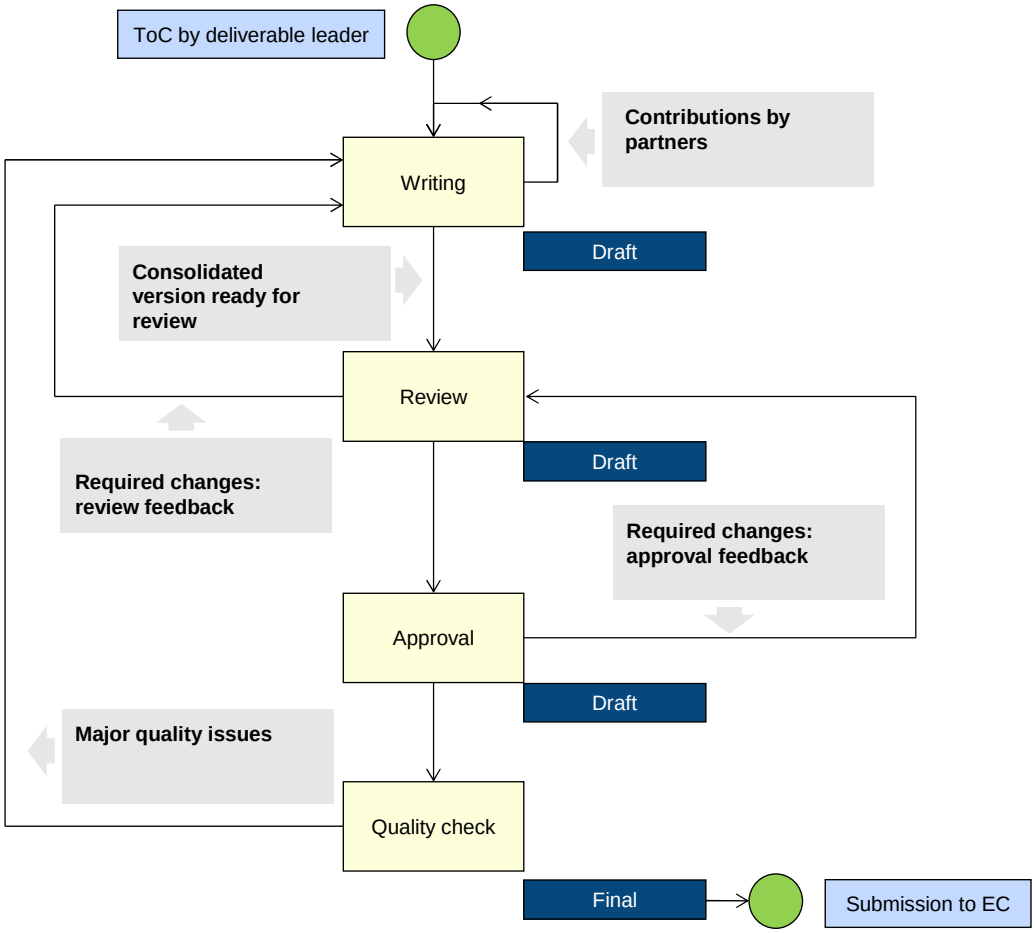
Quality review procedure for documents starts four weeks before the official submission of the deliverable to the EC, so deliverable editor must consolidate a version one month ahead of the official issue date. The draft is uploaded to the CIPSEC repository for any interested partner to review and provide feedback.

Every deliverable is reviewed by two quality assessors (internal reviewers), who are assigned on a yearly basis. The quality assessors are members of the project team, but they are not involved in the work that leads to the deliverable they review. The internal reviewers are expected to evaluate the deliverables and provide feedback according to the following criteria:

Criteria	Scope
Technical	■ Technical decisions are appropriately elaborated and justified.
Innovation	■ Innovative aspects are sufficiently drawn up and well explained. ■ Described work represents technical innovation or advance ahead the state-of-the-art and is clearly exposed. ■ Described work is expected to represent a significant impact (e.g. in standards, internal to the Consortium, etc.). ■ The deliverable will lead to further outputs, such as papers, standards contributions, or exploitable outcomes.
Style and format	■ Executive summary allowing readers to understand document objectives and scope. ■ Clear writing and logical order: easy to read and to understand by different types of public, but specially it targets adequately the intended audience. ■ Content is focused on key issues, with a suitable level of detail. ■ Completeness: there are no significant omissions. ■ Suitable conclusions. ■ Appropriate references. ■ Template compliance. ■ Correct English spelling and grammar. ■ Content-free of relative temporal references.

The feedback by the quality assessors is documented in a reviewed document. The feedback is implemented under supervision of the work package leader in close collaboration with the deliverable editor, who is actually the one executing the quality improvement. The deliverable editor must consolidate a revised version of the deliverable for approval two weeks.

The deliverable undergoes a subsequent release check by the Project Coordinator. This review might call for additional quality improvements by the deliverable authors.



Process Stage	Starts When	Duration	Roles involved	
Writing			Deliverable editor Involved participants	
Review	4 weeks before submission date	2 weeks: 1 reviewing + 1 updating	Deliverable editor Reviewer	
Approval	2 weeks before submission date	1 week	Deliverable editor Approval reviewer	Security Advisory Board
Quality check	1 week before submission date	1 week	Deliverable editor Project Coordinator	

During the document management process and, specially, during the review process several issues might arise:

- A delay of n days must be notified by document editor to PC and WP leader at least 2n days before the due date. Recovery actions must be defined and agreed between the deliverable editor and the WP leader in order to reduce the impact of the delay as much as possible. The WP leader briefs the PC about the decision.
- If PC does not accept the deliverable before delivery date due to lack of quality or due to other reasons:
  - Deliverable editor, WP leader and PC will agree on a recovery plan.
  - PMB could be reached for corrective actions if PC deems the issue is serious.
  - If needed, PC will inform Project Officer about the issue and the corrective measures.

5.2 Software

The quality level of a software component can be assessed by certain characteristics. In particular, the ISO/IEC 9126 standard describes a software quality model that proposes the following six characteristics (factors), which are sub-divided into sub-characteristics (criteria), for assessing software quality.

For a given development, not all the characteristics must be necessary applicable. Characteristics can only be measured (and are assumed to exist) when the related functionality of a given system is present. The idea behind having a comprehensive list is to have these characteristics in mind when developing the different outcomes, but also when reviewing the associated deliverables.

Functionality	**Reliability**	**Usability**
It refers to how well software provides desired functions. It can be used for assessing, controlling and predicting the extent to which the software satisfies the functional requirements.	It defines the capability to maintain the level of performance when used under specified conditions for defined periods of time.	It refers to the ease of use for a given function. This is, how well software can be understood, learned, used and liked by the user.
■ Suitability. ■ Accuracy. ■ Interoperability. ■ Security. ■ Compliance.	■ Maturity. ■ Fault-tolerance. ■ Recoverability.	■ Understandability. ■ Learnability. ■ Operability. ■ Attractiveness.
Efficiency	**Maintainability**	**Portability**
It is concerned with the utilisation and time performance (minimizing time overhead) of resources when providing the required functionality under stated conditions.	It is the effort needed to make modifications for error correction, improvement, or adaption to changes in the environment or requirements.	It is the ability of software to be transferred from one environment to another.
■ Time behaviour. ■ Resource behaviour.	■ Analysability. ■ Changeability. ■ Stability. ■ Testability.	■ Adaptability. ■ Installability. ■ Co-existence. ■ Replaceability.

Framework of reference

The framework of reference provides the perimeter that allows everyone involved in the development and operation of the software to have a clear perspective about what the guidelines to address this activity should be. The following lines of action are proposed:

- Technology architecture: MVC pattern will be applied, in order to split application data, user interface, and control logic into three distinct components.
- Data model standards: nomenclature, standardization criteria and criteria for performance improvement.
- Design rules: recommendations and best practices for data access, logical and physical design of information storage structures, and naming.
- Design patterns: best practices used by experienced software developers that are not language-specific; so, they should be considered as templates to be implemented in the correct situation.
- Assurance inspection based upon quality control of coding and data models.
- Stress and performance requirements, in accordance with guidelines for establishing the maximum acceptable response times depending on context and workload levels.

Technical checking

Version management and delivery might include a set of technical checks that are applicable to both the source code and the generated results. While not directly perceived by the end user, it allows a quality improvement in terms of clarity, maintainability and system performance. Proposed verification points are listed below.

Check	Scope
Data model	To review and validate the logical and physical data models generated during analysis and design phases, checking that it follows the rules of good design, naming rules established in technical regulations, and that the designed structure for data have been properly implemented and can cover the requirements.
Static source code	Verification of static code consists of checking the quality of the source code based on the applicable best practices. sonarqube
Services	Services will be functionally certified as far as performance and stability criteria are concerned.
Deployment	It will ensure that new versions can be implemented upon an environment that has the required infrastructure, core platforms and components.
Performance, stress and resource consumption	This activity aims to certify the right performance of modules under overload and stress situations. Different tests will be carried out on a simulation-based scenario: concurrent users, test duration, and rate of increase in the number of users.

Functional checking

These activities intend to ensure that software outcomes are free of functional errors. These tests are executed straight on the deployed platform and are strongly related to the perceived quality for the end user. Hence they are of utmost importance. Specifically, the project team will carry out the following checks:

Check	Scope
Functional verification	Certify that the developed software is functionally tailored to the needs raised by the user.

Check	Scope
Verification regression testing	Ensure the proper functioning of the framework beforehand any rise to production.
Solution assessment	Experts support users for assessment, providing functional, methodological and technical expertise.
Analysis of perception	The technical and functional tests described above allow to measure product quality quantitatively. However, they do not allow rating an important aspect likewise, such quality perceived by the user. To do this, analysis of perceived quality by organizations / departments and end users is proposed.

Coding standards

When making the development of the different modules, coding criteria should be established to ensure that source code has reached a certain quality.

There is a plethora of tools designed to support developers for compliance with established rules and conventions, helping them to identify code that do not meet these rules. The most recognized in this area are CheckStyle and PMD.

	**Checkstyle**	It helps programmers to write Java code matching coding standards. It automates the process of checking Java code to release developers of this important but tedious task.
	**PMD**	Scanning tool for Java code that seeks potential risks: bugs, dead code, not optimized code, complex expressions, duplicate code, etc. It integrates with best known development environments.

Quality Management Platform

Once the tools to ensure the quality of the source code, unit testing, and automated integration have been defined, it is necessary to integrate them under a unified platform for verification of software quality and implementation tests.

Additionally, there must be a repository that eases project managers, quality managers and members of the development team to obtain reports and statistics on the status of projects, and compliance regarding quality indicators and test coverage.

For this purpose the use of SonarQube™ (formerly known as Sonar) is suggested. SonarQube™ is a centralized portal that allows managing code quality of developed software, providing visual information and monitoring about evolution of the indicators for each project.

Feature	sonarqube
Dashboard	Overview of the status and quality of the projects portfolio.
Source code inspection	Ability of navigate through projects, components, and source code packages to evaluate quality, test coverage, and to identify rule violations of a particular object.
Coding rules	Exhaustive catalog of rules and coding standards that allow designing a profile of quality assurance that meets all needs.
Unit tests	Evaluation and analysis of the covered percentage of unit tests associated with the project source code.
Standard metrics	Standard metrics related with code, cyclomatic complexity, duplicate code, comments, etc.
Evolution	Statistics associated with the evolution of each project, or group of projects, analyzing trends in compliance with rules, code size, test coverage, etc.
Maven	Maven plugin integration.
Integration with existing components	Orchestration and use of the most commonly used quality analysis tools: CheckStyle, PMD, Findbugs, Clover, Cobertura, etc.
Plugins	Extension of functionality, reports and statistics from specific plugins developed for Sonar.
Security	Ability to require authentication for access to the projects maintained in the portal.

Continous integration

Systems that have been developed under a version control platform, and have been managed and built upon Maven, need frequent further integration of the code developed by different team members in order to:

- Minimize the risk of issues, delays, and quality shortages surrounding the final integration.
- Prevent non-timely availability of a certified and stable version.

Each of the integrations is verified by an automated system for test design and execution, to allow error detection regarding integration as quickly as possible. Most development teams qualify this method as ideal to significantly reduce integration issues, allowing quick development of integrated and completed software. The advantages that come from the use of a continuous integration system are:

- Developers can detect and troubleshoot integration issues on a seamless basis, preventing last minute problems in the construction and delivery of the final product.
- Uninterrupted availability of a version for testing, demos, presentations or beforehand releases.
- Immediate and continuous execution of unit tests.
- Continuous monitoring of project quality metrics.

Jenkins is an automation engine with an unparalleled plugin ecosystem to support a variety of tools in delivery pipelines, whether the goal is continuous integration, automated testing, or continuous delivery.[4]

Feature	Jenkins
Continuous Integration and Continuous Delivery	As an extensible automation server, Jenkins can be used as a simple CI server or turned into the continuous delivery hub for any project.
Easy installation	Jenkins is a self-contained Java-based program, ready to run out-of-the-box, with packages for Windows, Mac OS X and other Unix-like operating systems.
Easy configuration	Jenkins can be easily set up and configured via its web interface, which includes on-the-fly error checks and built-in help.
Plugins	With hundreds of plugins in the Update Center, Jenkins integrates with practically every tool in the continuous integration and continuous delivery toolchain.
Extensible	Jenkins can be extended via its plugin architecture, providing nearly infinite possibilities for what Jenkins can do.
Distributed	Jenkins can easily distribute work across multiple machines, helping drive builds, tests and deployments across multiple platforms faster

Platform-specific security recommendations

Where applicable, following recommendations will be considered:

- iOS Security

  https://www.apple.com/business/docs/iOS_Security_Guide.pdf

- Android Best Practices for Security & Privacy

  https://developer.android.com/training/articles/security-tips.html

- Java Coding Guidelines. CERT Division of the Software Engineering Institute at Carnegie Mellon University identified "best" coding practices:

  https://www.securecoding.cert.org/confluence/display/java/Java+Coding+Guidelines

6 Risks assessment

Risk Assessment is a continuous process oriented to early identification of any deviation in the achievement of objectives and / or scope of the project work plan, in the foreseen timing with the allocated resources, and with the expected quality. Risk assessment intends to apply the right countermeasures and considers the following steps:

<table>
<tr><th>Stage</th><th colspan="5">Scope</th></tr>
<tr><td>Identify</td><td colspan="5">Seek for risks before they materialize. Methods to identify risks include: monitoring project activities, examining documentation, observing, and participating in discussions and meetings.</td></tr>
<tr><td rowspan="13">Analyse</td><td colspan="5">Processing risk data into decision making oriented-information.</td></tr>
<tr><td colspan="5">Area: cost, schedule, quality or scope.
Related WP where the risk could happen.</td></tr>
<tr><td colspan="5">Probability (P)</td></tr>
<tr><td>1</td><td><1%</td><td colspan="3">Highly Unlikely/Improbable. Could ignore, but leave on risk register</td></tr>
<tr><td>2</td><td>1 - 20%</td><td colspan="3">Not very likely. Low, but not impossible</td></tr>
<tr><td>3</td><td>21 - 49%</td><td colspan="3">Likely/Possible. Fairly likely to occur</td></tr>
<tr><td>4</td><td>50 - 85%</td><td colspan="3">Very Likely. More likely to happen than not</td></tr>
<tr><td>5</td><td>>85%</td><td colspan="3">Almost Certain. Assume risk will occur</td></tr>
<tr><td colspan="2">Impact (I)</td><td>Effort</td><td>Delivery</td><td>Performance</td></tr>
<tr><td>1</td><td>Trivial</td><td>Trivial increase.</td><td>Negligible.</td><td>A few shortfalls in non-key acceptance criteria.</td></tr>
<tr><td>2</td><td>Minor</td><td>Small increase.</td><td>Small setback.</td><td>Some shortfalls in one or two non-key acceptance criteria.</td></tr>
<tr><td>3</td><td>Moderate</td><td>Significant increase.</td><td>Significant setback.</td><td>Substantial shortfall in one or two key acceptance criteria. Single non-critical criteria missed.</td></tr>
<tr><td>4</td><td>High</td><td>Large increase.</td><td>Large setback.</td><td>Significant shortfalls in more than two key acceptance criteria.</td></tr>
<tr><td>5</td><td>Severe</td><td>Very large increase.</td><td>Very large setback.</td><td>Major shortfall in any key acceptance criteria. Major criteria missed.</td></tr>
<tr><td colspan="2">P x I</td><td>1 – 5
Low risk
(Acceptable)</td><td>6 – 15
Medium risk
(Undesirable)</td><td>16 – 25
High risk (Unacceptable)</td></tr>
<tr><td>Plan</td><td colspan="5">Translate risk information into decisions and mitigation actions. A risk response plan should include the strategy and action items to address the strategy. The corrective actions should include what needs to be done, who is doing it, and when it should be completed.</td></tr>
<tr><td>Implement</td><td colspan="5">To execute the decisions and mitigation plans.</td></tr>
<tr><td>Track/control</td><td colspan="5">Monitoring risk indicators and mitigation actions.
Correcting for deviations from planned risk actions. The risk monitoring will be performed in the periodic meetings at the different project levels: WP and PMB meetings.</td></tr>
<tr><td>Communication</td><td colspan="5">All the previous steps are supported by the communication process, so that information and feedback is spread throughout all risk management functions and project management bodies.</td></tr>
</table>

In order to successfully accomplish this Risk Assessment process, the cooperation of project partners is instrumental. Project partners must participate by providing risk input (any issue that might have negative impact over the success of the project), and supporting risk mitigation planning and execution activities. In this sense, Risk Assessment is a shared responsibility among all partners.

Each deliverable editor is responsible for the risk management of the deliverable he/she is in charge of, and directly reports to its WP leader.

At WP level, each WP leader is responsible for the compliance of his/hers WP and reports directly to STC in the areas of quality and scope, and to PC regarding quality, scope, time, and cost.

If a WP leader is not able to manage a certain risk, it will be raised to the PC. Risks involving any interdependency between WPs will be managed by PC. PC can escalate to PMB, depending on the risk nature and severity.

A risk registry is maintained by PC in collaboration with WP leaders.

Some, mainly non-technical, risks (e.g., administrative, financial, legal) may affect multiple WPs and also the partners of the project (such as a partner withdrawing from the project, overspending, IPR conflicts etc). Next table presents in brief such potential risks, their impact and the contingency plan for each case.

Description	WP	Proposed risk-mitigation measures
Replicability for different domains	General	Dissemination and standardisation efforts, adapting the framework requirements to the standards implemented abroad EU.
Regulation		Monitoring throughout project lifetime and post-project commercialization strategy.
Complexity		User-friendly tools and training courses.
Cost		Consortium's costs for providing the security solutions; Client's costs related to dealing with the potential attacks and its consequences
Partner withdrawal / Underperforming partner / Key staff or skills leaving the project		Get early indication to seek similar competencies within consortium. Transfer the budget accordingly. Otherwise initiate adding a new partner.
Delays in milestones or deliverables.		Carefully monitor progress so as to quickly detect any delay. Shift allocated effort to non-critical tasks, even between partners.
Conflict between partners		Decision making process and conflict resolution procedure.
Lack of internal communication.		Regular meetings, appropriate commuinication channels and procedures.
Underestimated effort		Continuous project surveillance and resources reallocation.
Product with similar characteristics		In deep covering of the potential market segments and initiatives running in parallel to the CIPSEC proposal.
Lacking a critical mass of users		Improved dissemination phase and fostered impact.
Difficulties in getting specs	WP2	Consortium and Advisory Board involvement.
Integration issues	WP4, WP5	Focus on a smaller number of deployed features. Decreasing the number of functionalities or the supported features in the operational pilot.

7 Innovation management

Innovation management in CIPSEC is conceived as a top-down process that spreads from the strategic level along all project activities. It merges different capabilities from the project: technology and knowledge (technical activity developed in WP1, WP2, WP3, WP4), market knowledge (WP1, WP5), and project resources (WP6).

The innovation model adopted in CIPSEC consists of a sequence of stages covering from the conception of the idea, at the proposal time, to the commercialization, at the end of the project. Considering the project outcomes, this innovation model describes the process of translating CIPSEC idea into a portfolio of products and services capable of creating value for end-users. Each of these steps involves interaction with the end-users, who actually participate in the conception and features collection of CIPSEC. In this sense, CIPSEC combines technology push innovation (from research to market) with market pull innovation (from market to technical activity).

	Innovation stage	**CIPSEC**		
		Proposal / WP	**Milestone**	
▼ Technology push ▼	Conception	Proposal		▲ Market pull ▲
	Specification	WP1. Adaptation of security components to Critical Infrastructure environments.	MS3. Functionality building blocks. MS4. CI taxonomy.	
	Research			
	Development	WP2. Development of the CIPSEC security framework for Critical Infrastructure environments.	MS5. Architecture system design. MS6. preliminary version of the CIPSEC platform.	
	Validation	WP3. Integration of CIPSEC solution to transportation, health and environment pilots.	MS7. Prototype ready for the operation environment tests. MS9 & MS12. Report for pilot integration. MS10. Preliminary report on CI intra/inter-dependencies. MS11. Adapted and optimized solution for the selected pilots	
		WP4. Refinements towards working prototypes in operational environment.	MS15. System ready for the experimentation. MS16. Prototype demonstration successfully conducted.	
	Commercialization	WP5. Exploitation and dissemination plan including standardization activities.	MS19. The business model for impact creation and exploitation is ready. MS8. Final CIPSEC security framework MS17. Final CIPSEC framework capabilities in TRL8: results evaluation.	

As depicted, stages of the innovation model match the CIPSEC work breakdown structure, project roadmap and project milestones. This allows a clear alignment between project tasks and innovation activity.

Innovation management requires a deep understanding of both market and technical aspects that are surrounding the project. This means scanning the environment in order to gather how external factors can affect the solution. These factors require an innovation environment that allows a seamless flow of knowledge within the Consortium. The collaborative environment should aim at suitable knowledge management of new ideas and innovations, knowledge sharing between project partners, and project work coordination for the alignment of different project phases.

Innovation is a shared responsibility within CIPSEC Consortium, where all partners can contribute, because searching the external environment is more feasible when different partners and different backgrounds are involved. Innovation Committee heads and coordinates efforts in this arena.

8 Conclusions

This project handbook recaps all the rules, guidelines and best practices that will be followed in order to ensure the success of the project. It provides the needed methodology to put in place a smooth communication among the different responsibility layers within the project, and the different kind of tasks: management, technical and dissemination. It intends to harmonize the work performed along the different dimensions of the project to make it converge on a global high-quality result. The main goal is to guarantee the satisfaction of the European Commission as funding body of the project as well as of the different stakeholders expecting the best outcomes from CIPSEC.

9 Annex

Acronyms

AEGIS	AEGIS IT RESEARCH LTD
ATOS	ATOS SPAIN SA
BD	BITDEFENDER SRL
CA	Consortium Agreement
CI	Critical Infrastructures
CFS	Certificate on the Financial Statements
COMSEC	COMSEC LIMITED
CSI	CONSORZIO PER IL SISTEMA INFORMATIVO (CSI PIEMONTE)
DB	DEUTSCHE BAHN NETZ AG
DoA	Description of Action
DX.Y	Deliverable number y, belonging to WP number x
EC	European Commission
EMP	EMPELOR GMBH
EPCIP	European Program for Critical Infrastructure Protection
ERNCIP	European Reference Network for Critical Infrastructure Protection
F2F	Face to face meetings
FORTH	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
GA	Grant Agreement
HCPB	HOSPITAL CLINIC I PROVINCIAL DE BARCELONA
IT	Information Technology
KPI	Key Performance Indicator
OT	Operational Technology
PAB	Project Advisory Board
PC	Project Coordinator
PMB	Project Management Board
SAB	Security Advisory Board
SME	Small and medium-sized enterprises
STC	Scientific & Technological Committee
SVN	Apache™ Subversion ®
TUD	TECHNISCHE UNIVERSITÄT DARMSTADT
UOP	UNIVERSITY OF PATRAS
UPC	UNIVERSITAT POLITECNICA DE CATALUNYA
WOS	WORLDSENSING LIMITED
WP	Work Package

10 References

[i] Consortium Agreement. H2020 Grant agreement no. 700378. Version v09, 2016-04-21

[ii] Grant Agreement Number 700378, between the Research Executive Agency, ATOS (the coordinator), and the rest of beneficiaries.

[3] ISO 8601:2004. Data elements and interchange formats -- Information interchange -- Representation of dates and times. International Organization for Standardization.

[4] https://jenkins.io/